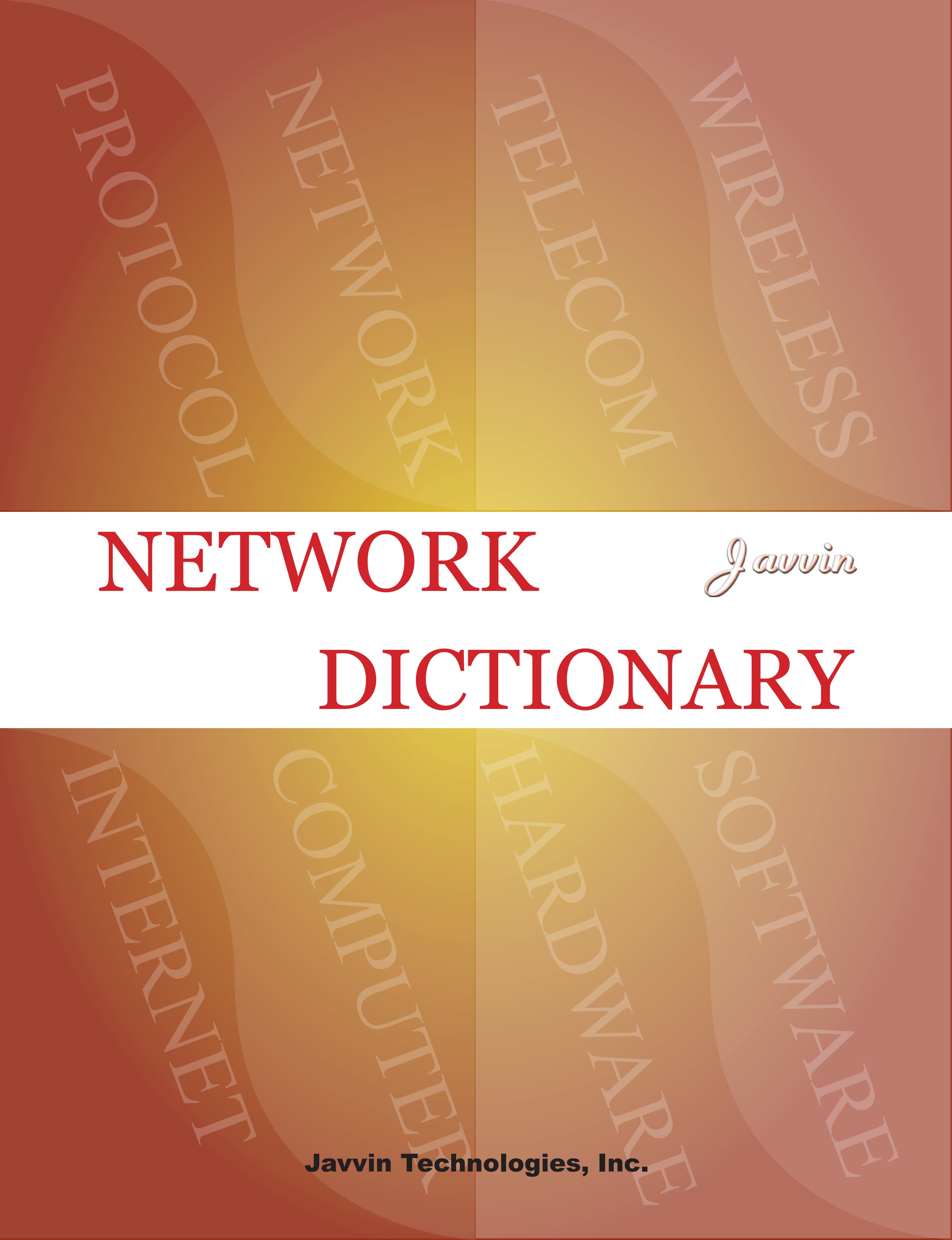


NETWORK DICTIONARY

Javvin

Javvin Technologies, Inc.

Table of Contents

# #

.NET Passport *Security*

.NET Passport, now called Windows Live ID, is a system developed by Microsoft Corporation for managing online identity. It is a "unified-login" service that allows users to log in to many websites using one account. It was originally positioned as a single sign-on service for all web commerce.

/etc/passwd *Security*

/etc/passwd is a file used in most UNIX and Linux systems for storing user information such as passwords.

µ-law *Telecom*

See Mu-law.

µTorrent *Software*

µTorrent is a Bittorrent client for Microsoft Windows suporting a very small footprint. It is designed to use as little cpu, memory and space as possible while offering all the functionality expected from advanced clients.

0-day *Security*

"Zero Day" or 0-day, in the security context, indicates that someone takes advantage of a security vulnerability on the same day when the vulnerability becomes generally known.

0G *Wireless*

0G refers to pre-cellular mobile telephony technology. These mobile telephones were usually mounted in cars or trucks. Typically, the transceiver (transmitter-receiver) is mounted in the vehicle trunk and attached to the "head" (dial, display, and handset) mounted near the driver seat.

10 Gigabit Ethernet Alliance *Networking, Organization*

The 10GEA (10 Gigabit Ethernet Alliance) was an independent organization which aimed to further 10 Gigabit Ethernet development and market acceptance. Founded in February, 2000, by a consortium of companies, the organization provided IEEE with technology demonstrations and specifications.

1000Base-CX *Networking, Protocol*

See 1000BaseCX.
IEEE Specification: IEEE 802.3z

1000BaseCX *Networking, Protocol*

1000BaseCX, also known as 1000Base-CX, is a physical layer specification for Gigabit Ethernet transmission over a special balanced 150 ohm cable shorter than 25m. This cable is a type of shielded cable. In order to minimize safety and interference concerns caused by voltage difference, both transmitters and receivers will share a common ground. The return loss for each connector is limited to 20db to minimize transmission distortions. The connector type for 1000Base-CX will be a DB-9 connector or HSSDC.
IEEE Specification: IEEE 802.3z

1000Base-F *Networking, Protocol*

See 1000BaseF.
IEEE Specification: IEEE 802.3z

1000BaseF *Networking, Protocol*

1000BaseF, also known as 1000Base-F, is a physical layer baseband specification for Ethernet communications over optical fibers. 1000Base-F uses 8B/10B ANSI X3T11 Fibre Channel FC-1 frame encoding, serializer/deserializer (SERDES) and NRZ on the fiber, clocked at 1250 Mbaud. 1000BaseF can support a fiber cable length of 500m full duplex on multimode fiber, and of 2-3km full duplex on single mode fiber.
IEEE Specification: IEEE 802.3z

1000Base-LH *Networking, Protocol*

See 1000BaseLH.
IEEE Specification: IEEE 802.3z

1000BaseLH *Networking, Protocol*

1000BaseLH, also known as 1000Base-LH, is a physical layer specification for Gigabit Ethernet over fiber optic cabling as defined in IEEE 802.3z. LH stands for long haul, and 1000Base-LH uses long wavelength laser (1310nm) over multimode and single-mode fiber. 1000BaseLH can support a maximum distance of 550m for multimode fiber, and of 10km for single mode fiber.
IEEE Specification: IEEE 802.3z

1000BaseLX *Networking, Protocol*

1000BaseLX, also known as 1000Base-LX, is a physical layer specification for Gigabit Ethernet over fiber optic cabling as defined in IEEE 802.3z. LX stands for long wavelength, and 1000Base-LX uses long wavelength laser (1310nm) over multimode and single-mode fiber as opposed to 1000Base-SX, which uses short wavelength laser over multimode fiber. The maximum distance of fiber is 550m for multimode and 5km for single mode.
IEEE Specification: IEEE 802.3z

1000Base-LX *Networking, Protocol*

See 1000BaseLX.
IEEE Specification: IEEE 802.3z

1000Base-SX *Networking, Protocol*

See 1000BaseSX.
IEEE Specification: IEEE 802.3z

1000BaseSX *Networking, Protocol*

1000BaseSX, also known as 1000Base-SX, is a physical layer specification for Gigabit Ethernet over fiber optic cabling as defined in IEEE 802.3z. SX stands for short wavelength, and 1000Base-SX uses short wavelength laser (850nm) over multimode fiber as opposed to 1000Base-LX, which uses long wavelength laser over both multimode and single-mode fiber. The

A

A & B Bit *Telecom*

A & B Bit is used in digital environments to convey signaling information. A bit equal to one generally corresponds to loop current flowing in an analog environment; A bit value of zero corresponds to no loop Current, i.e., to no connection. Other signals are made by changing bit values, for example, a flash-hook is sent by briefly setting the A bit to zero.

A Links *Telecom*

A Links, also known as SS7 access links, connect an end office or signal point to a mated pair of signal transfer points. They may also connect signal transfer points and signal control points at the regional level with the A-links assigned in a quad arrangement.

A.b *Networking*

Hardware See ACCESS.bus.

A&B Bit Signaling *Telecom*

A&B Bit Signaling, also called 24th channel signaling, is a procedure used in T1 transmission facilities in which each of the 24 T1 subchannels devotes 1 bit of every sixth frame to the carrying of supervisory signaling information. On T1 lines that use Extended SuperFrame (ESF) framing, the signaling bits are robbed from the 6th, 12th, 18th, and 24th frame, resulting in "ABCD" signaling bits.

A/D Converter *Hardware*

See Analog/Digital Converter.

A3 Algorithm *Security*

A3 Algorithm is used to encrypt Global System for Mobile Communications (GSM) cellular communications. In practice, A3 and A8 algorithms are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4). Development of A3 and A8 algorithms is considered a matter for individual GSM network operators although sample implementations are available.

A3/A8 *Security*

A3/A8 refers to two algorithms, A3 and A8, that are used to encrypt Global System for Mobile Communications (GSM) cellular communications. Since A3 and A8 algorithms are generally implemented together, they are often known as A3/A8. An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4). Development of A3 and A8 algorithms is considered a matter for individual GSM network operators although sample implementations are available.

A5 Algorithm *Security*

A5 Algorithm is used to encrypt Global System for Mobile Communications (GSM) cellular communications. An A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem (BSS).

A8 Algorithm *Security*

A8 Algorithm is used to encrypt Global System for Mobile Communications (GSM) cellular communications. In practice, A3 and A8 algorithms are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic, as defined in 3GPP TS 43.020 (03.20 before Rel-4). Development of A3 and A8 algorithms is considered a matter for individual GSM network operators although model implementations are available.

AAA *Security*

See Access control, Authorization, and Auditing, or Authentication, Authorization, and Accounting.

AAA Server *Security*

An AAA server is a server with AAA software or applications to process user requests for access to computer/network resources and to provide authentication, authorization, and accounting (AAA) functions.

AAL *Networking*

See ATM Adaptation Layer.

AAL0 *Networking*

See ATM Adaptation Layer Type 0.

AAL1 *Networking*

See ATM Adaptation Layer Type 1.

AAL2 *Networking*

See ATM Adaptation Layer Type 2.

AAL3/4 *Networking*

See ATM Adaptation Layer Type 3/4.

AAL5 *Networking*

See ATM Adaptation Layer Type 5.

AARNet *Networking*

See Australian Academic and Research Network.

AARON *Software*

AARON is a screensaver program written by artist Harold Cohen who created the original artistic images. AARON utilizes artificial intelligence to continuously create original paintings on PCs.

AARP *Networking*

B

B Channel *Networking, Telecom*
See Bearer Channel.

B2B *Networking*
See Business-to-Business.

B2BUA *Networking*
See Back-to-Back User Agent.

B2C *Networking*
See Business-to-Consumer.

B2evolution *Software*
B2evolution is a multi-lingual, multi-user, multi-blog publishing system written in PHP and backed by a MySQL database. It is distributed under the GNU General Public License and is available without charge.

B3ZS *Telecom*
See Bipolar 3 Zero Substitution.

B6ZS *Telecom*
See Bipolar 6 Zero Substitution.

B8ZS *Telecom*
See Bipolar 8 Zero Substitution.

Babble *Telecom*
Babble refers to noise or confusion, which is the aggregate cross-talk from interfering channels.

