Glossary

Symbols

10Base2 10 Mbps/baseband/185 metres. The IEEE standard for thinwire (coaxial cable) Ethernet.

10Base5 10 Mbps/baseband/500 metres. The IEEE standard for thickwire Ethernet.

10BaseF 10 Mbps/baseband/Fibre. The IEEE standard for fibre optic based Ethernet.

10BaseT 10 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.

100BaseT 100 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.

802.2 The IEEE standard for the definition of the Logical Link Control protocol for LANs.

802.3 The IEEE standard for the definition of the CSMA/CD (Ethernet) medium access method for LANs.

A

abuse of privilege When a user performs an action that they should not have, according to organizational policy or law.

AARP AppleTalk Address Resolution Protocol.

access control lists (ACL) Lists configured within a router (or layer 3 switch) that define the filters applied to control access between devices subnets or applications.

access mode The level of access i.e. read-only, read-write, or none, that is defined for an SNMP management object.

ACL See “access control lists (ACL)” on page 1.

AC Access Concentrator.

ACK *Acknowledgement*. A response message sent to indicate that a block of data arrived at its destination without error. For example, at the link level, an

acknowledgement indicates successful transmission across a single hardware link; at the transport level, an acknowledgement indicates successful transmission between end systems (possibly over multiple hardware links). See "NAK" on page 21.

Adjacency A state existing between two OSPF routers. These routers build their routing databases by exchanging link state advertisements, often termed *hello* messages. When a pair has completed the process, the routers are said to be "adjacent."

Address mask See "subnet mask" on page 29.

Address resolution The process of resolving and mapping hardware MAC addresses into their corresponding network layer IP addresses. Depending on the underlying network, address resolution may require broadcasts on a local network. See "ARP" on page 3, and "RARP" on page 26.

address resolution protocol See "ARP" on page 3.

Aging The process applied to a routing table, such as an OSPF link state database, whereby entries are aged to prevent the database filling up with entries that are no longer valid. If an entry reaches a specified maximum age before an update is received for that entry, the entry is no longer used in routing decisions and is eventually removed from the database.

AH *Authentication Header*. An additional IP header, used in both IP version 4 and IP version 6, providing authentication of the IP payload and most of the IP header.

AIS *Alarm indication signal*. A signal transmitted in lieu of the normal signal on an E1 or T1 line to indicate to the receiving equipment that there is a transmission interruption located at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute See "ANSI" on page 2.

AMI *Alternate mark inversion*. A line code (used for T1) that employs a ternary signal to convey binary digits.

anonymous FTP Anonymous FTP enables a user to retrieve documents, files, programs, and other archived data from anywhere in the Internet without having to establish a user ID and password. By using the special user ID of anonymous the network user will bypass local security checks and will have access to publicly accessible files on the remote system. See archive site, FTP.

ANSI *American National Standards Institute*. An organisation responsible for coordinating and approving U.S. standards. Standards approved by ANSI are often called ANSI standards. ANSI is the U.S. representative to ISO.

AppleTalk A networking protocol developed by Apple Computer for communication between Apple Computer products and other computers, that is independent of the network layer on which it is run. Implementations exist for LocalTalk, a 235Kb/s local area network; and EtherTalk, a 10Mb/s local area network.

application-level firewall A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing.

Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than from the internal host.

Area Border Router A term used within OSPF routing systems. An OSPF routing environment comprises an *autonomous system* (AS) that is subdivided into *areas*. Areas communicate with each other via a common *backbone*. An area border router is a router nominated to interface between its own area and the backbone. See the OSPF chapter.

archie A system to automatically gather, index and serve information on the Internet. The initial implementation of archie provided an indexed directory of file names from all anonymous FTP archives on the Internet. Later versions provide other collections of information. See archive site.

archive site A machine that provides access to a collection of files across the Internet. An "anonymous FTP archive site", for example, provides access to this material via the FTP protocol. See anonymous FTP, archie.

area In general terms, an area is a group of contiguous networks and hosts, and routers having interfaces to any of those networks and hosts. Areas are used to reduce routing traffic, since each area maintains its own topological database. In OSPF terminology, *internal routers* route traffic within areas, and *area border routers* link areas to form an autonomous system. In DECnet terminology, a network is divided into areas of up to 1023 *nodes*, and each area has a unique identifier from 1 to 63 (DECnet Phase IV). *Type 1* routers route traffic within areas and *Type 2* or *area routers* route traffic between areas. See "DECnet address" on page 10.

area router In DECnet terminology, an area router routes traffic between DECnet areas. See "DECnet address" on page 10.

ARP *Address Resolution Protocol*. The TCP/IP protocol used to dynamically map a high level IP address to a low-level physical (hardware) address on a local area network. ARP applies only across a single physical network and is limited to networks that support hardware broadcast. See the following entries: "Address resolution" on page 2, "proxy ARP" on page 25, and "RARP" on page 26.

ASCII *American Standard Code for Information Interchange*. A standard character-to-number encoding widely used in the computer industry.

ASIC *Application Specific Integrated Circuit*. An integrated circuit (chip) manufactured to perform a specific function, such as network layer switching.

Note that when this technology is applied to networking, the terminology associated with certain functions changes. For example, the term *router* changes to l*ayer 3 switch*, and the term *bridge* changes to *layer 2 switch*.

assigned A term used with the router to refer to the state of an asynchronous port that currently has a logical connection to a service on the network.

Assigned Numbers A set of values (usually numeric) used by TCP/IP protocols. They are documented in a number of RFCs, the most recent being RFC 1340. See "RFC" on page 26.

assignment A term used with the router to refer to the logical connection between an asynchronous port, to which a user's terminal is connected, and a service on the network which the user is accessing.

asynchronous Transmission in which each character is sent individually. The time intervals between transmitted characters may be of unequal length. Transmission is controlled by *start* and *stop* elements before and after each character. See "synchronous" on page 30.

asynchronous call control (ACC) A facility within a router (or layer 3 switch) that enables it to communicate via an asynchronous device such as a modem, usually to connect through a public switched telephone network (PSTN).

Asynchronous Ports Ports that use an asynchronous mode of transmission. In a router or switch, these ports are often used to connect configuration terminals. See "synchronous" on page 30.

ATTACH A Netware utility that enables a network station to access additional file servers after having logged on to one file server using the LOGIN utility.

attention character A term used with the router to refer to a special character (either [Break] or [Ctrl/P]) that signals to the router that the next character is a function character and should be sent to the terminal server software, not the remote process to which the user is assigned. Function characters signal to the router that a special action is to be taken.

AUI *Attachment Unit Interface*. An Ethernet interface that allows a device to be attached to a range of Ethernet media by using a transceiver, e.g. 10BASE2, 10BASET, 10BASE5, 10BASEF. See "BNC" on page 6.

authentication The property of verifying the actual sender of a message and the procedure to confirm the identity of the sender. Authentication can be subdivided into weak and strong authentication. Traditional reusable passwords are considered weak authentication because, if compromised, they can be used to repeatedly gain access to a host. Stronger authentication methods are normally based on cryptographic techniques and often rely on the authorised user knowing something unique (such as a password or passphrase) and having something (such as a key or hardware token).

authentication token A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

authorisation The process of determining what types of activities a user is permitted to undertake. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity.

autobauding A operational mode of the terminal server software in the router, in which the router automatically adjusts the speed of an asynchronous port to match the speed of the terminal connected to the port.

autonomous system A collection of gateways or routers under one administrative entity using a common interior gateway protocol (IGP). Gateways and routers within an autonomous system have a high degree of trust.

B

B7ZS *Bipolar with 7-zero substitution*. A method for enforcing a minimum ones density on an AMI encoded T1 line, in which bit 7 of an all zero timeslot octet is replaced with a one.

B8ZS *Bipolar with 8-zero substitution*. An AMI line code used on T1 lines in which a unique code replaces occurrences of eight consecutive zero signal elements. The unique code includes BPVs.

backbone A high capacity network component that provides an interconnection path for its attached subnetworks.