Back End *Networking*
Back End, in the context of a computer system, refers to a node or software program that provides services to a front end. The front end typically interfaces with users directly while the back end may communicate with other systems such as databases and other systems.

Back Orifice *Security*
Back Orifice is a rootkit program designed for the purpose of exposing the security deficiencies of Microsoft's Windows operating systems. The program's name is inspired by the name of Microsoft's BackOffice product.

Back Orifice 2000 *Security*
Back Orifice 2000 (BO2K) is an open source remote administration tool for Windows systems. Back Orifice is a rootkit program designed for the purpose of exposing the security deficiencies of Microsoft's Windows operating systems. It comes with a client and a server. The server is lightweight and inobtrusive. A dynamic plugin architechture allows for easy system extensions.

Back Pressure *Networking*
Back Pressure, in the context of networking, refers to the propagation of network congestion information upstream through an internetwork.

Backbone *Networking*
Backbone is the part of a network that acts as the primary path for all network traffic, which requires very high bandwidth. A backbone network of a service provider typically connects many enterprise subnetworks and networks of smaller service providers. An enterprise backbone network typically connects many LANs and data centers.

Backbone Cabling *Telecom*
Backbone Cabling refers to a portion of premises telecommunications cabling that provides connections between telecommunications closets, equipment rooms and entrance facilities. It consists of the transmission media (optical fiber cable), main and intermediate cross-connects, and terminations for the horizontal cross-connect, equipment rooms, and entrance facilities. Backbone cabling, sometimes called backbone wiring, can further be classified as inter-building backbone (cabling between buildings), or intra-building backbone (cabling within a building).

Backchannel *Networking*
Backchannel refers to the practice of using networked computers to maintain a real-time online conversation while other live spoken sessions are going on. For example, backchannel is popular in conferences and classrooms where audiance and students can use Wi-Fi connections and laptop computers to do online chat during class.

Back-channel *Telecom*
Back-channel is, in an asymmetric telecommunications system, typically a low-speed or less-than-optimal transmission channel opposite to the main channel's direction. An example of this is in ADSL where "A" stands for "asymmetric", and the channel from the subscriber to the supplier is slower and may be of less capacity than the channel from the supplier to the subscriber.

Backdoor *Security*
Backdoor, also called a trapdoor, is an undocumented way of gaining access to a program, online service or an entire computer system. The backdoor, usually written by the author of the software for some special purpose, is a potential security risk for whoever known or found its way to use this backdoor to gain an unauthorized access.

Background Noise *Telecom*
Background Noise is the random signals that can be attributed to the unpredictable movement of free elections in a communication channel.

Backhaul *Wireless*
In wireless technology, backhaul refers to transporting voice and data traffic from a cell site to the switch.

Back-Haul *Telecom, Networking*
Back-Haul is a communications path which takes traffic farther

C

C Programming Language *Software*

The C programming language (often, just “C”) is a general-purpose, procedural, imperative computer programming language developed in the early 1970s by Dennis Ritchie for use on the Unix operating system. The first major program written in C was the UNIX operating system. It has since spread to many other operating systems. Although originally designed as a systems programming language, C has proved to be a powerful and flexible language that can be used for a variety of applications, from business programs to engineering. C is a particularly popular language for personal computer programmers because it is relatively small -- it requires less memory than other languages.

C# *Software*

C# is an object-oriented programming language developed by Microsoft as part of their .NET initiative, and later approved as a standard by ECMA and ISO. C# has a procedural, object-oriented syntax based on C++ that includes aspects of several other programming languages (most notably Delphi, Visual Basic, and Java) with a particular emphasis on simplification (fewer symbolic requirements than C++, fewer decorative requirements than Java).

C/I *Wireless*

See Carrier-to-Interference ratio.

C/N *Wireless*

See Carrier-to-Noise ratio.

C++ *Software*

C++, originally named “C with Classes, is a high-level programming language developed by Bjarne Stroustrup at Bell Labs. C++ adds object-oriented features to its predecessor, C. C++ is a statically-typed free-form multi-paradigm language supporting procedural programming, data abstraction, object-oriented programming, and generic programming. C++ is one of the most popular programming languages. The C++ programming language standard was ratified in 1998 as ISO/IEC 14882:1998, and the current version of which is the 2003 version, ISO/IEC 14882:2003. A new version of the standard (known informally as C++0x) is being developed.

C7 *Telecom*

See Common Channel Signaling 7.

CA *Security*

See Certification Authority.

CA Certificate *Security*

CA certificates are digital certificates issued by one certification authority (CA) for another CA. CA certificate identifies the certification authority (CA) that issues server and client authentication certificates to the servers and clients that request these certificates. Because it contains a public key used in digital signatures, it is also referred to as a signature certificate. If the CA is a root authority, the CA certificate may be referred to as a root certificate.

CA Hierarchy *Security*

CA hierarchy, also called a hierarchy of trust, is a hierarchical collection of certificate authorities (CAs) bound together by trust relationships.

CA-ACF2 *Security*

See Computer Associates Access Control Facility.

CAAD *Software*

See Computer Aided Architectural Design.

Cable *Networking, Hardware*

Cable is the physical transmission medium of a group of metallic conductors or optical fibers that are bound together and wrapped in a protective cover, and insulation between individual conductors/fibers and for the entire group.

Cable Modem *Hardware*

Cable modem provides access of computers to network over cable TV lines. Most cable modems supply a 10 Mbps Ethernet connection for the home LAN. Cable modem achieve higher access speed to the World Wide Web than phone lines using dial up modem or even ADSL modem. The actual performance of a cable modem Internet connection can vary depending on the utilization of the shared cable line in that neighborhood, but typical data rates range from 300 Kbps to 1500 Kbps.

Cable Modem Termination System *Networking, Hardware*

Cable Modem Termination System (CMTS) is a specially designed router or a bridge for data networking. CMTS is located at the headend of service providers and used to aggregate traffic from multiple Cable Modems and then communicate with the backbone network.

Cable Range *Networking*

Cable Range refers to the range of network numbers that is valid for use by nodes on an extended AppleTalk network. The cable range value can be a single network number or a contiguous sequence of several network numbers. Node addresses are assigned based on the cable range value.

Cable Router *Networking, Hardware*

Cable Router is a router optimized for data-over-CATV hybrid fiber-coaxial (HFC) applications. Cable router is often combined with cable modern used as an access device at home or Small Office Home Office (SOHO) for the Internet access via cable operators.

Cable Television *Networking*

D

D Channel *Telecom*

D Channel, an ISDN term, refers to the channel that carries control and signaling information. (The “D” stands for “delta” channel.) The B-channel (“B” for “bearer”) carries the main data. The D-channel carries control and signaling information.

D Type Channel Bank *Telecom*

D type Channel Bank refers to the terms used in T1 technology. Channel Bank defines the type of formatting that is required for transmission on T1 trunk. The purpose of a Channel Bank in the telephone company is to form the foundation of multiplexing and demultiplexing the 24 voice channels (DS0). D type Channel Bank is one of the type of Channel Bank which is used for digital signals. There are five kinds of Channel Banks that are used in the System: D1, D2, D3, D4, and DCT (Digital Carrier Trunk).

D/A Converter *Hardware*

See Digital-to-Analog converter.

DACL *Security*

See Discretionary Access Control List.

DACS *Telecom*

See Digital Access and Cross-Connect System.

Daemon *Software*

In Unix and other computer multitasking operating systems, a daemon is a computer program that runs in the background, rather than under the direct control of a user; they are usually instantiated as processes. The Daemon program, often started at the time the system boots and runs continuously without intervention from any of the users on the system, forwards the requests to other programs (or processes) as appropriate. Typically daemons have names that end with the letter “d”; for example, syslogd is the daemon which handles the system log. Windows OS refers to daemons as System Agents and services.

Daisy Wheel Printer *Hardware*

A daisy wheel printer is a type of computer printer that produces high-quality type, and is often referred to as a letter-quality printer (this in contrast to high-quality dot-matrix printers, capable of near-letter-quality (NLQ) output). To print a character, the printer rotates the disk until the desired letter is facing the paper. Then a hammer strikes the disk, forcing the character to hit an ink ribbon, leaving an impression of the character on the paper. You can change the daisy wheel to print different fonts. There were also, and still are daisy wheel typewriters, based on the same principle.

D-AMPS *Wireless*

See Digital AMPS.

DARCS *Software*

See David’s Advanced Revision Control System.

Dark Fiber *Telecom, Hardware*

Dark fiber refers to unused fiber-optic cables that have been laid out in the field. Oftentimes companies lay more lines than what’s needed in order to curb costs of having to do it again and again. The dark strands can be leased to others who want to establish optical connections among their own locations.

DARPA *Organization*

See Defense Advanced Research Projects Agency.

Data *Software*

Data, in information industry, refers to distinct pieces of information, usually formatted in a special way. All information systems are divided into two general categories: data and programs. Data can exist in a variety of forms -- as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person’s mind. Programs refer to the collections of instructions for manipulating data, which may be software programs for compute processing, or a set of instructions for manual data operation.

Data Access Arrangement *Hardware*

Data Access Arrangement (DAA) provides the analog circuits that electrically isolate the modem from the phone line, separating the modem from the telephone line higher voltage. The FCC requires this feature of any device that connects to the PSTN, including fax machines and set-top boxes, and most manufacturers build modems around a FCC-approved DAA design.

Data Access Protocol *Networking, Protocol*

Data Access Protocol (DAP) is a protocol in the Digital Network Architecture to provide remote file access to systems supporting the DECnet.

DEC/HP Protocol

Data Aggregation *Security*

Data Aggregation is the ability to get a more complete picture of the information by collecting and analyzing several different types of records from various channels at once.

Data Architect *Software*

A data architect is a person responsible for making sure an organization’s strategic goals are optimized through the use of enterprise data standards. Data architect’s job frequently includes the set up and maintain a metadata registry and allows domain-specific stakeholders to maintain their own data elements.

Data Architecture *Software*

Data architecture describes how data is processed, stored, and utilized in a given system. It provides criteria for data processing operations that make it possible to design data flows and also control the flow of data in the system. Data architecture also includes topics such as metadata management, business semantics, data

E

E Channel *Telecom*
See Echo Channel.

E&M *Telecom*
See recEive and transMit.

E&M Leads Signaling *Telecom*
E&M Leads Signaling is a type of signaling in telecommunications. It indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.

E&M Signaling *Telecom*
E&M Signaling is a signaling method on a DS0 timeslot such that the signaling bits are used to indicate call states, such as on-hook, off-hook, alerting, and dial pulsing.

E.123 *Telecom*
E.123 refers to the ITU-R recommendation which is the notation for national and international telephone numbers recommendation. E.123 defines a standard way to write telephone numbers, email addresses, and web addresses.

E.164 *Telecom*
E.164 refers to an ITU- recommendation that defines the international telecommunication numbering plan and telephone number format used for the PSTN and some other data networks. E.164 numbers can have a maximum of 15 digits. It is an evolution of standard telephone numbers.

E.214 *Wireless*
E.214 is a telephone numbering plan used for delivering mobility management related messages in GSM networks. The E.214 number, derived from the IMSI E.214 numbers, is composed of two parts. The first part (the E.164 part) is made up of a country code followed by the network code. The second part of the number is made from the MSIN part of the IMSI which identifies an individual subscriber.

E1 *Telecom, Protocol*
E1 or E-1 is the European/China format for digital signal transmission, while T1/DS1 is for the North America/Japan. E1 carries signals at 2 Mbps with 32 channels at 64Kbps each, whereas 30 DS0 channels for voice/data and 2 channels for signaling and controlling. For T1, it carries signals at 1.544 Mbps with 24 channels at DS0 64Kbps each. E1 and T1 lines may be interconnected for international use.
ITU-T Protocol

E-1 *Telecom, Protocol*
See E1.

E164 NUmber Mapping *Networking, Protocol*
Electronic Numbering (ENUM or Enum), also refered to as “E164 NUmber Mapping” or “Telephone Number Mapping”, is a suite of protocols to unify the telephone system with the Internet by using E.164 addresses with Dynamic Delegation Discovery System (DDDS) and Domain Name System (DNS). ENUM is a standard adopted by the Internet Engineering Task Force (IETF) that uses the domain name system (DNS) to map telephone numbers to Web addresses or uniform resource locators (URL). The goal of the ENUM standard is to provide a single number to replace the multiple numbers and addresses for an individual’s home phone, business phone, fax, cell phone, and e-mail.
IETF Specification: RFC 3761

E2 *Telecom*
E2 or E-2 refers to the European Digital Signal 2 which is the European standard for digital physical interface at 8.448 Mbps.

E-2 *Telecom*
See E2.

E2A *Networking*
E2A is a legacy protocols for providing OAM&P functions between a network element and an operations support system.

E3 *Telecom, Protocol*
E3 or E-3 is the European/China format for digital signal transmission while T3/DS3 is for the North America/Japan. E3 carries data at a rate of 34.368 Mbps. E3 can carry 16 E1 channels. E3 and T3 lines may be interconnected for international use.
ITU-T Protocol

E-3 *Telecom, Protocol*
See E3.

E4 *Telecom*
E4 or E-4 refers to the European Digital Signal 4 which is the European standard for digital physical interface at 139.264 Mbps.

E-4 *Telecom*
See E4.

E-911 *Wireless*
See Enhanced 911.

E911 Service *Wireless*
E911 Service, short for Enhanced 911 Service, is a North American telephone network (NANP) feature of the 911 (or basic 911) emergency calling system which can automatically report the telephone number and location of 911 calls made from wireline phones.

E-AGCH *Wireless*
See E-DCH Absolute Grant Channel.

EAP *Security*
See Extensible Authentication Protocol.

EAP over LAN *Security, Protocol*
EAP over LAN (EAPOL), defined in the IEEE 802.1X, offers an effective framework for authenticating and controlling user traffic

F

F2F *Networking*

See Friend-to-Friend.

FAA *Telecom*

See Facility Accepted.

FACCH *Wireless*

See Fast Associated Control Channel.

Faceplate *Hardware*

Faceplate is the plate installed over a switch or receptacle. The plate also covers the wall opening and thus protects the wiring. A motherboard faceplate is the plate that fits over a motherboard ports to supply a secure casing around the ports. A motherboard faceplate helps keep the motherboard enclosed within a PC and helps prevent dust from accumulating on the motherboard. Motherboard faceplates typically are installed into the back of a computer case.

Facilities Based Private Switched Network Services *Telecom*

Facilities Based Private Switched Network Services refers to the services provided by so called Facilities Based Carriers, a long-distance service provider that owns its own physical facilities as opposed to the bulk of the long-distance companies who are resellers.

Facility Accepted *Telecom*

Facility Accepted (FAA) is one of the message type codes in BICC protocol. It indicates that the FAR is accepted and the use of the facility or operation towards the other side is accepted.

Facility Data Link *Telecom*

Facility Data Link (FDL) is a 4-kbps channel provided by the Extended Superframe (ESF) T1 framing format. The FDL performs outside the payload capacity and allows a service provider to check error statistics on terminating equipment without intrusion.

Facility Loopback *Telecom*

Facility Loopback refers to signal looped back toward the incoming facility. This technique is often used in T1 testing.

Facility ReJect *Telecom*

Facility ReJect (FRJ) is one of the message type code in BICC (Bearer independent Call Control) protocol (which, in turn, is part of SS7 protocol suite). Facility ReJect message indicates that the request to use the facility (an operation) towards the other side is denied. An example of such operations or facilities could be coin phones.

Facility-Based Carriers *Telecom*

Facility-based Carriers refers to a local or long-distance service provider that owns its own physical facilities.

Facsimile Transmission *Telecom*

Fax, also called Facsimile Transmission, is a system of communication or delivery for paper documents or other graphics material in which a special digital image scanner scans the pages of the document, compresses the scanned image using CCITT Group Compression, and transmits the digital signals by wire or radio to a FAX receiver at a remote point.

Fading *Wireless*

Fading is the variation in signal strength from its normal value. Fading is normally negative and can be either fast or slow. It is normally characterized by the distribution of fades, Gaussian, Rician, or Rayleigh.

Failure Domain *Networking*

Failure Domain is a Token Ring network area in which a failure has occurred in a Token Ring, defined by the information contained in a beacon. When a station detects a serious problem with the network (such as a cable break), it sends a beacon frame that includes the station reporting the failure, its NAUN, and everything in between. Beaconing in turn initiates a process called auto-reconfiguration.

Fair Information Practices *Security*

Fair Information Practices (FIP) are standards governing collection and use of personal data.

Fallback *Networking*

Fallback is a mechanism used by ATM networks when rigorous path selection does not generate an acceptable path. The fallback mechanism attempts to determine a path by selectively relaxing certain attributes, such as delay, in order to find a path that meets some minimal set of desired attributes.

False Acceptance *Security*

False acceptance, also called a type II error, is a mistake occasionally made by biometric security systems. In an instance of false acceptance, an unauthorized person is identified as an authorized person.

False Acceptance Rate *Security*

False Acceptance Rate (FAR) is often used in biometric access control systems. The false acceptance rate (FAR) is a measure of the likelihood that the access system will wrongly accept an access attempt, that is, will allow the access attempt from an unauthorized user.

False Negative *Security*

A false negative is the term applied to a failure in an alerting system -- most commonly in an anti-virus product or intrusion detection system. It occurs when a virus or intrusion condition exists, but is “allowed” (or ignored or missed) by the alerting system.

False Positive *Security*

G

G.703 *Telecom, Protocol*

G.703, a standard based on Pulse-code modulation (PCM) standard, specifies voice over digital networks. Voice to digital conversion according to PCM requires a bandwidth of 64 kbps (+/-100 ppm), resulting in the basic unit for G.703. G.703 specifies the physical and electrical characteristics of hierarchical digital interfaces at a rate up to 140Mbit/s.
ITU-T Specification: G.703

G.704 *Telecom, Protocol*

G.704 defines the synchronous frame structure used at primary and secondary hierarchy levels on G.703 interfaces up to 45Mbit/s. The conventional use of G.704 on a 2Mbit/s primary rate circuit provides 30 discrete 64kbit/s channels, with a further 64kbit/s channel available for common channel signalling.
ITU-T Specification: G.704

G.707 *Telecom, Protocol*

G.707 defines the Synchronous Digital Hierarchy (SDH) Bit Rates.
ITU-T Specification: G.707

G.708 *Telecom, Protocol*

G.708 defines the Network Node Interface (NNI) for Synchronous Digital Hierarchy (SDH).
ITU-T Specification: G.708

G.709 *Telecom, Protocol*

G.709 defines the Synchronous Multiplexing Structure.
ITU-T Specification: G.709

G.711 *Telecom, Protocol*

G.711 is an ITU-T standard for audio companding released in 1972. It is primarily used in telephony. G.711 represents 8-bit compressed pulse code modulation (PCM) samples for signals of voice frequencies, sampled at the rate of 8000 samples/second. G.711 encoder will create a 64 kbit/s bitstream. There are two main algorithms defined in the standard: mu-law algorithm (used in North America & Japan) and a-law algorithm (used in Europe and other countries).
ITU-T Specification: G.711

G.721 *Telecom, Protocol*

G.721 is a 32 kbps Adaptive Differential Pulse Code Modulation (ADPCM) speech compression algorithm. The sampling rate is 8 KHz. G.721 produces toll quality speech. With transmission error rates higher than 10.4, the perceived quality of G.721 is better than G.711. G.721 is the first ADPCM standard. Later came the standards of G.726 and G.727 for 40, 32, 24 and 16 kbps.
ITU-T Specification: G.721

G.722 *Telecom, Protocol*

G.722 is a wideband speech coding algorithm supporting bit rates of 64, 56 and 48 kbps. In G.722, the speech signal is sampled at 16000 samples/second. G.722 can handle speech and audio signal bandwidth upto 7 kHz, compared with 3.6 kHz in narrow band speech coders. G.722 coder is based on the principle of Sub Band - Adaptive Differential Pulse Code Modulation (SB-ADPCM). The signal is split into two sub-bands and samples from both bands are coded using ADPCM techniques.
ITU-T Specification: G.722

G.722.1 *Telecom, Protocol*

G.722.1 is an ITU-T standard for speech codecs that compresses 50Hz -7KHz audio signals into one of two bit rates, 24 or 32 Kbps.
ITU-T Specification: G.722.1

G.723 or G.723.1 *Telecom, Protocol*

G.723, also known as G.723.1 in more precise terms, is a standard-based voice codec providing voice quality (300 Hz to 3400 Hz) at 5.3 / 6.3 kbps. It was designed for video conferencing/telephony over standard phone lines, and is optimized for real-time encoding & decoding. G.723.1 is part of the H.323 (IP) and H.324 (POTS) standards for video conferencing.
ITU-T Specification: G.723 and G.723.1

G.726 *Telecom, Protocol*

G.726 is a ITU-T speech codec based on ADPCM operating at bit rates of 16-40 kbit/s. The most commonly used mode is 32 kbit/s, since this is half the rate of G.711, thus increasing the usable network capacity by 100%. G.726 specifies how a 64 kbps A-law or μ-law PCM signal can be converted to 40, 32, 24 or 16 kbps ADPCM channels where the 24 and 16 kbps channels are used for voice in Digital Circuit Multiplication Equiment (DCME) and the 40 kbps is for data modem signals (especially modems doing 4800 kbps or higher) in DCME.
ITU-T Specification: G.726

G.727 *Telecom, Protocol*

G.727 is an embedded Adaptive Differential Pulse Code Modulation (ADPCM) algorithms at rates of 40, 32, 24 and 16 kbit/s. G.727 defines the transcoding law when the source signal is a pulse-code modulation signal at a pulse rate of 64 kbit/s developed from voice frequency analog signals as fully specified by G.711.
ITU-T Specification: G.727

G.728 *Telecom, Protocol*

G.728, based on the Low-Delay Code Excited Linear Prediction (LD-CELP) compression principles, is a 16 kbps compression standard. G.728 has an algorithmic coding delay of 0.625 ms. G.728 normally compresses toll quality speech at 8000 samples/second. G.728 Annex G (G.728 G) is a fixed point specification of the coder working at a bit rate of 16000 bits/second. G.728 Annex I (G.728 I) is the packet loss concealment (PLC) technique used

H

H.225 *Telecom, Protocol*

H.225, a key protocol in the H.323 VOIP architecture defined by ITU-T, is a standard to cover narrow-band visual telephone services defined in H.200/AV.120-Series Recommendations. It specifically deals with those situations where the transmission path includes one or more packet-based networks, each of which is configured and managed to provide a non-guaranteed QoS, which is not equivalent to that of N-ISDN, such that additional protection or recovery mechanisms beyond those mandated by Rec.

ITU-T Specification: H.225

H.225.0 *Telecom, Protocol*

H.225.0, also called as H.225, is the specific document number for RAS, use of Q.931, and use of RTP under the H.323 VOIP architecture.

ITU-T Specification: H.225.0

H.235 *Telecom, Protocol*

H.235 is the security recommendation for the H.3xx series systems. In particular, H.235 provides security procedures for H.323-, H.225.0-, H.245- and H.460-based systems. H.235 is applicable to both simple point-to-point and multipoint conferences for any terminals which utilize H.245 as a control protocol.

ITU-T Specification: H.235

H.245 *Telecom, Protocol*

H.245, a control signaling protocol in the H.323 multimedia communication architecture, is for the exchange of end-to-end H.245 messages between communicating H.323 endpoints/terminals. The H.245 control messages are carried over H.245 control channels. The H.245 control channel is the logical channel 0 and is permanently open, unlike the media channels. The messages carried include messages to exchange capabilities of terminals and to open and close logical channels.