BACP *Bandwidth Allocation Control Protocol.* A protocol used to control the bandwidth of a datacommunications channel by increasing or decreasing the number of assigned circuits. The protocol can control the bandwidth of ISDN connections by adding or removing B channels or of PPP connections by adding PPP links from a multilink bundle.BACP is an IETF standard defined in RFC 2125.

bandwidth A way of specifying the capacity of a communications channel. In practical applications, the term is used to specify either a range of analogue frequencies or the rate of a digital transmission. Analogue bandwidth is usually defined as being the difference between the highest and lowest frequencies transmitted and is specified in Hertz (Hz). Digital bandwidth is usually defined as being the highest data rate transmitted and is specified in bits per second (bps).

Note that the *maximum bandwidth* set by the switch's EGRESSLIMIT parameter specifies the maximum data rate supplied *to* a port (from internal queues) prior to transmitting onto the line. This *maximum bandwidth* setting can therefore be lower than the maximum data rate capacity of the port.

BAP

Bandwidth Allocation Protocol. An IETF protocol, defined in RFC 2125, that provides a mechanism for two PPP peers to manage the bandwidth available to the protocols using a multilink PPP bundle by negotiating gracefully to add and remove links from the multilink bundle.

Basic Rate Access A mode of access to an ISDN service that provides two 64 kbit/s B channels for data and one 16 kbit/s D channel for link control and management. The access point is normally at a customer's premises. See "BRI" on page 6, "ISDN" on page 18, and"Primary Rate Access" on page 25.

bastion host A bastion is defined in *Webster's Collegiate Dictionary* as *a projecting part of a fortification*. In networking terms it is a system that often sits between private (trusted) and public (untrusted) networks as a first line of defence. The bastion host applies an access control policy to block unwanted traffic. In practice a bastion host may be a firewall or other custom configured server.

baud The number of times per second that a transmitted signal can change its state. It is sometimes referred to as being the signalling rate. Although the baud rate is sometimes equal to the bit rate, this should not be taken to be a rule. For example, the complex encoding techniques employed by many modems, enable them to transmit bit rates that are far greater than their baud rate.

BBR *Battery-Backed RAM*. See "NVS" on page 23.

BECN *Backward Explicit Congestion Notification*. A bit set in a frame sent from a Frame Relay network to a station attached to the network which indicates that congestion was experienced in the network in the opposite direction to that in which the frame was travelling. It applies to the DLC for the specified frame only. A typical response would be for the station to reduce the rate of transmissions on the specified DLC until congestion eased. See "DLC" on page 11, and "FECN" on page 13.

best-effort delivery Characteristic of network technologies that do not provide reliability at the data link and network layers. The combination of IP and UDP protocols provides a best-effort delivery service to applications.

BIA *Best Information Algorithm*. An algorithm, similar to split horizon, used to determine which interfaces to send routing information broadcasts to, and what the broadcasts should contain.

block A unit of data in NVS. For example, one block is used to store a file.

BNC *Bayonet Nut Connector*. A connector type used for 10BASE2 (thinwire) coaxial cable. It is also used on the router for ISDN Primary Rate and G.703 interfaces. The term bayonet refers to the way the connector slides in and then twists to lock the connection. See "AUI" on page 4.

boot A term used in computing to refer to the process of starting a computer, loading the operating system or executive program from disk or ROM.

BOOTP A forerunner to DHCP, the BOOTP protocol (defined in RFC 951) enables a workstation to obtain its IP address from a network server. Once this phase is completed the workstation may then use the protocol to initiate a file transfer - often to load the boot file - usually using TFTP file transfer protocol. See "DHCP" on page 10.

Border Gateway Protocol (BGP) A routing protocol that enables two routers (or switches) operating in different routing domains to exchange routing information to facilitate inter-domain data transmission. See Chapter 49, Border Gateway Protocol version 4 (BGP-4).

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

BPV *Bipolar violation*. A non-zero signal element in a E1 or T1 ternary line code signal that has the same polarity as the previous non-zero signal element.

BRI *Basic Rate Interface*. In the router, the name of the software module, and the name assigned to logical interfaces, that provide Basic Rate Access to an ISDN service. See "Basic Rate Access" on page 5, "ISDN" on page 18, and "PRI" on page 25.

bridge A device that connects two or more networks and forwards packets between them. Bridges normally operate at the MAC level, for example connecting Ethernets. Bridges can usually be configured to filter packets; that is, to forward only certain traffic. Bridges differ from repeaters and routers in that bridges store and forward complete packets, whereas repeaters simply forward re-timed electrical signals from one cable to another. See "repeater" on page 26, and "router" on page 27.

broadcast A packet delivery system that delivers a copy of a given packet to all hosts attached to the network. For example, Ethernet. See "directed broadcast" on page 10, "multicast" on page 21, and "unicast" on page 32.

BSD *Berkeley Software Distribution*. Implementation of the UNIX operating system and its utilities developed and distributed by the University of California at Berkeley. "BSD" is usually preceded by the version number of the distribution, e.g., "4.3BSD".

buffer A block of memory used to store data temporarily.

bundle A number of active PPP links, with a common peer, grouped together as a single PPP link using the multilink procedure as defined in RFC 1990.

C

Cache An area of fast memory used for storing frequently used data rather than accessing slower general storage areas such as disk or slower speed RAM.

CCITT *International Consultative Committee for Telegraphy and Telephony*. A unit of the International Telecommunications Union (ITU) of the United Nations. CCITT sets standards, known as "Recommendations," for all internationally controlled aspects of analog and digital communications. For example, CCITT defined the X.25 network protocols.

CCP *Compression Control Protocol.* A PPP NCP used to negotiate the use of compression on a PPP interface. CCP is an IETF standard defined in RFC 1962.

CCS *Common Channel Signalling*. The use of a single dedicated channel to carry call signalling information for all the channels on a E1/T1 line, as opposed to in-band signalling.

CD *Carrier Detect*. A modem control line which is an input to the router from a modem or NTU signifying that the modem or NTU is receiving a valid carrier signal. CD asserted at both ends of a data link is an indication that the link is operational.

CFLASH *CompactFlash* A small, removable mass storage device that uses FLASH memory.

CHAP *Challenge-Handshake Authentication Protocol*. A method of authenticating users accessing a computer resource over a point-to-point network link. The method comprises a three-way process whereby an authenticator sends a challenge message with a keyword to a peer system. The peer must then apply a common algorithm to the keyword and return the result to the authenticator. The authenticator applies the same process internally and compares the two results. Depending on the match, the authenticator may allow or deny access to the peer system. The authenticator may initiate this process at any time throughout the peer session.

challenge/response An authentication technique whereby a server sends an unpredictable challenge to the user who computes a response using some form of authentication token. See "CHAP" on page 7.

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 transmission errors. The sender computes a checksum and appends it to a

packet when transmitting. The receiver verifies the packet's contents by re-computing the checksum and comparing it to the value sent. Many TCP/IP protocols use a 16-bit checksum computed with one's compliment arithmetic.

CIR *Committed Information Rate.* The rate, measured in bits per second and averaged over a set time interval, at which a Frame Relay network provider contracts to transfer information across the network under normal conditions.

circuit A term used in networking to refer to a logical stream of data between two users in the network. A single physical link may have several circuits running on it.

CLLM *Consolidated Link Layer Management.* A mechanism used in Frame Relay networks for link management, in which the network sends messages to devices attached to the network containing information about the status of the DLCs used by the device.

CLNS Connectionless Network Service.

coaxial cable An electrical cable in which a piece of wire is surrounded by insulation and a tubular conductor (or mesh) whose axis of curvature coincides with the centre of the piece of wire, hence the term "coaxial". Examples include thick- and thinwire Ethernet.

Collision The meeting of two simultaneously transmitted signals on an Ethernet LAN cable segment. Ethernet networks overcome collision problems by requiring both transmitting stations to stop and wait a random time before retransmitting.

CompactFlash *CFLASH* A small, removable mass storage device that uses FLASH memory.

compression A technique for reducing the size of data stream, prior to storage or transmission. Mathematical algorithms are often applied that remove repeated or unused components of a data stream. When the file is opened or the data stream received, a complimentary algorithm is applied to reconstruct the original data stream.

congestion A condition that occurs when the offered load exceeds the capacity of a data communication path.

connection (Netware) A number assigned to any station that attaches to a Netware file server, to control communications between the file server and the attached station. Each attached station has a different number.

connectionless A model of interconnection in which communication takes place without first establishing a connection. It is sometimes called datagram. Each packet of data is treated as a separate entity containing a source and destination address. Usually, connectionless services can drop packets or deliver them out of sequence. Packets may also take different routes to the same destination. Examples include LANs, IP and UDP.

connection-oriented The model of interconnection in which communication proceeds through three well-defined phases: connection establishment, data transfer, connection release. Examples are X.25 and TCP.

CoS *Class of Service.* A way for time-critical applications to get the best possible service when the system is overloaded.

CRC *Cyclic Redundancy Check*. A method of checking the integrity of received data, using a polynomial algorithm based on the content of the data. The term is also used to refer to the computed value. The sender computes a CRC and appends it to a packet when transmitting. The receiver verifies the packet's contents by re-computing the CRC and comparing it to the value sent. CRCs are more expensive to compute than a checksum, but can detect more errors.

cryptographic checksum A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting file system tampering on UNIX.

CPU *Central Processing Unit*. In the router, this is a microprocessor that controls all operations necessary to the functioning of the router.

CSMA/CD *Carrier Sense Multiple Access with Collision Detection*. The access method used by local area networking technologies such as Ethernet. Multiple stations contend for access to a transmission medium by listening to see if it is idle. A mechanism is provided to detect when two stations simultaneously attempt to transmit data.

D

daemon A UNIX term referring to a process that is not connected with a user but performs a service, such as a mail daemon or an FTP server daemon.

data driven attack A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

data flow A categorisation of packets that obey a predefined rule and are processed in a similar manner.

data link layer The network layer that is responsible for data transfer across a single physical connection, or series of bridged connections, between two network entities.

data over voice A method of emulating an ISDN voice call over which data can be transmitted.

datagram A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network. See "frame" on page 14, "packet" on page 23.

DB37 A 37-pin D-shaped plug or socket which is commonly used to provide RS-232 or RS-530 interfaces. The router uses DB37 sockets in conjunction with transition cables to provide a composite X.21, RS-232 or V.35 interface.

DCE *Data Communication Equipment.* The term applied by X.25 protocols to equipment that forms a packet switching network, to distinguish it from the computers and terminals that connect to the network. See "DTE" on page 11.

DDP *Datagram Delivery Protocol*. A protocol used to transmit AppleTalk datagrams across the Internet.

DE *Discard Eligibility*. A bit set in a frame sent from a station connected to a Frame Relay network, to the Frame Relay network, which indicates that this frame can be discarded in preference to others if congestion is experienced. See "BECN" on page 6, and "FECN" on page 13.

debugging The process of rectifying faults, usually existing within computer code.

DECnet Digital Equipment Corporation's proprietary network architecture.

DECnet address A number assigned to each node in a DECnet network of the form *area.node*, where *area* is a number from 1 to 63 (for DECnet Phase IV) identifying the area, and *node* is a number on the range 1 to 1023 which identifies the DECnet node within the area. Each node in a DECnet area must have a unique node number, but nodes from different areas may have the same node number. The combination of area and node should be unique within the network.

default route A routing table entry which is used to direct packets addressed to networks not explicitly listed in the routing table. See "route table" on page 27.

default traffic class A traffic class which provides a "catch-all" for any traffic that does not fit one of the user-defined traffic classes. See "traffic class" on page 31.

defence in depth The security approach whereby each system on the network is secured to the greatest possible degree.

DES *Data Encryption Standard*. A widely used 56-bit encryption algorithm. DES encryption is required to be supported by all SSH clients and servers.

designated router In DECnet terminology, a given broadcast circuit (e.g. an Ethernet) will have one designated router to which end nodes forward all packets requiring routing decisions. It is sometimes also called the *default* or *preferred* router. In OSPF terminology, in a multi-access network with more than one router, the designated router generates the link state advertisements for the network as well as performing other special functions. In PIM-SM terminology, the designated router is elected by all routers in the subnetwork to do all the PIM multicast routing for the subnetwork.

DHCP *Dynamic Host Configuration Protocol*. A method of automatically allocating IP addresses. A DHCP server holds a pool of IP addresses from which it draws individual ones as it allocates them to users when they log on.

dialup A temporary, as opposed to dedicated, connection between machines established over a standard phone line.

directed broadcast A packet deliver system that delivers a copy of a given packet to "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 routing A routing method whereby routers build a table of distances against available paths, that is, distance vector. In practice, cost factors may be built into the router distance components. The router selects the appropriate path (router port) usually based on the least cost route.

DL *Data link*. A 4 kbps data link provided by the T1 ESF that is used for maintenance and performance monitoring of the T1 link.

DLC *Data Link Connection*. The data link connection (circuit) between two stations in a Frame Relay network.

DLCI *Data Link Connection Identifier*. A number used to uniquely identify a DLC to the local station. Each DLC from a given station has a different DLCI, but the same DLC can be identified by different DLCIs by the two stations at each end of the DLC.

DMAC *Direct Memory Access Controller*. An integrated circuit that mediates the transfer of data between a peripheral, such as an Ethernet controller, and memory, without CPU intervention.

DNS *Domain Name System*. The distributed name/address mechanism used in the Internet. It comprises distributed online databases that contain mappings between human-readable names and IP addresses, and servers which provide translation services to client applications.

DNS spoofing Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

domain A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), e.g., "machine.company.com". See "DNS" on page 11.

dot address See "dotted decimal notation" on page 11.

dotted decimal notation The syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses in the Internet, e.g. 172.16.9.197.

downline loading A term used with the router to refer to the process of transferring a code patch over a TCP/IP link from a TFTP server to the router. It is a mechanism for fixing bugs and adding enhancements to the software used in the router.

DS1 *Digital signal level 1*. A digital signal transmitted at the nominal rate of 1.544 Mbit/s.

DSAP *Destination Service Access Point*. The address for the destination user of a service. A remote IPX process would be considered the DSAP from the point of view of the local data link module. See "SSAP" on page 29.

DTE *Data Terminal Equipment*. The term applied by X.25 protocols to computers and terminals to distinguish them from the packet switching network to which they connect. See "DCE" on page 9.

DTR *Data Terminal Ready*. An RS-232C electrical signal asserted by the router on a port when it is ready to transmit and receive data on the port.

E

E1 A wide area digital transmission scheme that carries data at a nominal rate of 2.048 Mbit/s.

ECP *Encryption Control Protocol*. A PPP NCP used to negotiate the use of encryption on a PPP interface. ECP is an IETF standard defined in RFC 1968.

EGP *Exterior Gateway Protocol*. A reachability routing protocol used by a gateway or router in one autonomous system to advertise the IP addresses of networks in that autonomous system to a gateway or router in another autonomous system.

Email *Electronic mail*. A system enabling a computer user to exchange messages with other computer users (or groups of users) via a communications network. Electronic mail is one of the most popular uses of internets.

Email address The address that is used to send electronic mail to a specified destination. For example, "ford.prefect@earth.com".

encapsulation The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

ENCO *Encryption/Compression Facility*. The software in the AR router responsible for providing encryption and compression services to other software modules, such as routing modules.

encryption The process of rendering messages unintelligible by applying a mathematical algorithm to both ends of a data channel. At the sending end, a *key* number is applied to a mathematical algorithm in order to encrypt the data. At the receiving end, either the same key or one mathematically related to it, is applied in a reverse process to resolve the original message.

EPROM *Erasable Programmable Read-Only Memory*. These devices contain the system software on the router, and may need to be changed in some circumstances to upgrade the software to a new release. They are non-volatile, meaning they retain their information during power-down. See "FLASH" on page 14.

ER PDU Error Report PDU.

ERP PDU Echo Reply PDU.

ERQ PDU Echo Request PDU.

ES-IS *End System to Intermediate System*. An ISO standard (9542) for enabling each end system (termed an *ES)* and router (termed an *IS)* to learn each other's existence and address. They achieve this by exchanging ESH and ISH *hello* messages.

ESF *Extended superframe format*. A T1 multiframe format that has 24 basic frames in the multiframe, and supports multiframe CRC and a Data Link.

ESP *Encapsulating Security Payload*. A method of encapsulating all or part of a data packet within an IP datagram.

Ethernet A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thinwire coaxial cable (10BASE2), thickwire coaxial cable (10BASE5), twisted pair cable (10BASET), or fibre optic cable.