ITU-T Specification: H.245

H.248 *Telecom, Protocol*

H.248, also known as Media Gateway Control protocol (Megaco), is for the control of elements in a physically decomposed multimedia gateway, enabling the separation of call control from media conversion. Megaco is a result of joint efforts of the IETF and the ITU-T Study Group 16. Therefore, the IETF defined Megaco is the same as ITU-T Recommendation H.248.

ITU-T Specification: H.248

H.261 *Telecom, Protocol*

H.261 is the video coding standard of the ITU. It was designed for data rates which are multiples of 64Kbit/s and is sometimes called p x 64Kbit/s (p is in the range 1-30). These data rates suit ISDN lines, for which this video codec was originally designed. H.261 transports a video stream using the real-time transport protocol, RTP, with any of the underlying protocols that carry RTP.

ITU-T Specification: H.261

H.263 *Telecom, Protocol*

The H.263, by the International Telecommunications Union (ITU), supports video compression (coding) for video-conferencing and video-telephony applications. H.263 was developed to stream video at bandwidths as low as 20K to 24K bit/sec and was based on the H.261 codec. As a general rule, H.263 requires half the bandwidth to achieve the same video quality as in the H.261. As a result, H.263 has largely replaced H.261. H.263 uses RTP to transport video streams.

ITU-T Specification: H.263

H.264 *Telecom, Protocol*

The H.264, also named Advanced Video Coding (AVC), is the MPEG-4 Part 10. H.264 is jointly developed by ITU and ISO. H.264 supports video compression (coding) for video-conferencing and video-telephony applications. The H.264 video codec has a very broad rang of applications that covers all forms of digital compressed video from, low bit-rate Internet streaming applications to HDTV broadcast and Digital Cinema applications with nearly lossless coding. H.264 is designed as a simple and straightforward video coding with enhanced compression performance, to provide a “network-friendly” video representation.

ITU-T Specification: H.264

H.323 *Telecom, Protocol*

H.323, a protocol suite defined by ITU-T, is for voice transmission over internet (Voice over IP or VOIP). In addition to voice applications, H.323 provides mechanisms for video communication and data collaboration, in combination with the ITU-T T.120 series standards. H.323 is one of the major VOIP standards on a par with Megaco and SIP.

ITU-T Specification: H.323

H.450.2 *Telecom, Protocol*

H.450.2 is the call transfer supplementary service in the H.323 VOIP architecture.

ITU-T Specification: H.450.2

H.450.3 *Telecom, Protocol*

H.450.3 is the call diversion supplementary service in the H.323 VOIP architecture.

ITU-T Specification: H.450.3

HAAT *Wireless*

See Height Above Average Terrain.

Hacker *Security*

Hacker is a computer and networking guru who tries to break into computer systems legelly or illegally.

Hackers On Planet Earth *Security*

I

I.N. *Telecom*
See Intelligent Network.

I/O *Hardware, Networking*
See Input/Output.

I/O Channel Controller *Hardware*
I/O Channel Controller (IOCC) is a simple CPU used to handle the task of moving data to and from the memory of a computer.

I/O Device *Hardware, Networking*
Input/Output (I/O) Device is for transfering data to or from a computer or a processor. Typical I/O devices include printers, hard disk, keyboard and mouse. Some devices are basically input-only devices (keyboard and mouse); others are primarily output-only devices (CD) and others provide both input and output of data (hard disk, diskette, writeable CD-ROMs).

I/O Space *Hardware*
I/O space is a special memory region in some processors reserved for the attachment of I/O devices. Memory locations and registers within a processor's I/O space can only be accessed via special opcodes.

I2C *Hardware*
See Inter-IC Bus.

I2O *Hardware*
See Intelligent I/O.

I2P *Networking*
See Invisible Internet Project.

IAB *Networking, Organization*
See Internet Architecture Board.

IAHC *Networking, Organization*
See Internet International Ad Hoc Committee.

IANA *Networking, Organization*
See Internet Assigned Number Authority.

IASE *Security*
See Information Assurance Support Environment.

IATF *Security*
See Information Assurance Technical Framework.

IBALANCE *Software*
IBALANCE is the specialized software that recieves the data from the various sensors and gyroscopes on the IBOT powered wheelchair mobility system, allowing the iBOT to maintain balance during certain maneuvers; for example, during curb climbing the seat remains level while parts of the chassis tilt to climb the curb.

IBM Director *Networking, Software*
IBM Director is an element management system (EMS) or workgroup management system (WMS). The software was originally written to run on OS/2 2.0. It has subsequently gone through a number of name changes in the interim. It was changed in 1996 to IBM PC SystemView. Later in that same year, it was renamed to TME 10 NetFinity. The following year, it reverted back to a slightly altered version of its original name: IBM Netfinity Manager.

IBM PC *Hardware*
International Business Machines Personal Computer (IBM PC) is typically a single user personal computer, although they have been adapted into multi-user models for special applications. The predecessor of the current personal computers and progenitor of the IBM PC compatible hardware platform, it was introduced in August, 1981. The original model was designated the IBM 5150. The competible models of the IBM PC dominate the personal computer market. The entire PC business of IBM was sold to the Chinese company Lenova in 2005.

IBM Systems Network Architecture *Networking, Protocol*
The IBM Systems Network Architecture (SNA) is one of the most popular network architecture models. Although now considered as a legacy networking model, SNA is still widely deployed. SNA was designed around the host-to-terminal communication model that IBM's mainframes use.
IBM Protocol

IBSS *Wireless*
See Independent Basic Service Set.

IBSS *Wireless*
See Infrastructure BSS.

IBTA *Networking*
See InfiniBand Trade Association.

IC *Hardware*
See Integrated Circuit.

ICANN *Networking*
See Internet Corporation for Assigned Names and Numbers.

ICD *Networking*
See International Code Designator.

ICE *Hardware*
See In-Circuit Emulator.

IceNewk *Security*
IceNewk, a variation of ping of death, is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

ICMP *Networking, Protocol*
See Internet Control Message Protocol.

ICMP Attack *Security*

J

J2EE *Software*

See Java 2 Platform, Enterprise Edition.

J2ME *Wireless*

See Java 2 Platform, Micro Edition.

Jabber *Security*

In networking world, Jabber means a faulty device (usually a NIC) that continuously transmits corrupted or meaningless data onto a network. This may cause denial of service of the entire network from transmitting data beacuse other devices will perceive the network as busy. Jabber may also means sending data packet greater than the maximum 1518 bytes as specified in IEEE 802.3. To prevent this, jabber control should be added to the hardware. Jabber is also the name of an open, XML-based protocol for instant messaging and presence. Jabber-based software is deployed on thousands of servers across the Internet.

Jabber Lock-Up *Networking*

Jabber Lock-Up is a scheme in hubs to ensure that the network is not disabled due to transmission of excessively long data packets. This protection scheme will automatically interrupt the reception of abnormally long streams of data to prevent jabber lock-up. Jabber lock-up protects the medium from being overrun with data packets from a possibly defective device.

Jack *Telecom*

Jack is a connecting device usually in the wall into which a plug can be plugged to from a connection such as the telephone jack.

JACK Audio Connection Kit *Software*

The JACK Audio Connection Kit (JACK) is a soundserver or daemon that provides low latency connections between so-called jackified applications. It is created by Paul Davis and others and licensed under the GPL. JACK is free audio software. It can use ALSA, PortAudio and (still experimental) OSS as its back-end. As of 2003, it runs on GNU / Linux and Mac OS X.

Jacobson's Algorithm *Networking*

Jacobson's algorithm is a set of congestion-avoidance and control algorithms that introduces the use of a congestion window (cwnd) to regulate the data-sending rate in TCP. Jacobson's algorithm is implemented in all modern TCP implementations.

JADE Programming Language *Software*

JADE is an object-oriented programming language that exhibits a seamlessly integrated object-oriented database management system. It is designed to be an end-to-end development environment, which allows systems to be coded in one language from the database server at one end down to the clients at the other.

Jakarta Project *Software*

The Jakarta Project creates and maintains open source software for the Java platform. It operates as an umbrella project under the auspices of the Apache Software Foundation, and all of Jakarta products are released under the Apache License.

Jamming *Wireless*

Jamming refers to the interference with the air radio transmission. It may be used by people who is trying to disturb the receiver from receiving the radio signal at a target frequency.

JANET *Networking*

See Joint Academic NETwork.

Japan UNIX Network *Networking*

Japan UNIX Network (JUNET) is a noncommercial network in Japan. It is designed to promote communications between Japanese and other researchers.

Japanese Total Access Communication System *Wireless*

Japanese Total Access Communication System (JTAGS) is a 1G technology deployed in Japan based on the European TACS system. JTAGS is operating in the 900-MHz band.

Java *Software*

Java, in computer programming, is an object-oriented programming language developed by Sun Microsystems. It resembles C++, but was designed to avoid some of C++'s most notorious flaws. The Java language is used extensively on the World Wide Web, particularly because of its cross-platform nature, and its sandbox security concept.

Java 2 Platform, Enterprise Edition *Software*

Java 2 Platform, Enterprise Edition (J2EE), now called Java Platform, Enterprise Editor (Java EE), is a programming platform -- part of the Java Platform -- for developing and running distributed multitier architecture Java applications, based largely on modular software components running on an application server. The Java EE platform is defined by a specification. Similar to other Java Community Process specifications, Java EE is also considered informally to be a standard because providers must agree to certain conformance requirements in order to declare their products as Java EE compliant; albeit with no ISO or ECMA standard.

Java 2 Platform, Micro Edition *Wireless*

Java 2 Platform Micro Edition (J2ME) is a technology that allows developers to use the Java programming language to create applications for mobile wireless devices.

Java Beans *Software*

Java beans, in computer programming, are a portable, platform-independent means of creating reusable components. Created by Sun Microsystems, Java Beans are intended to be similar in functionality to OpenDOC, ActiveX, OLE, and COM.

Java Bytecode *Software*

Java bytecode is the form of instructions that the Java virtual ma

K

K Desktop Environment *Software*

K Desktop Environment (KDE) is a free desktop environment and development platform built with Trolltech's Qt toolkit. It runs on most Unix and Unix-like systems, such as Linux, BSD, AIX and Solaris. There are also ports to Mac OS X using its X11 layer and to Microsoft Windows using Cygwin.

KA9Q *Networking, Wireless*

KA9Q, also called KA9Q NOS or simply NOS, was a popular early implementation of TCP/IP and associated protocols for amateur packet radio systems and smaller personal computers connected via serial lines. It was named after the amateur radio callsign of Phil Karn, who first wrote the software for a CP/M system and then ported it to DOS on the IBM PC. KA9Q NOS is obsolete now. For some people, KA9Q is also a name for the IP-over-IP Tunneling protocol.

Ka-Band *Wireless*

Ka-Band refers to the bandwidth of electromagnetic wave between 33 GHz to 36 GHz, which is primarily used in satellites operating at 30 GHz uplink and 20 GHz downlink for mobile voice communications.

Kad Network *Networking*

The Kad Network is a completely decentralized file-sharing network that does not make use of central servers. It implements the Kademlia P2P overlay protocol. Currently, two client programs use this network: eMule and MLdonkey. The majority of users on the Kad network are also connected to servers on the eDonkey network, and Kad network clients typically query known nodes on the eDonkey network in order to find an initial node on the Kad network.

Kademlia *Networking*

Kademlia is an overlay network protocol for decentralized peer-to-peer computer networks. It specifies the structure of the network, regulates communications between nodes and how the exchange of information has to take place. Kademlia nodes communicate among themselves using the transport protocol UDP. Kademlia nodes store data by implementing a distributed hash table.

Karma *Software*

In the computer software context, Karma is the name of a software package to aid signal processing and image processing for scientific applications.

Karn's Algorithm *Networking*

Karn's Algorithm is an algorithm used in the TCP to improve round-trip time estimations by helping transport layer protocols such as TCP distinguish between good and bad round-trip time samples. Karn's algorithm can prevent erroneous segment Round Trip Time (RTT) measurements due to segment retransmissions. Karn's algorithm was originally designed to be used in packet radio networks, and it is very resistant to packet loss. The problem with Karn's algorithm is that it does not adapt to high variations of delay.

Kazaa Lite *Software*

Kazaa Lite, also known as K-Lite, is a peer-to-peer file-sharing computer program. Kazaa Lite is an unauthorized modification of the Kazaa Media Desktop application which excludes adware and spyware and provides slightly extended functionality. It became available in April, 2002. It can be downloaded free of charge, and, as of mid-2005, is almost as widely used as the official Kazaa client itself. It connects to the same FastTrack network and thus allows to exchange files with all Kazaa users.

Kazaa Lite K++ *Networking, Software*

Kazaa Lite K++ is a later versions of Kazaa Lite included K++, which added a memory patcher that removed search limit restrictions, multi-source limits, and set one's "participation level" to the maximum of 1000. KaZaA Lite K++ has the ability to resume downloads, play files, block your IP address from the RIAA. Kazaa Lite K++ is obsolete and replaced by Kazaa Lite Resurrection (or simply Kaza Lite).

Kazaa Lite Resurrection *Networking, Software*

Kazaa Lite Resurrection, also known as Kazaa Lite, is a P2P file sharing client that supports the FastTrack P2P network. Kazaa Lite Resurrection is to continue the development forward on the now obsolete Kazaa Lite K++ application. Kazaa Lite Resurrection technology utilizes the core of Kazaa Media Desktop (KMD) and runs on Windows. Kazaa Lite Resurrection does not contain any adware or spyware. It also offers numerous improvements over KMD such as no bit-rate limits, expanded support for multi-source downloads, and additional P2P tools.

Kazaa Lite Revolution *Networking, Software*

Kazaa Lite Revolution is an alternative, unauthorized FastTrack P2P network client. Kazaa Lite Revolution, instead of Kazaa Media Desktop, may be used to connect to FastTrack. Revolution is sometimes advertised as an improved version of KMD. Their appearance is similar, but Revolution removes all advertising and adds several new features and tools. Kazaa Lite Revolution is a different application from Kazaa Lite Resurrection.

Kazaa *Networking, Software*

Kazaa, also spelled as Kazzaa, is a free, peer-to-peer file sharing service over the Internet. To use Kazaa, a person downloads and installs a software client of Kazaa. Kazaa clients communicate with various registration servers, using Internet protocols, to identify files for sharing or download. The Kazaa P2P network holds peer registration information and then brokers connections between any two peer clients for file sharing.

L

L0phtcrack *Security*

L0phtCrack is the de facto standard NT password auditing tool for U.S. industry, government and military. L0phtcrack recovers passwords from Windows NT registries or network sniffer logs in a variety of fashions, including exhaustive keyspace attacks.

L1 Cache *Hardware*

Level 1 (L1) cache, also known as primary cache, is a memory cache built into the CPU. L1 cache is used by the central processing unit of a computer to reduce the average time to access memory. The cache is a smaller, faster memory which stores copies of the data from the most frequently used main memory locations. As long as most memory accesses are to cached memory locations, the average latency of memory accesses will be closer to the cache latency than to the latency of main memory.

L2 Cache *Hardware*

Level 2 (L2) cache, also known as secondary cache or RAM cache, is the cache memory external to the CPU. L2 cache memory resides on a separate chip from the microprocessor chip. L2 cache contains a subset of the contents of main memory. The design of the memory and L2 cache is a significant way designers differentiate their systems.

L2CAP *Wireless, Protocol*

See Logical Link Control and Adaptation Protocol.

L2F *Security, Protocol*

See Layer 2 Forwarding Protocol.

L2TP *Security, Protocol*

See Layer 2 Tunneling Protocol.

L2TP Access Concentrator *Networking*

L2TP Access Concentrator (LAC) is a node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

L2TP Network Server *Networking*

L2TP Network Server (LNS) is a node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC.

L2TP Session *Networking*

L2TP Session, also known as L2TP call, refers to the communications transactions using Layer 2 Tunneling Protocol (L2TP) between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS) that support tunneling of a single PPP connection. L2TP session (or call) is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel.

L2TP Tunnel *Networking*

L2TP Tunnel refers to the logic link between the two Layer 2 Tunneling Protocol (L2TP) endpoints: the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols such as Point-to-Point Protocol (PPP) are then run through the L2TP tunnel.

L3 Cache *Hardware*

Level 3 cache is the third-fastest cache memory available to a CPU. It usually consists of SRAM chips located on the motherboard. The “L3” indicates that the CPU attempts to access this cache after accessing the L1 and L2 cache. Level 3 cache is now the name for the extra cache built into motherboards between the microprocessor and the main memory.

Label *Telecom, Networking*

Label, in telecommunication, is one type of information contained in a signaling message that is used to identify the particular circuit, call, or management transaction to which the message is related.

Label Bit Rate *Networking, Telecom*

Label Bit Rate (LBR) is a service category for label VC traffic in an ATM network. Link and per-VC bandwidth sharing can be controlled by relative bandwidth configuration at the edge and each switch along a label VC. No ATM traffic-related parameters are specified.

Label Distribution Protocol *Networking, Protocol*

Label Distribution Protocol (LDP) is a signaling protocol in the MPLS (Multi Protocol Label Switching) architecture. In the MPLS network, 2 label switching routers (LSR) must agree on the meaning of the labels used to forward traffic between and through them. LDP defines a set of procedures and messages by which one LSR (Label Switched Router) informs another of the label bindings it has made.

IETF Specification: RFC 3036

Label Forwarding Information Base *Networking*

Label forwarding information base (LFIB) is a data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

Label Imposition *Networking*

Label Imposition is the act of putting the first label or tag on a packet, which is a necessary procedure in a Multiprotocol label

M

M Plane *Telecom*
See Management Plane.

M2PA *Telecom*
See MTP2 Peer-to-peer user Adaptation layer.

M2UA *Telecom*
See MTP2-User Adaptation layer.

M3UA *Telecom*
See MTP3-User Adaptation layer.

MAC *Networking*
See Media Access Control.

MAC *Security*
See Mandatory Access Control.

MAC Address *Networking*
Media Access Control address (MAC address) is a unique identifier attached to most forms of networking equipment. A MAC address is 48 bits long. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows: 48-3F-0A-91-00-BC. Most layer 2 network protocols use one of three numbering spaces managed by the IEEE: MAC-48, EUI-48, and EUI-64, which are designed to be globally unique.

MAC Address Learning *Networking*
MAC address learning is a service that characterizes a learning bridge, in which the source MAC address of each received packet is stored so that future packets destined for that address can be forwarded only to the bridge interface on which that address is located. Packets destined for unrecognized addresses are forwarded out every bridge interface. This scheme helps minimize traffic on the attached LANs. MAC address learning is defined in the IEEE 802.1 standard.

MAC Address Spoofing *Security*
MAC Address spoofing, also known as MAC spoofing, refers to use other's MAC address to gain unauthorized access to a network. MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker.

MAC Key *Security*
MAC key is the message authentication code (MAC) key used with Schannel protocols.

MAC Layer *Networking*
Media Access Control Layer (MAC Layer) is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC card) to another across a shared channel.

Mac OS *Software*
See Macintosh Operating System.

Mac OS X *Software*
Mac OS X is the tenth and the latest version of the Macintosh operating system, and is designed and developed by Apple Computer to run on their Macintosh line of personal computers. Mac OS X is built on Darwin, an open source Unix-like environment which is based on the BSD source tree, and the Mach micro-kernel.

MAC Duplication *Security*
MAC duplication is a type of denial of service (DoS) attack against switched networks.

MAC Flooding *Security*
MAC flooding is a type of denial of service (DoS) attack against switched networks. Switches maintain a list (called a translation table) that maps individual MAC addresses on the network to the physical ports on the switch. In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table. The result of this attack causes the switch to enter a state called fail-open mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. A malicious user could then use a packet sniffer running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and IM conversations), which would normally not be accessible, were the switch operating normally.

MAC Spoofing *Security*
MAC spoofing, also known as MAC address spoofing, is an attack that involves spoofing the Media Access Control (MAC) address of legitimate hosts. MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker.

Machine Code *Software*
Machine code, also known as machine language, is a system of instructions and data directly understandable by computer central processing unit. Every CPU model has its own machine code, or instruction set, although there is considerable overlap between some. If CPU A understands the full language of CPU B, it is said that CPU A is compatible with B. CPU B may not be compatible with CPU A, as A may know a few codes that B does not.

Machine Code Instruction *Software*
Machine code instruction is the "words" of a machine or a computer. Instructions are patterns of bits with different patterns corresponding to different commands to the machine. Every CPU model has its own machine code, or instruction set, although

N

NACK *Networking*
See Not Acknowledge.

NACN *Wireless*
See North American Cellular Network.

NACS *Networking*
See NetWare Asynchronous Communication Services.

NADF *Networking*
See North American Directory Forum.

NADN *Networking*
See Nearest Active Downstream Neighbor.

NADS *Wireless*
See North American Digital Standards.

Nagle Algorithm *Networking*
The Nagle algorithm was designed to reduce LAN and other network congestion from TCP applications and remains a standard feature of TCP implementations since 1980s. The Nagle algorithm works by aggregating data on the sending side of TCP applications. It accumulates sequences of small messages into larger TCP packets before data reaches the wire, thereby preventing the generation of unnecessarily large numbers of small packets. When the Nagle algorithm works as designed, TCP applications utilize network resources more efficiently.

Nagware *Software*
Nagware, also known as annoyware, is a type of shareware software. Other types of shareware include demoware, crippleware, freeware, adware, and even spyware. Nagware reminds, or nags, the user to register it by paying a fee. It usually does this by popping up a message when the user starts the program or, worse, intermittently while the user is using the application. These messages can appear as windows obscuring part of the screen or message boxes that can quickly be closed.

NAK *Networking*
See Negative Acknowledgment.

Naked Call *Telecom*
Naked Call refers to an incoming call that receives no greeting message and no call menus/flexible routing before it is routed into an ACD (Automatic Call Distribution) queues.

Naked DSL *Telecom*
Naked DSL is a digital subscriber line without a PSTN (Public Switched Telephone Network) service. In other words, only a standalone DSL internet service is provided on the local loop. In regular DSL, a wire runs from the telephone switch to a POTS (Plain Old Telephone Service) splitter. The POTS splitter separates the DSL and voice bands and then a wire carrying both services runs from the splitter to the cable head, where it continues on to the customer on an outside plant. But Naked DSL the portion of cable from the switch to the POTS splitter is removed, therefore removing dial tone from the line.

Name Binding *Software*
In programming languages, name binding refers to the association of values with identifiers. An identifier bound to a value is said to reference that value. Since computers themselves have no notion of identifiers, there is no binding at the machine language level -- name binding is an abstraction provided by programming languages. Binding is intimately connected with scoping, as scope determines when binding occurs.

Name Binding Protocol *Networking, Protocol*
Name Binding Protocol (NBP) is the AppleTalk transport-level protocol used for translating network device names to addresses and manages the use of names on AppleTalk networks. NBP enables AppleTalk protocols to understand user-defined zones and device names by providing and maintaining translation tables that map names to their corresponding socket addresses.
Apple Protocol

Name Caching *Networking*
Name Caching is a method by which remotely discovered host names are stored by a router for use in future packet-forwarding decisions to allow quick access.

Name Resolution *Networking*
Name Resolution is the process of associating a name with a network location.

Name Server *Networking*
Name Server is connected to a network that resolves network names (such as URL) into network addresses (such as IP addresses).

Namespace *Networking*
A namespace is an abstract container providing context for the items (names, or technical terms, or words) it holds and allows disambiguation of items having the same name (residing in different namespaces - compare: URL). As a rule, names in a namespace cannot have more than one meaning, that is, two or more things cannot share the same name. A namespace is also called a context, as the valid meaning of a name can change depending on what namespace applies.