EtherTalk A data link level protocol developed by Apple Computer that allows an AppleTalk network to be connected by Ethernet.

exclusion filter A process in which a router discards data from sources whose addresses appears in an exclusion list, rather than forwarding the data to other networks, effectively filtering the data from internetwork traffic. See "inclusion filter" on page 16.

F

fast buffer memory Fast buffer memory is cached by the CPU and is available only for program variable storage. It cannot be used for packet buffers. Also called *fast memory.*

FCS *Frame check sequence*. Bytes added to a frame so that the integrity of the frame may be checked. Typically the bytes are a CRC of the data in the frame.

FDDI *Fibre Distributed Data Interface*. A high-speed (100Mbps) fibre optic LAN standard based on token ring. See "LAN" on page 19.

FECN *Forward Explicit Congestion Notification*. A bit set in a frame sent from a Frame Relay network to a station attached to the network which indicates that congestion was experienced in the network in the same direction to that in which the frame was travelling. It applies to the DLC for the specified frame only. See "DLC" on page 11, and "BECN" on page 6.

FIFO *First In, First Out*. A first in, first out buffer. FIFO buffers are useful for handling data that arrives in bursts, as the data can be buffered until the computer is able to process it. Data is processed (removed from the buffer) in the order it was added to the buffer. A contrasting buffer system is LIFO (Last In, First Out), often referred to as a *stack*.

file server (Netware) A computer that provides network stations with controlled access to shared resources (such as disk subsystems and printers) attached to the file server or the network. The Netware Operating System is loaded on the file server and controls security and station-to-station communications.

file transfer The process of copying of a file from one computer to another over a computer network. See "anonymous FTP" on page 2, and "FTP" on page 15.

File Transfer Protocol See "FTP" on page 15.

filter Within the router, A filter is a process used to select which packets will be processed by the router, and which will be ignored or discarded. Selection may be based on addresses (such as exclusion and inclusion filters) or protocol type (such as SAP filters).

FiltSpec *Filter specification*. The specification of the source of a traffic flow for which resource reservations are made.

firewall A system or combination of systems that enforces a boundary between two or more networks.

flag A program-readable indicator that can be used to signal an event or a state, or provide simple data values (e.g. TRUE/FALSE, ON/OFF, use option X). For example, in the HDLC data link protocol, the bit pattern 01111110 is used to flag the beginning and end of a frame.

FLASH A new memory technology which combines the non-volatile features of EPROMs with the easy in-system reprogramming of conventional volatile RAM. See "EPROM" on page 12.

flash compaction A process used to remove all deleted files within the flash memory. The current files are first copied to a new location and then the block is cleared from flash memory. Compaction occurs when the flash used for deleted files reaches a preset limit.

flow control Control of the rate at which devices inject packets into a network, usually to avoid congestion. Flow control mechanisms can be implemented in hardware and/or software, at various protocol layers, and with varying complexity. See "XON/XOFF" on page 34.

flow group Used to group similar traffic together.

FlowSpec *Flow specification*. The specification of the characteristics of a traffic flow for which resource reservations are made.

fragment A piece of a packet. When a router is forwarding an packet to a network that has a maximum packet size smaller than the packet size, it is forced to break up that packet into multiple fragments. These fragments will be reassembled at the destination. See "fragmentation" on page 14, and "MTU" on page 21.

fragmentation The process in which a packet is broken into smaller pieces to fit the requirements of a given physical network. The reverse process is termed reassembly. See "fragment" on page 14, and "MTU" on page 21.

frame A self-contained unit of link layer data usually containing a header with addressing information and a trailer with a CRC. That is, network layer packets are encapsulated with additional link layer information to become frames. See "datagram" on page 9, "encapsulation" on page 12, and "packet" on page 23.

Frame Relay Frame Relay is a network service, defined by various CCITT, ANSI and vendor standards, to which stations (DTEs) may connect via synchronous lines. Data is sent between the stations via circuits in the Frame Relay network. Frame Relay is similar to X.25 in that a single physical link to the network carries many different streams of data. However, Frame Relay operates only at the data link layer, and is simpler and more efficient than X.25. Error detection and correction is left to higher protocol levels.

FRLI *Frame Relay Logical Interface.* (pronounced "frilly") An entity representing a group of one or more DLCs on a Frame Relay interface as a single interface for use by a higher layer protocol.

FTP *File Transfer Protocol*. The TCP/IP standard, high-level protocol for transferring files from one computer to another over a network. FTP is also usually the name of the program that the user invokes to execute the protocol. *See "anonymous FTP" on page 2.*

function A special character sent to the terminal server software in the router, rather than the remote process to which the user's terminal is assigned, to indicate that a special action is to be taken. A function is sent to the router by pressing the *attention* character ([Break] or [Ctrl/P]) followed by a function character.

G

G.703 A CCITT Recommendation defining the physical and electrical characteristics of a 2048 kbps interface. Primary Rate Access to an ISDN service always uses a G.703 interface, but G.703 can also be used for non-ISDN applications.

GARP *Generic Attribute Registration Protocol*. A generic protocol to enable stations on a bridged LAN to register or de-register attribute values such as VLAN identifiers.

gateway The original Internet term for what is now called router or more precisely, IP router. In modern usage, the terms "gateway" and "application gateway" refer to systems that perform translation from some native protocol or physical data format to another. Examples include electronic mail gateways which translate between X.400 and RFC 822 mail message formats. See "router" on page 27.

Generic Packet Classifier Defines packet matching rules that classify packets into data flows.

GUI *Graphical User Interface.* The portion of a computer system accessed by users whereby they select functions by using controls such as icons, drop-down lists, and scroll bars rather than by entering text-based commands.

H

HDB3 *High density bipolar of order 3*. An AMI line code used on E1 lines, in which a unique code is used to replace occurrences of four consecutive zero signal elements. The unique code includes BPVs.

HDLC *High level Data Link Control*. ISO's data link level protocol for OSI. It was adapted by CCITT for its link access protocol (LAP/LAPB) used with X.25 networks. See "LAP/LAPB" on page 19.

header The portion of a packet, preceding the actual data, containing source and destination addresses, and error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time. See "Email" on page 12, and "packet" on page 23.

hello packet Hello packets are used in a number of network protocols to perform similar functions. Typically, a Hello packet advertises a node's presence to the network or establishes and maintains information about the presence of other nodes (including hosts and routers) in the network.

heterogeneous network A network running multiple network layer protocols such as DECnet, IP, IPX.

HMAC *Hashed Message Authentication Code* A method of generating a message authentication code using a secure hash function such as MD5 or SHA-1. HMAC is defined in RFC2104.

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

host An (end-user) computer system that connects to a network, such as a PC, minicomputer of mainframe.

host-based security The technique of securing an individual system from attack. Host based security is operating system and version dependent.

HTTP HyperText Transport Protocol. A protocol used for conveying information across the World Wide Web. For example, HTTP is often used to enable communication between Web servers or between a Web server and a user browser.

hunt group A set of DCE-DTE links that can be accessed from a remote DTE via a single DTE address.

I

ICMP *Internet Control Message Protocol*. The TCP/IP protocol that is used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers, and hosts use ICMP to send reports of problems about datagrams to the original source that sent the datagram.

IDEA An encryption algorithm, optionally supported by SSH clients and servers.

IEEE *Institute of Electrical and Electronics Engineers*. A standards-making body in the U.S. responsible for the 802 standards for local area networks.

IEEE 802.3 See “802.3” on page 1.

IETF *Internet Engineering Task Force*. One of the task forces of the IAB (*Internet Activities Board*). It is a large, open community of network designers, operators, vendors, and researchers whose purpose is to coordinate the operation, management and evolution of the Internet, and to resolve short-range and mid-range protocol and architectural issues. It is a major source of proposals for protocol standards which are submitted to the IAB for final approval.

IGMP *Internet Group Management Protocol* A protocol for managing the addition and deletion of hosts from multicast groups.

IGP *Interior Gateway Protocol*. The generic term for protocols that exchange routing information between collaborating routers within an autonomous system. RIP and OSPF are examples of IGPs. See “EGP” on page 12, “OSPF” on page 23, and “RIP” on page 26.

inclusion filter A process in which a router forwards data to other networks only from sources whose addresses appear in an inclusion list, effectively

filtering data from other sources from internetwork traffic. See "exclusion filter" on page 13.

insider attack An attack originating from inside a protected network.

instance A term used in the router to refer to an instantiation of an interface type associated with a particular synchronous port or Ethernet port on the router.

interface One of the physical ports on the router, including the Ethernet, asynchronous and synchronous ports.

interface type The type (Ethernet, Frame relay or Point-to-Point) of one of the interfaces on the router.