Naming Scheme *Networking*
A naming scheme is a plan for naming objects. Naming schemes are often used for objects connected into computer networks.

NAMPS *Wireless*
See Narrowband Advanced Mobile Phone Service.

Nanika *Software*
Nanika is a desktop accessory application developed by Sagawa Toyoaki. Nanika is composed of three parts: “materia”, which is

O

O.K.I.
Software

See Open Knowledge Initiative.

OA&M
Telecom

See Operation, Administration and Maintenance.

OADM
Telecom

See Optical Add-Drop Multiplexer.

OAKLEY Key Determination Protocol
Security, Protocol

The OAKLEY Key Determination Protocol is based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP. OAKLEY was proposed as a protocol "by which two authenticated parties can agree on secure and secret keying material.

IETF Specification: RFC 2412

OAM Cell
Networking, Telecom

Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits. OAM cells provide a virtual circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up and the router is operational.

OAM&P
Telecom

See Operation, Administration, Maintenance and Provisioning.

OARnet
Networking

See Ohio Academic Resources Network.

OATH
Security

See Open Authentication.

OATH
Software

See Object-Oriented Abstract Type Hierarchy.

OBEX
Wireless

See OBject Exchange.

Object
Software

Generally, Object refers to any item that can be individually selected and manipulated. In computer programming such as object-oriented programming, an object is an individual unit of run-time data storage that is used as the basic building block of programs. These objects act on each other, as opposed to a traditional view in which a program may be seen as a collection of functions, or simply as a list of instructions to the computer. Each object is capable of receiving messages, processing data, and sending messages to other objects. Each object can be viewed as an independent little machine or actor with a distinct role or responsibility.

Object Code
Software

Object code, also known as object file, is an intermediate representation of code generated by a compiler after it processes a source code file. Object files contain compact, pre-parsed code, often called binaries, that can be linked with other object files to generate a final executable or code library. An object file is mostly machine code that can be directly executed by a computer's CPU. An object file contains not only the object code, but also relocation information that the linker uses to assemble multiple object files into an executable or library, program symbols (names of variables and functions), and debugging information.

Object Database
Software

Object database refers to a type of database in which information is represented in the form of objects. The database management system for an object database is referred to variously as a ODBMS or OODBMS. Object database technologies becomes useful when: (1) a relational database becomes cumbersome to be used with complex data; (2) data is generally manipulated by application software written using object-oriented programming languages and tools such as C++, Java, Borland Delphi and C#, and the code needed to translate between this representation of the data, and the tuples of a relational database can be tedious to write and time-consuming to execute.

Object Database Management System
Software

Object Database Management System (ODBMS), also known as Object Oriented Database Management System (OODBMS), refers to the database management system for an object database. Benchmarks between ODBMSs and relational DBMSs have shown that ODBMS can be clearly superior for certain kinds of tasks. The main reason for this is that many operations are performed using navigational rather than declarative interfaces, and navigational access to data is usually implemented very efficiently by following pointers. Critics of ODBMS, suggest that pointer-based techniques are optimized for very specific "search routes" or viewpoints. However, for general-purpose queries on the same information, pointer-based techniques will tend to be slower and more difficult to formulate than relational.

Object Desktop Network
Software

The Object Desktop Network (OD or ODNT) is a software subscription service created by Stardock. Launched in 1995 on OS/2, it transitioned in 1997/98 to the Windows platform. Subscribers typically download Object Desktop components across the Internet using Stardock Central, although CD snapshots are available on request. Once downloaded, users may use released versions of components forever.

OBject Exchange
Wireless

OBject EXchange (OBEX or IrOBEX) is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and

P

P equals NP *Security*

Polynomial (P) equals nondeterministic polynomial (NP) question asks: if positive solutions to a YES/NO problem can be verified quickly, can the answers also be computed quickly? In information security, an “P and NP” problem defies any brute-force approach at solution because finding the correct solution would take trillions of years or longer even if all the supercomputers in the world were put to the task. Some mathematicians believe that this obstacle can be surmounted by building a computer capable of trying every possible solution to a problem simultaneously. This hypothesis is called P equals NP, in information security.

P versus NP *Security*

P versus NP (polynomial versus nondeterministic polynomial) refers to a theoretical question presented in 1971 by Leonid Levin and Stephen Cook, concerning mathematical problems that are easy to solve (P type) as opposed to problems that are difficult to solve (NP type).

P/F *Networking*

See Poll/Final Bit.

P2MP *Networking*

See Point-to-Multipoint.

P2P *Networking*

See Peer-to-Peer.

P3P *Security*

See Platform for Privacy Preferences Project.

P7zip *Software*

P7zip is a port of the command line version of the 7-Zip file archiver -- famous for its introduction of the high-compression 7z format -- to POSIX-conforming operating systems, such as Unix, Linux, Windows NT (or greater version) and Mac OS X. It is free software, available under the LGPL free software license.

PABX *Telecom*

See Private Automatic Branch Exchange.

Packaged Software *Software*

Packaged software refers to a commercial application program or collection of programs developed to meet the needs of a variety of users, rather than custom designed for a specific user or company. Packaged software is normally put on a CD (or disks), packaged in a box and sold to the general public.

Packed Encoding Rules *Wireless*

Packed Encoding Rules (PER) is a set of rules that specifies how ASN.1-defined information is encoded when transmitted, and how it is decoded when received. PER is a successor to the Basic Encoding Rules (BER). It is more efficient in terms of the number of bytes transmitted and the size of the generated encoder and decoder.

Packet *Networking*

A packet, in data networking, is one unit of binary data formatted for transmission on a network. To improve communication performance and reliability, each message sent between two network devices is often subdivided into packets by the underlying hardware and software. Packet formats generally include a header, the body containing the message data (also known as the payload), and sometimes a footer (also known as the trailer). The packet header lists the origin and destination of the packet and often indicates the length of the message data. The packet footer contains data that signifies the end of the packet. Both the packet header and footer may contain error-checking information.

Packet Analysis *Networking*

Packet analysis is a process for a software program or a hardware device (plus software) to capture packets and then decode their headers and trailers information to understand the data and information inside the packet encapsulated by the protocol.

Packet Analyzer *Networking*

Packet Analyzer is a software or hardware tool to capture and analysis packets. It is also called protocol analyzer since the tool must decode the protocols that encapsulate the packets.

Packet Assembler/Disassembler *Networking*

Packet Assembler/Disassembler (PAD) is the component of a packet transmission system that segments the transmit data into packets and returns the received data to longer messages.

Packet Buffer *Hardware, Networking*

Packet buffer is the memory space reserved for storing a packet awaiting transmission or for storing a received packet. Packet buffer is set aside specifically for either storing a packet that is awaiting transmission over a network or storing a packet that has been received over a network. The memory space is either located in the network interface card or in the computer that holds the card.

Packet Control Unit *Wireless*

The Packet Control Unit (PCU) is a late addition to the GSM standard. It performs some of the processing tasks of the Base Station Controller (BSC), but for packet data. The allocation of channels between voice and data is controlled by the base station, but once a channel is allocated to the PCU, the PCU takes full control over that channel. The PCU can be built into the base station, built into the BSC, or even in some proposed architectures, it can be at the SGSN site.

Packet Data Convergence Protocol *Wireless, Protocol*

Packet Data Convergence Protocol (PDCP) is used in UMTS 3G network to map higher-level protocol characteristics onto the characteristics of the underlying radio-interface protocols, providing protocol transparency for higher-layer protocols. PDCP also provides protocol control information compression.

Q

Q Signaling *Telecom, Protocol*

Q Signaling (QSING) is a common channel signaling protocol based on ISDN Q.931 standards and used by many digital PBXs.
ITU-T Protocol

Q.2931 *Telecom, Protocol*

Q.2931, based on Q.931, is a signaling protocol, which specifies the procedures for the establishment, maintenance and clearing of network connections at the B-ISDN user network interface. The PNNI and the UNI specifications are based on Q.2931. The procedures are defined in terms of messages exchanged.
ITU-T Specification: Q.2931

Q.700 *Telecom, Protocol*

Q.700, an ITU-T specification, provides an introduction to CCITT Signalling System No. 7 (SS7).
ITU-T Specification: Q.700

Q.703 *Telecom, Protocol*

Q.703, an ITU-T specification, defines the Signalling System No. 7 (SS7) - Message Transfer Part, Signalling Link.
ITU-T Specification: Q.703

Q.704 *Telecom, Protocol*

Q.704, an ITU-T specification, defines the Signalling System No. 7 (SS7) - Message Transfer Part, Signalling System No. 7 - Signalling Network Functions and Messages.
ITU-T Specification: Q.704

Q.705 *Telecom, Protocol*

Q.705, an ITU-T specification, defines the System No. 7 - Signalling network structure.
ITU-T Specification: Q.705

Q.706 *Telecom, Protocol*

Q.706, an ITU-T specification, defines the Signalling System No. 7 - Message Transfer Part Signalling Performance.
ITU-T Specification: Q.706

Q.712 *Telecom, Protocol*

Q.712, an ITU-T specification, defines the Signalling System No. 7 (SS7) - Definition and Function of SCCP Messages.
ITU-T Specification: Q.712

Q.713 *Telecom, Protocol*

Q.713, an ITU-T specification, defines the Signalling System No. 7 - SCCP Formats and Codes.
ITU-T Specification: Q.713

Q.716 *Telecom, Protocol*

Q.716, an ITU-T specification, defines the Signalling System No. 7 - Signalling connection control part (SCCP) performance.
ITU-T Specification: Q.716

Q.725 *Telecom, Protocol*

Q.725, an ITU-T specification, defines Signalling System No. 7 - Signalling performance in the telephone application.
ITU-T Specification: Q.725

Q.730 *Telecom, Protocol*

Q.730, an ITU-T specification, defines the ISDN User Part (ISUP) supplementary services.
ITU-T Specification: Q.730

Q.731 *Telecom, Protocol*

Q.732, an ITU-T specification, provides the Stage 3 description for numbering identification supplementary services using Signalling System No. 7 (SS7).
ITU-T Specification: Q.731

Q.732 *Telecom, Protocol*

Q.733, an ITU-T specification, provides the Stage 3 description for call offering supplementary services using Signalling System No. 7 (SS7).
ITU-T Specification: Q.732

Q.733 *Telecom, Protocol*

Q.734, an ITU-T specification, provides the Stage 3 description for call completion supplementary services using No. 7 Signalling System (SS7).
ITU-T Specification: Q.733

Q.734 *Telecom, Protocol*

Q.734, an ITU-T specification, provides the Stage 3 description for multiparty supplementary services using Signalling System No. 7.
ITU-T Specification: Q.734

Q.735 *Telecom, Protocol*

Q.735, an ITU-T specification, provides the Stage 3 description for community of interest supplementary services using SS7.
ITU-T Specification: Q.735

Q.736 *Telecom, Protocol*

Q.736, an ITU-T specification, provides the Stage 3 description for charging supplementary services using Signalling System No. 7 (SS7).
ITU-T Specification: Q.736

Q.737 *Telecom, Protocol*

Q.737, an ITU-T specification, provides the Stage 3 description for additional information transfer supplementary services using Signalling System No. 7 (SS7).
ITU-T Specification: Q.737

Q.761 *Telecom, Protocol*

Q.761, an ITU-T specification, provides Signalling System No.7 (SS&) – ISDN user part (ISUP) functional description.
ITU-T Specification: Q.762

Q.762 *Telecom, Protocol*

Q.762, an ITU-T specification, defines the general function of

R

R Programming Language *Software*

The R programming language, sometimes described as “GNU S”, is a programming language and software environment for statistical computing and graphics. It was originally created by Ross Ihaka and Robert Gentleman (hence the name R) at the University of Auckland, New Zealand, and is now developed by the R core team. R is considered by its developers to be an implementation of the S programming language, with semantics derived from Scheme.

RACE *Networking*

See Research on Advanced Communications in Europe.

RACE *Wireless*

See Research in Advanced Communications Equipment.

Race Condition *Security*

A race condition exploits the small window of time between a security control being applied and when the service is used.

Race Condition Ranging *Networking*

Race Condition Ranging refers to the process of acquiring the correct timing offset such that the transmissions of a cable modem are aligned with the correct mini-slot boundary.

RACF *Security*

See Resource Access Control Facility.

RACH *Wireless*

See Random Access Channel.

Raconteur *Software*

Racter, short from raconteur, was an artificial intelligence computer program that generated English language prose at random. Its existence was revealed to the world in 1984. The great sophistication claimed for the program was, however, a hoax, as could be seen by investigation of the template system of text generation.

Racter *Software*

See Raconteur.

Radiation Monitoring *Security*

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Radio *Wireless*

Radio is the electromagnetic waves whose frequencies are below 3,000 GHz as defined in Article 2 of the Radio Law in general. However, in practice, radio is generally refered to as electromagnetic waves whose frequencies are between 10 kHz and 300 GHz.

Radio Access Network *Wireless*

Radio Access Network (RAN) is the ground-based infrastructure required for delivery of third-generation (3G) wireless communications services, including high-speed mobile access to the Internet. The RAN must be able to manage a wide range of tasks for each 3G user, including access, roaming, transparent connection to the public switched telephone network and the Internet, and Quality of Service (QoS) management for data and Web connections.

Radio Access Network Application Part *Wireless, Protocol*

Radio Access Network Application Part (RANAP) is the Radio Network Layer signaling protocol used in a UMTS system on the Iu interface. It is responsible for functions including the setting up of a RAB (Radio Access Bearer) between the CN (Core Network) and the RNC (Radio Network Controller).
ITU-T Protocol

Radio Broadcast Data System *Wireless*

Radio Broadcast Data System (RBDC), an replacement of Emergency Braodcast System, allows radio stations to send text messages, such as emergency warning and traffic alerts to radios installed with special display screens.

Radio Common Carrier *Wireless*

Radio Common Carrier (RCC) refers to a service provider for public mobile service.

Radio Configuration *Wireless*

Radio Configuration (RC) defines the physical channel configuration of cdma2000 (IS-2000) signals. Each RC specifies a set of data rates based on either 9.6 or 14.4 kbps. RC1 is the backwards-compatible mode of cdmaOne for 9.6 kbps voice traffic. It includes 9.6, 4.8, 2.4, 1.2 kbps data rates and operates at Spread Rate 1 (SR1). RC3 is a cdma2000 specific configuration based on 9.6 kbps that also supports 4.8, 2.7, and 1.5 kbps for voice, while supporting data at 19.2, 38.4, 76.8, and 153.6 kbps. RC3 also operates at SR1.

Radio Frequency *Wireless*

Radio Frequency generally refers to wireless communications with frequencies below 300 GHz. Formally, according to the Article 2 of th Radio Law, radio frequency is below 3,000 GHz. Radio frequencies can be used for communications between a mobile telephone and an antenna mast.

Radio Frequency Communication *Wireless*

Radio Frequency Communication (RFCOMM) is a Bluetooth protocol which is a simple set of transport protocols, providing emulated RS232 serial ports (up to sixty simultaneous connections of a bluetooth device at a time). RFCOMM is sometimes called Serial Port Emulation. The Bluetooth Serial Port Profile is based on this protocol.

Radio Frequency Identification *Wireless*

Radio frequency identification (RFID) is a system for tagging

S

S Programming Language *Software*

S programming language, developed primarily by John Chambers and (in earlier versions) Rick Becker and Allan Wilks of Bell Laboratories, is a programming language and software environment for statistical computing and graphics. There are two implementations of S programming language: the R programming language, and Insightful's S-PLUS.

S/I *Wireless*

See Signal-to-interference ratio.

S/Key *Security*

S/KEY is a one-time password system developed for Unix-like operating systems that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. S/Key is supported in Linux via Pluggable authentication modules, OpenBSD, NetBSD, and FreeBSD.

S/MIME *Networking*

See Secure Multipurpose Internet Mail.

S/N *Wireless*

See Signal-To-Noise Ratio.

S/W *Software*

See Software.

SAA *Software*

See Systems Application Architecture.

SABP *Wireless*

See Service Area Broadcast Protocol.

SACCH *Wireless*

See Slow Associated Control Channel.

SACL *Security*

See System Access Control List.

Sacrificial Lamb *Security*

Sacrificial lamb refers to a server placed outside the firewall with the expectation that it may become compromised.

Sadmind *Security*

Sadmind is a worm that compromises one platform to attack another.

SAFE Architecture *Security*

SAFE Architecture is a network security framework developed by Cisco Systems. SAFE is intended to be a flexible and dynamic blueprint for network security that is based on the Cisco Architecture for Voice, Video, and Integrated Data (AVVID).

Safe Harbor *Security*

In literal terms, a safe harbor or safe harbour consists of a protected harbor or haven which provides safety from weather or attack. For information security, because of differences in approaches to the enforcement of privacy in computerized personal data, the US Department of Commerce and the European Commission developed a "safe harbor" framework. US companies that certify to the the safe harbor are assured of EU "adequacy" recognition, and are consequently safe from prosecution by European authorities under the European privacy laws.

Safe Harbor Agreement *Security*

Safe Harbor Agreement is an international agreement regarding the transfer of personally identifiable information (PII).

Safe Harbor Principles *Security*

Safe Harbor Principles are a series of directives for harmonizing privacy protection practices between the United States and the European Union (EU).

Safety *Security*

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

SAINT *Security*

See Security Administrator's Integrated Network Tool.

Sales Force Automation *Software*

Sales force automation (SFA) is a process of using software to automate the sales functions and process in a business, including order processing, contact management, information sharing, inventory monitoring and control, order tracking, customer management, sales forecast analysis and employee performance evaluation.

SALT *Wireless*

See Speech Application Language Tags.

Salt *Security*

In password protection, salt is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system.

Sam Spade *Security*

Sam Spade is a site for tracking down spammers and a set of tools for the same purpose.

Samba *Networking*

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients regardless which operating system -- Linux, Unix, IBM system 390, Open VMS or Windows -- it is based on. Samba can be run on multiple platforms including Microsoft Windows, UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses the TCP/IP

T

T.120 *Telecom, Protocol*

The T.120, an ITU-T standard, is made up of a suite of communication and application protocols. T.120 protocols are designed for multipoint Data Conferencing and real time communication, including multilayer protocols which considerably enhance multimedia, MCU and codec control capabilities. Depending on the type of T.120 implementations, the resulting product can make connections, transmit and receive data and collaborate using compatible data conferencing features, such as program sharing, whiteboard conferencing and file transfer.

ITU-T Specification: T.120

T.30 *Telecom, Protocol*

The T.30, an ITU-T standard, describes the overall procedure for establishing and managing communication between two fax machines.

ITU-T Specification: T.30

T.38 *Telecom, Protocol*

The T.38, an ITU-T standard, defines procedures for real-time Group 3 facsimile communication over IP networks.

ITU-T Specification: T.38

T1 *Telecom*

T1 is a digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding.

T1 Access Line *Telecom*

T1 Access line is a 1.544 Mbps T1 line that provides twenty-four 64 Kbps data channels and uses in-band signaling. This type of line can contain all switched channels, all nailed-up channels, or a combination of switched and nailed-up channels.

T1 Cable *Telecom*

T1 Cable refers to a physical cable for T1 Line. T1 cable is two twisted pairs of 22 AWG, 100 ohm wire with the added characteristic that each pair is individually shielded.

T1 Carrier *Telecom*

T1 Carrier is a dedicated phone connection, a time-division multiplexed digital transmission facility, supporting data rates of 1.544Mbits per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second. Each 64Kbit/second channel can be configured to carry voice or data traffic. Most telephone companies allow you to buy just some of these individual channels, known as fractional T-1 access. Developed in the 1960s, the T1 carrier is designed to operate full duplex over two pairs in unshielded twisted pair (UTP) cable.

T1 Line *Telecom*

T1 Line is a general term for a digital carrier typically leased from a local or long-distance provider, capable of transmitting 1.544 Mbps of electronic information. A T1 line is point-to-point, as opposed to a dialable ISDN line. T1 lines may be used fractionally or at their full bandwidth. E1 is the approximate European equivalent, prevalent also in Mexico. E.g., the UT video network is composed primarily of leased T1 lines that carry compressed video and Internet data between UT components.

T1 PRI Line *Telecom*

T1 PRI Line is a T1 line that uses 23 B channels for user data, and one 64 kbps D channel for ISDN D-channel signalling. The B channels can be all switched, all nailed up, or a combination of both. This type of PRI line is a standard in North America, Japan, and Korea.

T1/DS-1 *Telecom*

T1/DS-1 is trunk level 1 that is the equivalent of 24 multiplexed voice grade channels at 64 Kbps. It is a dedicated phone connection with a total speed of 1,544 Mbps.

T2/DS-2 *Telecom*

T2/DS-2, trunk level 2, is a facility that is equivalent of 4 multiplexed T1 Channels at a speed of 6.3 Mbps.

T3 *Telecom*

T3 is a digital WAN carrier facility. T3 transmits DS-3-formatted data at 44.736 Mbps through the telephone switching network.

T3 Line *Telecom*

T3 Line is a high-speed connection capable of transmitting data at a rate of 45 Mbps. A T3 Line represents a bandwidth equal to about 672 regular voice-grade telephone lines. A T3 Line is typically installed as a major networking artery for corporations and universities with a high-volume network traffic.

T3/DS-3 *Telecom*

T3/DS-3, trunk level 3, is a facility that is equivalent of 28 multiplexed T1 channels at a speed of 45 Mbps.

T4/DS-4 *Telecom*

T4/DS-4, trunk level 4, is a facility that is equivalent of 6 multiplexed T3 channels at a speed of 274 Mbps.

TAB *Telecom*

See Telephone Answering Bureau.

TABS *Telecom*

See Telemetry Asynchronous Block Serial.

TAC *Networking*

See Terminal Access Controller.

TACACS *Security*

See Terminal Access Controller Access Control System.

TACACS+ *Security*

See Terminal Access Controller Access Control System (version 3).

U

U Interface *Telecom*
U Interface, also known as the local digital subscriber line (DSL) loop, is the interface between the telco and the user.

UAA *Networking*
See Universally Administered Address.

UART *Networking*
See Universal Asynchronous Receiver/Transmitter.

Uauth *Security*
See User Authentication.

UB Net/One *Networking*
See Ungermann-Bass Net/One.

UBR *Networking*
See Unspecified Bit Rate.

UBR+ *Networking*
See Unspecified Bit Rate Plus.

UCAID *Networking*
See University Corporation for Advanced Internet Development.

UCD *Wireless*
See Uplink Channel Descriptor.

UDLP *Wireless*
See UniDirectional Link Protocol.

UDP *Networking*
See User Datagram Protocol.

UDP Flood *Security*
A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

UDP Port Numbers *Networking*
UDP Port Numbers are designed to distinguish multiple applications running on a single device with one IP address from one another. In the UDP header, there are "SourcePort" and "DestinationPort" fields which are used to indicate the message sending process and receiving process identities defined. The combination of the IP address and the port number is called "socket".

UDP Scan *Security*
UDP Scan, also known as UDP port scan, refers to performing port scans to determine which UDP ports are open. UDP scan can be used by attackers to launh attacks or for legitimate reasons.

UDP Port Scanning *Security*
UDP port scanning is the process of performing port scans to determine which User Datagram Protocol (UDP) ports are open. UDP scan can be used by attackers to launh attacks or for legitimate reasons.

UDP Tunneling *Security*
UDP tunneling refers to a method of using User Datagram Protocol (UDP) to establish a covert channel.

U-Frame *Networking*
See Unnumbered Frame.

UGS *Wireless*
See Unsolicited Grant Service.

UHF *Wireless*
See Ultra High Frenquency.

UICC *Wireless*
See USIM Integrated Circuit Card.

UI-Frame *Networking*
See Unnumbered Information Frame.