International Organisation for Standardisation See "ISO" on page 18.

internet A collection of networks interconnected by a set of routers that allows them to function as a single, large virtual network.

Internet (note the capital "I") The largest internet in the world consisting of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet is a multiprotocol network but generally carries TCP/IP.

Internet address See "IP address" on page 17.

Internet Draft Working documents of the IETF that are usually precursors to RFCs.

Internet Protocol See "IP" on page 17.

interoperability The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully.

intrusion detection Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

Inverse ARP A form of ARP specific to Frame Relay networks that enables a station to request a protocol (such as IP) address of the station at the remote end of a DLC, given the DLCI.

IP *Internet Protocol*. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself. See "dotted decimal notation" on page 11.

IP datagram The fundamental unit of information passed across the Internet. It contains a source and destination address along with data and a number of fields which define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

IP interface An entity representing an IP layer attached to a layer 2 interface and all information the IP routing algorithm needs to know to use the layer 2

interface to transmit datagrams over that physical connection. An IP interface consists of one or more IP logical interfaces.

IP logical interface An entity which represents an IP layer interface and holds all network layer specific information such as network address, mask, metric, etc. Multiple logical interfaces can be bundled together in a single IP interface.

IP splicing/hijacking An attack in which an active, established, session is intercepted and co-opted by the attacker. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorised user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP spoofing An attack in which a system attempts to illicitly impersonate another system by using its IP network address.

IPSEC *IP Security Working Group* An IETF working group responsible for the development of Internet Security features and protocols.

IPX (Netware) *Internetwork Packet eXchange*. A Netware protocol for the exchange of message packets on an internetwork. It is based on Xerox Corporation's Internetwork Packet Protocol.

IPX.COM (Netware) A Netware program that runs on a network station. It loads the IPX/SPX protocol stacks and provides communications with file servers and other network stations. IPX.COM has been superseded by the ODI protocol stack which supports multiple protocol stacks, such as IPX and TCP/IP. See "ODI (Netware)" on page 23.

ISDN *Integrated Services Digital Network*. A technology which combines voice and digital network services in a single medium, making it possible for telecommunications providers to offer customers digital data services as well as voice connections through a single "wire". The standards that define ISDN are specified by CCITT.

IS-IS *Intermediate System-Intermediate System*. The OSI interior gateway protocol for exchanging routing information between routers within an autonomous system. See "ES-IS" on page 12.

ISO ***International Organisation for Standardisation***. An international body that develops standards in many areas, including network protocols. It is best known for the seven-layer OSI (Open Systems Interconnection) suite of network protocols.

J

jumper A small removable plastic encapsulated connector used to select electrical functions. If a jumper is installed, a connection is established, and vice versa. Jumpers in the router must only be moved when the power is disconnected.

K

L

LAN *Local Area Network*. Any physical network technology (such as Ethernet) that operates at high speed (typically 10 Mbits per second or more) over short distances (up to a few kilometres). See "FDDI" on page 13, "MAN" on page 20, and "WAN" on page 33.

LAP/LAPB A modified form of HDLC that CCITT chose as the link level protocol for X.25 networks. LAPB provides for the reliable transfer of a packet from a host to an X.25 packet switch.

LAPD Lightweight Directory Access Protocol. A client server protocol that is used for accessing directory based information in a similar but simplified manner to the X.500 directory protocol.

layer Communication networks for computers may be organized as a set of more or less independent protocols, each in a different layer (also called level). The lowest layer governs direct host-to-host communication between the hardware on different hosts; the highest layer consists of user applications. Each layer builds on the layer beneath it. For each layer, programs at different hosts use protocols appropriate to the layer to communicate with each other. TCP/IP has five layers of protocols; OSI has seven. The advantages of different layers of protocols is that the methods of passing information from one layer to another are specified clearly as part of the protocol suite, and changes within a protocol layer are prevented from affecting the other layers. This greatly simplifies the task of designing and maintaining communication programs.

layer 2 Interface An entity representing the layer 2 interface in the OSI/ISO network model and referred to as a link layer interface. Examples are Ethernet (to be more precise, IEE802.3), PPP, and Frame Relay.

LBO *Line build out*. An electrical network, or equivalent in digital signal processing, used to increase the electrical length of a cable section.

LC *Logical channel*. A channel over which an X.25 call can be made on the DCE-DTE link. There are a finite number of LCs on an X.25 line.

LCN *Logical channel number*. The number of an X.25 logical channel.

LCP *Link Control Protocol*. Part of the Point-to-Point Protocol that establishes and configures a link between the two stations at each end of a point-to-point link.

LED *Light Emitting Diode*. A luminous indicator.

Lempel-Ziv A mathematical algorithm used for compressing data.

LLC *Logical Link Control*. The upper portion of the data link layer as defined in IEEE 802.2. The LLC sublayer presents a uniform interface to the user of the data link service, usually the network layer. Beneath the LLC sublayer is the MAC sublayer.

LMI *Local Management Interface*. A term used with Frame Relay networks to describe the dialogue between a station (DTE) and the Frame Relay network

used for management functions. The LMI is carried over a separate DLC from network data.

local interface A default logical interface for all locally generated IP packets.

Logging The process of storing information about events that occurred on the firewall or network.

LOGIN A Netware utility that enables a network station to identify itself to a Novell® file server and gain authorisation to use services provided by the server.

loopback A state in which data transmitted is also received. Normally it is used to test data links by applying a loopback at various points and verifying successful reception of the data transmitted.

LPD *Line Printer Daemon*. A UNIX printer server application that manages remote print jobs. It uses a TCP/IP-based protocol.

M

MAC *Media Access Control*. The lower portion of the data link layer. The MAC differs for various physical media. See "LLC" on page 19.

MAC address The hardware address of a device connected to a shared media. For example, the MAC address of a PC on an Ethernet is its Ethernet address.

MAN *Metropolitan Area Network*. Any of several new physical network technologies that operate at high speeds (typically 100 Mbits per second or more) over metropolitan areas. See "LAN" on page 19 and "WAN" on page 33.

management information base See "MIB" on page 20.

mask A bit pattern used to "mask out" portions of data.

MD5 *Message Digest algorithm 5*. A method of producing a hash, or fingerprint, of a block of data. MD5 is defined in RFC1321.

Member port A switch port that has received a listener join for a particular multicast group.

metric A concept used to describe the cost of a route across a network, the distance to the destination at the remote end of the route, or the capacity of the route.

MIB *Management Information Base*. The set of parameters an SNMP management station can query or set in the SNMP agent of a network device (e.g., router). Standard MIBs have been defined, and vendors can develop private MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. See "SNMP" on page 28.

MIOX *Multiprotocol Interconnect over X.25*. An encoding scheme designed for carrying IP and other protocols over X.25 virtual circuits. See RFC 1356.

mirror ports A port configured to receive (for monitoring) the traffic travelling to and from another port. Mirrored ports are usually used to capture data for viewing on a protocol analyser.

MLD *Multicast Listener Discovery*. A protocol used by IPv6 to manage multicast group membership. See "Querier" on page 26.

MMJ *Modified Modular Jack*. A six-position modular connector similar to that used for voice communication. It is commonly used in DEC environments for asynchronous (RS-232) interfaces.

modem *Modulator/demodulator*. A device that takes digital data from a computer and encodes it in analog form for transmission over a phone line. See "NTU" on page 23.

modulus The number of unique values available for use as sequence numbers in X.25 packets. For example, if an X.25 packet has a 1 byte control field with 3 bits for each sequence number, the valid range for sequence numbers is 23-1, or 0 to 7, and the modulus is 8.

MOSPF *Multicast Open Shortest Path First*. A multicast routing protocol.

MTU *Maximum Transmission Unit*. The largest possible unit of data that can be sent on a given physical medium. For local area networks (e.g. Ethernet), the MTU is determined by the network hardware. For wide area networks using serial lines, the MTU is determined by software. The MTU of Ethernet is 1500 bytes. See "fragmentation" on page 14.

multi-homed gateway A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a multi homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

multicast A special form of broadcast where copies of the packet are delivered to only a subset of all possible destinations. See "broadcast" on page 7, "directed broadcast" on page 10, and "unicast" on page 32.

Multicast Listener Discovery See "MLD" on page 21.

multidrop A method of communication where more than two devices may be simultaneously connected to one serial link.

N

NAK *Negative acknowledgement*. A response sent to indicate unsuccessful reception of information. Usually, a NAK triggers retransmission of the lost data. See "ACK" on page 1.

name resolution The process of mapping a name into the corresponding address. See "DNS" on page 11.

NAT See "network address translation (NAT)" on page 22.

NBMA *Non-broadcast Multi-access.* A network topology with multiple access points, such as X.25 or Frame Relay, that does not support broadcasting, or in which broadcasting is not feasible.

NCP (Netware) *Network Control Protocol*. A Netware protocol.

NCP *Network Control Protocol*. A protocol forming part of the Point-to-Point Protocol, used to establish and configure different network layer protocols

running over point-to-point links. Each network layer protocol (e.g. IP, IPX, DECnet) has its own associated NCP.

network A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs, MANs or WANs.

network address The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See "IP address" on page 17.

network address (Netware) A unique number that identifies a particular network. See "MAC address" on page 20, and "station address (Netware)" on page 29.

network address translation (NAT) A system of economising on IP addresses. NAT enables a private network domain to use a pool of non-unique IP addresses for internal sessions whilst also assigning a smaller pool of unique IP addresses for external sessions. When a device requires an external session, the router maps the local device's IP address with one from the external pool. The router then exchanges these addresses (in the IP header) each time the data moves between internal and external networks.

network number See "network address" on page 22.

network station (Netware) Any device connected to a network by means of a network interface card (e.g. an Ethernet card) and a communication medium. Examples include PCs, bridges, routers and printers.

network-level firewall A firewall in which traffic is examined at the network protocol packet level.

Netware A family of networking operating systems from Novell®.

NETx.EXE (Netware) A Netware program which runs on a PC, in conjunction with the ODI stack, to provide communication between the PC and the Novell network. See "ODI (Netware)" on page 23, and See "VLM (Netware)" on page 32..

NIC *Network Information Center*. A group at SRI International, Menlo Park, CA, responsible for providing users with information about TCP/IP and the connected Internet. The machine named NIC.DDN.MIL is an online archive of RFCs and other documents related to TCP/IP.

NLM (Netware) *Netware Loadable Module*. An executable program that can be loaded and unload from a Novell® file server's memory while the server is operating. Some NLMs are supplied with the Novell® operating system; others are supplied by third party developers. An NLM typically provides services to the operating system and/or users, such as disk drivers, LAN drivers, management utilities, protocol stacks and server applications.

NLPID *Network Layer Protocol Identifier*. A flag in a frame sent over a Frame Relay network that indicates the type of network layer PDU carried in the data portion of the frame.

node An addressable device attached to a computer network. See "host" on page 16, and "router" on page 27.

non-volatile storage See "NVS" on page 23.

Novell®, Inc. A vendor of internetworking operating systems and hardware, such as Novell® Netware.

NSAP Network Service Access Point.

NTU *Network Terminating Unit*. A device that takes digital data from a computer and encodes it for transmission over digital telecommunication lines. It is the equivalent of a modem for modern digital links. See "modem" on page 21.

NVS *Non-Volatile Storage*. Static RAM that has its contents preserved through router power cycles through the use of a battery that maintains power to the RAM. Also referred to as non-volatile memory or battery-backed RAM (BBR) on the router.

O

octet An octet is 8 bits. This term is used in networking, rather than byte, because some systems have bytes that are not 8 bits long.

ODI (Netware) *Open Data-Link Interface*. A standard interface that allows multiple transport protocols (such as IPX and TCP/IP) to share the same network interface hardware or media-specific device driver, to access a Novell network. On a network station, the interface consists of several modules — LSL.COM, a media-specific driver (MLID) and IPXODI.COM. ODI supersedes IPX.COM which only allows a single transport protocol (IPX) to use the network interface hardware. ODI is used by both NETX and VLMs.

OSI *Open Systems Interconnection*. A suite of protocols, specifically ISO standards, to be the international standard computer network architecture. See "ISO" on page 18.

OSPF *Open Shortest Path First*. A standard IGP for the Internet. It is a link state, as opposed to distance vector, routing protocol. See "IGP" on page 16.

P

packet A self-contained unit of data prepared for network transmission. A packet contains information such as a destination address or a channel identifier to enable it to be routed through a network. Note that the term tends to be used for transmission at the *network* layer rather than the data link layer, where the term *frame* is more commonly used. Common packet based protocols are IP and X.25.

packet switching A communications paradigm in which packets (messages) are individually routed between hosts, with no previously established communication path.

PAD *Packet Assembler Disassembler*. A term used with X.25 networks to refer to a terminal multiplexer device that forms a connection between terminals and hosts across an X.25 network. A PAD accepts characters from a terminal and

sends them across an X.25 network in packets, and it accepts packets from an X.25 network, extracts the characters, and sends them to a terminal.

PADI PPPoE Active Discovery Initiation.

PADO PPPoE Active Discovery Offer.

PADR PPPoE Active Discovery Request.

PAPS Active Discovery Session-confirmation.

parity A method of checking the integrity of characters transmitted serially. It does this by defining an extra bit whose value is set to ensure either an even (even parity) or odd (odd parity) number of '1' bits in the character.

patch A piece of computer code used to correct or enhance an existing piece of code. In the router, patches are applied by "overlying" them on existing code in RAM. The patches are loaded into the router using a process called *downline loading*.

PATH message The message sent from the source of the traffic flow to the destination(s), containing the session parameters, sender parameters and sender TSpec.

PDU *Protocol Data Unit*. A packet containing a protocol-specific header followed by user data.

perimeter-based security The technique of securing a network by controlling access to all entry and exit points of the network.

permanent assignment A term used with the router to refer to a permanent link established between two asynchronous ports on a router or routers connected via TCP/IP. The link is effectively a pipe through the network through which data is passed.

PIM-DM *Protocol Independent Multicast—Dense Mode.* A multicast routing protocol.

PIM-SM *Protocol Independent Multicast—Sparse Mode.* A multicast routing protocol.

ping *Packet InterNet Groper*. A program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. The term is used as a verb: "Ping host X to see if it is up!".

Point-to-Point Protocol See "PPP" on page 24.

PPP *Point-to-Point Protocol*. PPP provides a method for transmitting packets over serial point-to-point links.

PPPoE Point to Point Protocol over Ethernet.

policy Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

port An entity, usually configurable, that provides a logical or physical connection to and from a device such as a router or switch. Physical ports are usually associated with a physical interface. Typical examples of physical ports

are Ethernet *Eth* or *switch* ports. Virtual ports are often used to define connections to the wide area network. A typical example is a frame relay network where each virtual port is mapped to a frame relay virtual circuit DLCI. See "interface" on page 17.

PRI *Primary Rate Interface*. In the router, the name of the software module, and the name assigned to logical interfaces, that provide Primary Rate Access to an ISDN service. See "BRI" on page 6, "ISDN" on page 18, and "Primary Rate Access" on page 25.

PRM *Performance Report Message*. A periodic message sent in one direction reporting on the performance of the T1 link in the opposite direction.

Primary Rate Access A mode of access to an ISDN service that provides 30 64 kbit/s B channels for data and one 64 kbit/s D channel for link control and management. The access point is typically at a customer's premises. See "Basic Rate Access" on page 5, "ISDN" on page 18, "PRI" on page 25.

privacy The property of ensuring that traffic on a secured connection may not be read by unauthorised persons. Privacy is normally ensured using cryptographic techniques (encryption) such as DES and Triple-DES.

privilege A term used in computing to refer the access rights or levels of authorisation given to users of computer systems. The higher the privilege, the more "powerful" the commands, and users can affect the operation of the system or the activities of other users. The router has two levels of privilege: *Manager* and *User*. Those with *User* privilege (most users) have access to a subset of the commands available to those with *Manager* level.

prompt A text string displayed on a terminal by a computer to indicate that it is ready to receive the next command from the user.

protocol A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (such as the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (such as the way in which two programs transfer a file across the Internet).

protocol stack A layered set of protocols that work together to provide a set of network functions. See "layer" on page 19, and "protocol" on page 25.

proxy A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether the user is permitted to use the proxy, performs any additional authentication, and then completes a connection on behalf of the user to a remote destination.

proxy ARP The technique in which one machine, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP allows a site to use a single IP address with two physical networks. Subnetting would normally be a better solution.

PSN *Packet Switch Node*. A dedicated computer whose purpose is to accept, route and forward packets in a packet switched network. See "packet switching" on page 23.

PVC *Permanent Virtual Circuit*. An X.25 virtual circuit that is permanently established.

Q

QOS *Quality of Service*. A measure of the quality of a transmission system, in terms of reliability and availability.

QOS Policy A collection of user-defined traffic classes and default traffic classes. See "traffic class" on page 31, and "default traffic class" on page 10.

queue A list of packets awaiting processing.

Querier In Multicast Listener Discovery (MLD), the router that sends Query messages to hosts, to determine which IPv6 multicast groups the hosts are interested in.

R

RAI*Remote alarm indication*. A signal transmitted in the outgoing direction on an E1 or T1 line when a terminal determines that it has lost the incoming signal. RAI is also called yellow alarm in USA T1 parlance.

RARP *Reverse Address Resolution Protocol*. An IP protocol which provides the reverse function of ARP. RARP maps a hardware (MAC) address to an internet address. It is used primarily by diskless nodes when they boot to find their internet address. See "ARP" on page 3, "IP address" on page 17, and "MAC address" on page 20.

RBS *Robbed Bit Signalling*. A mechanism used on T1 lines for carrying call signalling information within the channel to which it refers by robbing bits from the channel.

reassembly The process in which a previously fragmented packet is reassembled before being passed to the transport layer. See "fragmentation" on page 14.

RED *Random Early Detection.* A method of discarding packets before a traffic class or flow group reaches its bandwidth limit.

repeater A device which propagates electrical signals from one cable to another without making routing decisions or providing packet filtering. See "bridge" on page 6, and "router" on page 27.

RESV message The message sent from the destination of the traffic flow to the source, containing the session parameters and reservation parameters for making the reservation.

RFC *Request For Comments*. The document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards but all Internet standards are written as RFCs.

RIP *Routing Information Protocol*. A distance vector, as opposed to link state, routing protocol. It is an Internet standard interior gateway protocol (IGP).

RIP (Netware) *Routing Information Protocol*. A Netware protocol for exchanging routing information between routers. It is a distance vector protocol which uses a hop count metric. It is derived from Xerox Corporation's XNS protocol.

RJ45 An 8-pin modular connector used on the router to provide asynchronous serial ports, ISDN Primary and Basic rate interfaces and Ethernet 10BASET interfaces. It is compatible with building wiring schemes such as PDS. See "MMJ" on page 21.

rlogin *Remote login*. A service offered by Berkeley 4BSD UNIX systems which allows users of one machine to log into other UNIX systems (for which they are authorized) and interact as if their terminals were connected directly. It is similar to the TCP/IP Telnet service.

route The path that network traffic takes from the source to the destination. It may include many gateways, routers, hosts, and physical networks.

route table A table listing information about routes to other hosts or networks, such as the remote network or host address, the interface down which the route exists, the distance to the remote address, and the cost of sending data over the route.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics." See "gateway" on page 15, "bridge" on page 6, and "repeater" on page 26.

RS-232 An EIA (Electronics Industry Association) standard that specifies the electrical characteristics of low speed interconnections between terminals and computers or between two computers.

RS-530 An EIA (*Electronics Industry Association*) standard that specifies the use of DB25 connectors to provide a combination of balanced (similar to X.21) and unbalanced signals. It is similar to V.35 but uses sensible connectors and handles 2.048 Mbps.

RSA A widely used public key encryption method. RSA public keying is central to the authentication and key exchange functions in the SSH protocol.

RSO *Remote Security Officer*. A user, defined in terms of an IP address, authorised to connect to an AR router using Telnet and login to a user account with Security Officer privilege. A user who is not an RSO can only login to a user account with Security Officer privilege from a terminal directly connected to an asynchronous port on the router.

RSVP *ReSerVation Protocol.* An IETF protocol for making resource reservations on an internet.

RSVP proxy agent A device which sets up and tears down resource reservations on behalf of devices which do not support RSVP.

S

SA *Security Association*. A method of identifying local and remote groups of hosts so that all communication between the groups may be encapsulated, encrypted and/or authenticated by some means.

SAP *Service Access Point*. The point at which the services of an network layer are made available to the next higher layer.

SAP (Netware) *Service Advertisement Protocol*. A Netware protocol used to propagate information about services (such as file server, printer server, and LAN spooler) among file servers and routers. It is also used by workstations to get the address of a server.

screened host A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

screened subnet A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.

screening router A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.

serial A method of transmission in which each bit of information is sent sequentially on a single channel rather than simultaneously as in parallel transmission.

server A network device that provides services to client stations. Examples include file servers and print servers.

service A term used with the router to refer to a connection to another port on (another) router, used to access dialup modems, hosts that do not support TCP/IP and other asynchronous devices.

service table A table listing information about services available on the network, such as the service's address.

session stealing See "IP splicing/hijacking" on page 18.

SF *Superframe format*. A T1 multiframe format that has 12 basic frames in the multiframe does not support multiframe CRC or a Data Link, also known as D4 framing.

SHA-1 *Secure Hash Algorithm 1*. A hash algorithm defined and endorsed by the US Government as a more secure alternative to MD5. It holds US Federal Information Processing Standard (FIPS) status and is described in US federal document FIPS 180-1.

SMP *Simple Management Protocol*. A new management protocol that incorporates the functions of SNMP with authentication, encryption and blockmode access. See "SNMP" on page 28 and "MIB" on page 20.

SNMP *Simple Network Management Protocol*. The Internet standard protocol developed to manage nodes on an IP network. See "MIB" on page 20.

social engineering An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user to gain illicit access to systems.

socket An entry point to a program. User programs communicate with transport providers such as UDP and TCP by means of sockets. Each user typically has a separate socket.

source quench A congestion control technique in which a machine experiencing congestion sends a message back to the source of the packets causing the congestion requesting that the source stop transmitting.

spoofing Impersonating a host by sending fake traffic claiming to be from its address. Spoofing is used to hijack existing connections and exploit trust relationships between hosts.

SPX *Sequenced Packet eXchange*. A Netware protocol providing connection-mode communications between two network stations. It uses IPX as its network layer carrier and provides guaranteed delivery of packets in order.

SSAP *Source Service Access Point*. The address of the user of a service. See "DSAP" on page 11.

SSH *Secure Shell*. A remote login protocol providing strong authentication through the use of RSA public and private keys, and data security via encryption. SSH also supports the tunnelling of arbitrary IP traffic between peers in a SSH session.

SSO *System Security Officer* The user in charge of the overall administration of a secure router. In particular, the SSO ensures that the key management requirements are fulfilled in a secure manner.

station See "network station (Netware)" on page 22.

station address (Netware) A unique number assigned to each station on a network that defines the station's address within the network. It is often the MAC address of the station's network interface card. A station's address is globally defined by the combination of a network address and a station address. See "MAC address" on page 20, and "network address" on page 22.

stop bits A technique used in asynchronous serial communications in which 1, 1.5 or 2 bits are transmitted after the start bit, a variable number of data bits and optional parity bit are transmitted. It is designed to frame the character.

stream printing A term used with the router to refer to a TCP-based printing service provided by the router, which uses a raw TCP connection between a client computer and the asynchronous port on the router to which the printer is connected.

stub network A stub network only carries packets to and from local hosts. Even if it has paths to more than one other network, it does not carry traffic for other networks. See "backbone" on page 5, "transit network" on page 31.

subnet A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask. See "subnet mask" on page 29, "IP address" on page 17, and "network address" on page 22.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the

Internet address and one or more bits of the local portion. Sometimes called *address mask*.

SVC *Switched Virtual Circuit*. A virtual circuit that is set up on demand.

synchronous Transmission in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronised. This eliminates the need for start-stop elements, as in asynchronous transmission, but requires a flag character to be transmitted when there is no data to transmit. See "asynchronous" on page 4.

Synchronous Tunneling See *"tunneling" on page -31*.

SYSR *System Redundancy*. A way of providing CPU redundancy by using two switch controllers: a Master and a Slave.

T

T1 A wide area digital transmission scheme that carries DS1 formatted data at a nominal rate of 1.544 Mbit/s, predominant in the USA and Japan. For European and NZ standard, see "E1" on page 12.

TA *Terminal Adaptor*. A device enabling the connection of a router without a native ISDN interface to an ISDN circuit.

TCP *Transmission Control Protocol*. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

TCP/IP Protocol Suite *Transmission Control Protocol over Internet Protocol*. This is a common shorthand that refers to the suite of transport and application protocols that runs over IP. See "IP" on page 17, "ICMP" on page 16, "TCP" on page 30, "UDP" on page 32, "FTP" on page 15, "Telnet" on page 30, and "SNMP" on page 28.

Telnet The virtual terminal protocol in the TCP/IP suite of protocols, which allows users of one host to log into a remote host and interact as normal terminal users of that host.

terminal server A device which connects many terminals to a LAN through one network connection. A terminal server can also connect many network users to its asynchronous ports for dial-out capabilities and printer access.

terminator A device placed on a length of coaxial cable to ensure electrical reflections from an un-terminated end are reduced. An Ethernet cable must have exactly two (50Ω) terminators — one at each end of the cable.

TFTP *Trivial File Transfer Protocol*. The TCP/IP standard protocol for file transfer with minimal capability and minimum overhead, based on UDP. It is often used by diskless workstations that keep software in ROM and use it to bootstrap themselves. It is used in the router for downloading patches.

time to live See "TTL" on page 31.

token ring A token ring is a type of LAN with nodes wired into a ring. Each node constantly passes a control message (token) on to the next; whichever

node has the token can send a message. “Token Ring” often refers to the IEEE 802.5 token ring standard, which is the most common type.

topology A network topology shows the computers and the links between them. A network layer must know the current network topology to be able to route packets to their final destination.

TOS *Type Of Service routing*. A routing scheme in which the choice of route depends on the characteristics of the underlying network topology as well as the shortest path to the destination.

traffic class The central part of the QOS solution, providing most of the QOS controls to allow the solution to be deployed. See “QOS” on page 26.

transceiver *Transmitter-receiver*. A device that connects a host interface to a local area network such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions. A transceiver is needed by some router models to connect to the appropriate Ethernet media (e.g. 10BASET, 10BASE2, 10BASE5, 10BASEF). All transceivers have an AUI interface. See “AUI” on page 4.

transit network A transit network passes traffic between networks in addition to carrying traffic for its own hosts. It must have paths to at least two other networks. See “backbone” on page -5 and “stub network” on page -29.

Triple DES An encryption algorithm involving the application of DES three times, using two or three different keys.

trojan horse A software entity that appears to do something normal but which in fact contains an attack program.

trusted router A concept used to refer to routers from which the router will accept routing information.

TSpec *Traffic Specification.* The specification of the characteristics of the traffic, as transmitted by the sender, in a network using RSVP.

TTL *Time To Live*. A technique used in best-effort delivery systems to avoid endlessly looping packets. For example, each IP datagram has a field in the header that indicates how long this packet should be allowed to survive before being discarded. It is primarily used as a hop count. Each time a router processes the packet, it decrements the time-to-live value. When the value reaches zero, the router discards the packet.

tunneling A technique used to transport data whose format is incompatible with the router network. The technique involves wrapping the unroutable protocol around one that is routable and can thus be forwarded across the network. Once it has crossed the router network, the routable protocol is removed and the data transcends the local network in its native form. Note that in secure networks, the original data may have been rendered unroutable because it has been encrypted.

tunneling router A router capable of tunneling data. See “tunneling” on page 31.

Type 1 router In DECnet terminology, a router that routes traffic within a DECnet area. See “area router” on page 3, “DECnet address” on page 10, “Type 2 router” on page 32.

Type 2 router In DECnet terminology, a router that routes traffic between DECnet areas. See "area router" on page 3, "DECnet address" on page 10, "Type 1 router" on page 31.

U

UDP *User Datagram Protocol*. A transport layer protocol in the TCP/IP suite of protocols. Like TCP, UDP uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.

unicast A packet broadcast to a single host attached to the network. See "broadcast" on page 7, "directed broadcast" on page 10, "multicast" on page 21.

URL *Uniform Resource Locator*. A standard format for specifying the name, type and location of documents and resources on an internet. The syntax is `type://host.domain[:port]/path/filename`, where `type` specifies the type of document or resource (for example, `http` is a file on a WWW server; `file` is a file on an anonymous FTP server; `Telnet` is a connection to a Telnet-based service). See "WWW" on page 33.

V

Virtual (LAN) Identifier. A twelve-bit identifier inserted into the *Tag Control Information field* of an IEEE802.3 MAC frame that specifies the VLAN number associated with the frame. Note that the *Tag Control Information field* forms part of an optional 4 octet *QTag Prefix* that may be inserted into the frame.

Virtual circuit A circuit in which connectivity between devices is established by configurable mappings rather than by a fixed physical path or connection. Virtual circuits often comprise paths created through switched networks where each path is mapped to a logical circuit, channel, or number. This technique enables many virtual circuits to share a single physical communications channel or interface. Typical examples are frame relay channels and X.25 switched virtual circuits.

virtual network perimeter A network that appears to be a single protected network behind firewalls, but which actually encompasses encrypted virtual links over untrusted networks.

virus A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

VLAN *Virtual Local Area Network*. A virtual (or logical) LAN is a local area network entity whose workstation membership is created by configuration rather than by physical connection. Plans enable workstations to be mapped on some other basis than geographic location, for example, by department or type of user.

VLAN tagging See "VLAN" on page 32.

VLM (Netware) A Netware program which runs on a PC, in conjunction with the ODI stack, to provide communication between the PC and the Novell network. VLMs have to some extent superseded NETX. They can optionally be used to access any version of Netware, but must be used for full access to

Netware 4.0. See "ODI (Netware)" on page 23, "NETx.EXE (Netware)" on page 22.

VPN *Virtual Private Network*. A private network built over an insecure public network, such as the Internet, in which communication between peer sites is encrypted to prevent unauthorised monitoring of session data and unauthorised access into the VPN from the public network.

VR *Virtual Router*. Two or more physical routers combined into a logical grouping, which operate together to provide a single logical gateway for hosts on the LAN.

VRID *Virtual Router Identifier*. A unique number that identifies a Virtual Router.

VT-100 A popular model of DEC terminal. Many third-party vendors make VT-100 compatible terminals. The term VT-100 is also used to describe the characteristics of terminals that may be connected to a device.

W

WAN *Wide Area Network*. Any physical network technology that spans large geographic distances. WANs usually operate a slower speeds than LANs or MANs. See "MAN" on page 20, "WAN" on page 33.

well-known port Any of a set of protocol port numbers preassigned for specific uses by transport level protocols, such as TCP and UDP. Examples of well-known port numbers include Telnet (23) and LPD (515).

window In general, a term used to describe a type of flow control mechanism in a network protocol. In an X.25 network, it is the number of unacknowledged packets that may be sent by a DTE, and is less than the modulus for the network. In a TCP/IP network, it is the number of octets that a station is prepared to receive.

wiretapping A generic name given to methods of electronic eavesdropping on traffic as it traverses a network. Wiretapping can compromise reusable passwords and reveal other sensitive information from a login session.

WWW *World Wide Web*. A hypertext-based, distributed information system based on a client-server architecture. Web browsers (client applications) request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs (Uniform Resource Locators). See "URL" on page 32.

X

X.21 The CCITT standard that defines the electrical characteristics of a compact, high speed (10 Mbps) interface between a DTE (Data terminal Equipment) and a DCE (Data Communication Equipment) on public data networks.

X.25 The CCITT standard protocol for transport level network service. It provides a reliable stream transmission service.

XNS *Xerox Network Standard*. The term used collectively to refer to the suite of internet protocols developed by researchers at Xerox Corporation. It is similar in philosophy to the Internet protocol suite but uses different packet formats and terminology.

XON/XOFF A method of flow control using the XON and XOFF characters.