UIM *Wireless*
See User Identity Module.

UIT *Software*
See User Interface Toolkit.

UK Education and Research Networking Association *Networking*
UK Education and Research Networking Association (UKERNA) is government-funded, with the primary aim of providing and developing a network infrastructure that meets the needs of the education and research communities. UKERNA manages the operation and development of JANET on behalf of JISC (Joint Information Systems Committee) for the UK Further and Higher Education Funding Councils. JISC also works in partnership with the Research Councils.

UKERNA *Networking*
See UK Education and Research Networking Association.

ULP *Networking*
See Upper-Layer Protocol.

Ultra High Frenquency *Wireless*
Ultra High Frenquency (UHF) refers to the RF spectrum between 300 MHz and 3 GHz.

Ultra Wideband *Wireless*
See Ultra-Wide-Band.

Ultra-Wide-Band *Wireless, Protocol*
Ultra-Wide-Band (UWB), also called digital pulse, is a wireless technology defined in IEEE 802.15.3 for transmitting digital data over a wide swath of the radio frequency spectrum with very low power. Because of the low power requirement, it can carry signals through doors and other obstacles that tend to reflect signals at

V

V.24 *Telecom, Protocol*

V.24 is an ITU-T standard for a physical layer interface between DTE and DCE. V.24 is essentially the same as the EIA/TIA-232 standard.

ITU-T Specification: V.24

V.25bis *Telecom, Protocol*

V.25bis is an ITU-T specification describing procedures for call setup and tear-down over the DTE-DCE interface in a PSDN.

ITU-T Specification: V.25bis

V.32 *Telecom, Protocol*

V.32 is an ITU-T standard serial line protocol for bidirectional data transmissions at speeds of 4.8 or 9.6 kbps.

ITU-T Specification: V.32

V.32bis *Telecom, Protocol*

V.32bis is an ITU-T standard that extends V.32 to speeds up to 14.4 kbps.

ITU-T Specification: V.32bis

V.34 *Telecom, Protocol*

V.34 is an ITU-T standard that specifies a serial line protocol. V.34 offers improvements to the V.32 standard, including higher transmission rates (28.8 kbps) and enhanced data compression.

ITU-T Specification: V.34

V.35 *Telecom, Protocol*

V.35 is an ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe, and is recommended for speeds of up to 48 kbps.

ITU-T Specification: V.35

V.42 *Telecom, Protocol*

V.42 is an ITU-T standard protocol for error correction using Link Access Procedure for Modems (LAPM).

ITU-T Specification: V.42

V.xx *Telecom*

V.xx refers to various types of ITU-T communication standard. Some are for simple serial line communication (e.g., V.24, otherwise known as RS232), others are for modem communication (e.g., V.21, V.22, V.23, V.32), and others are for special uses (e.g., V.42, an error correction protocol). Sometimes, these standards are up-dated, and changed slightly, then they have bis added to the end (e.g., V.42bis a data compression protocol).

V5.2-User Adaptation Layer *Telecom, Protocol*

V5.2-User Adaptation Layer (V5UA) is a protocol in the SIGTRAN protocol stack for the backhauling of V5.2 messages over IP using the Stream Control Transmission Protocol (SCTP). This protocol may be used between a Signaling Gateway (SG) and a Media Gateway controller (MGC). It is assumed that the SG receives V5.2 signaling over a standard V5.2 interface.

IETF Specification: RFC 3807

V5UA *Telecom*

See V5.2-User Adaptation Layer.

VAC *Hardware*

See Volts Alternating Current.

Vacant Code Tone *Telecom*

Vacant Code Tone is used in crossbar systems to indicate that the dialed office code is unassigned. In step-by-step areas, this signal is called vacant level tone. For operator-originated calls, the verbal announcement is preceded by two flashes. In modern systems, recorded verbal announcements are used for this service. Vacant Code Tone is Low Tone for 0.5 seconds on, 0.5 seconds off, 0.5 seconds on and 1.5 seconds off.

Vacant Position Tone *Telecom*

Vacant Position Tone is a steady low tone. It is applied to all straightforward trunks terminating in a vacated position in manual offices.

Valgrind *Software*

Valgrind is a free programming tool for memory debugging, memory leak detection, and profiling. Valgrind was originally designed to be a free version of Purify for Linux on x86, but has since evolved to become a generic framework for creating dynamic analysis tools such as checkers and profilers. It is widely used by Linux programmers.

Valid Certificate *Security*

Valid Certificate refers to a digital certificate for which the binding of the data items can be trusted; one that can be validated successfully.

Validity Check *Telecom*

Validity Check refers to any check that is designated to ensure the quality of a transmission in a telecommunications system. A validity check compares a group of bits with the code being used to ensure that group of bits constitutes a valid character.

Value-Added Network *Networking*

Value-added Network (VAN) is a computer network or subnetwork that transmits, receives, and stores Electronic Data Interchange (EDI) transactions on behalf of its customers.

Value-Added Service *Telecom*

Value-Added Service (VAS), in telecommunications industry, refers to the non-core services or all services beyond standard voice calls. Conceptually, value-added services add value to the standard service offered by the telecommunications carrier, encouraging the user to use their phone more and allowing the carrier to drive up their ARPU (Average Revenue Per User).

W

W2K *Software*

See Windows 2000.

W32.Kriz Virus *Security*

The Kriz virus (known more formally as W32.Kriz, W32.Kriz.dr, or PE_KRIZ) infects files on Windows 9x and Windows NT and 2000 systems. It has a potentially devastating payload that triggers on December 25th of any year once an infected file is run. When this happens, the virus overwrites files on the floppy disk drive, hard drive, RAM drive, and network drives.

W3C *Networking*

See World Wide Web Consortium.

WAE *Wireless*

See Wireless Application Environment.

Wafer *Hardware*

Wafer is a piece of thin, round semiconductor material (typically silicon) which is used to make microchips. Typically, Silicon crystal is grown into a large cylindrical ingot, then sliced into very thin wafers.

WAFS *Security*

See Wide-Area File Service.

WAIS *Networking*

See Wide Area Information Server.

Walking 1s Test *Hardware*

Walking 1s test is a memory test that involves moving a 1 bit through a byte or word to systematically confirm each bit can hold a 1 value. All of the other bits are set to 0 during the test.

Walsh Code *Wireless*

Walsh Code is a group of spreading codes having good autocorrelation properties and poor crosscorrelation properties. Walsh codes are the backbone of CDMA systems and are used to develop the individual channels in CDMA. For IS-95, here are 64 codes available. Code 0 is used as the pilot and code 32 is used for synchronization. Codes 1 though 7 are used for control channels, and the remaining codes are available for traffic channels. Codes 2 through 7 are also available for traffic channels if they are not needed. For cdma2000, there exists a multitude of Walsh codes that vary in length to accommodate the different data rates and Spreading Factors of the different Radio Configurations.

WAMP *Software*

See Microsoft Windows, Apache, MySQL and Perl/PHP/Python.

WAN *Networking*

See Wide Area Network.

WAN Interface Card *Networking*

WAN Interface Card (WIC) is a type of Network Interface Card (NIC) that connects the system to the WAN link service provider. For example, the ATM card is a WIC.

Wannabee *Security*

Wannabee is a generally pejorative term for somebody who would like to be thought of as more proficient than he or she actually is. The implication is that wannabees are not actually capable of being what they want to be. It is often used to describe “wannabee hackers”. Script kiddies can be described as wannabee hackers or crackers.

WAP *Security*

See Wireless Application Protocol.

WAP *Wireless*

See Wireless Access Point.

WAP Binary XML *Wireless*

WAP Binary XML (WBXML), a compact representation of XML, is part of the presentation logic in Wireless Application Protocol (WAP). WBXML significantly improves the efficiency of transmitting XML over narrow bandwidth networks, where data size is of paramount importance.

WAP Forum *Wireless, Organization*

The WAP Forum has been consolidated into the Open Mobile Alliance (OMA) and no longer exists as an independent organization.

WAP Identity Module *Wireless*

WAP Identity Module (WIM) is the security module implemented in the SIM card for WAP applications. WIM provides security services for WAP applications, and allows you to use digital signature. SIM cards with security module are provided by the SIM card issuer.

War Chalking *Security, Wireless*

War chalking refers to marking buildings or sidewalks with chalk to show others where it’s possible to access an exposed company wireless network. These access points are typically found through war driving.

War Dialer *Security*

War Dialer is a computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing *Security*

War Dialing is the process of dialing all the numbers in a range in order to find any machine that answers.

War Driving (Wardriving) *Security, Wireless*

War driving (wardriving) is the process of traveling around looking for wireless access point signals that can be used to get network access. Some computer hackers are content to simply map any open, unsecured WLANs they find. Others have adopted the

X

X Display Manager Control Protocol
Networking, Protocol

X Display Manager Control Protocol (X3T9.5) is isused to communicate between X terminals and workstations running the UNIX operating system.

X.Org Protocol

X Multimedia System
Software

The X Multimedia System (XMMS) is a free audio player very similar to Winamp, that runs on many Unix-like operating systems.

X Protocol
Networking, Protocol

The X Window System Protocol, also known as X Window or X Protocol, is a graphics architecture used as the graphical system on UNIX systems (primarily) and Linux systems. The X Window System is also used, less commonly, on VMS, MVS, and MS-Windows systems. X Window System (X Protocol) provides an inherently client/server-oriented base for displaying windowed graphics. X Window provides a public protocol by which client programs can query and update information on X servers.

X.org Protocol

X Recommendations
Networking

X Recommendations refers to a set of CCITT (now ITU-T) documents that describe data communication network standards. Well-known ones include X.25 Packet Switching standard, X.400 Message Handling System, and X.500 Directory Services.

X Terminal
Networking

X Terminal is an X Windows application that allows a user simultaneous access to several different applications and resources in a multi-vendor environment through the implementation of X Windows. Instead of transmitting vast amounts of X information over the data link, the server software is executed on the host system and eliminates the time-consuming data transfer. Sophisticated data compression techniques and an optimized protocol then send only the minimum amounts of display commands to the terminal. With minimal data being received, the processor and custom graphics engine within these powerful X Terminals are free to concentrate on decompressing drawing commands and maintaining error-free communications.

X Window
Networking, Protocol

The X Window System Protocol, also known as X Window or X Protocol, is a graphics architecture used as the graphical system on UNIX systems (primarily) and Linux systems. The X Window System is also used, less commonly, on VMS, MVS, and MS-Windows systems. X Window System (X Protocol) provides an inherently client/server-oriented base for displaying windowed graphics. X Window provides a public protocol by which client programs can query and update information on X servers.

X.Org Protocol

X Window Display Manager
Software

X Window Display Manager (XDM) is the default display manager for the X Window System. It is a bare-bones X display manager. It was introduced with X11 Release 3 in October, 1988, to support the standalone X terminals that were just coming onto the market. It was written by Keith Packard. Because of its lack of configurability, users of GNOME, KDE or Enlightenment tend to use other managers such as GDM, KDM or Entrance instead of XDM.

X Window System
Networking, Software

X Window System is a distributed, network-transparent, device-independent, multitasking windowing and graphics system originally developed by MIT for communications between X terminals and UNIX workstations. It provides the standard toolkit and protocol to build graphical user interfaces (GUI) on Unix, Unix-like operating systems, and OpenVMS -- almost all modern operating systems support it. X provides the basic framework for a GUI environment: drawing and moving windows on the screen and interacting with a mouse and/or keyboard.

X.121
Networking, Protocol

X.121 is an ITU-T address format of the X.25 protocol suite used as part of call setup to establish a switched virtual circuit between Public Data Networks (PDNs), connecting two network user addresses (NUAs). It consists of just fourteen digits and is sent over the Packet Layer Protocol (PLP) after the packet type identifier (PTI). IP addresses can be mapped to X.121 as described in RFC 1236.

ITU-T Specification: X.121

X.21
Networking, Protocol

X.21 is an ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

ITU-T Specification: X.25

X.21bis
Networking, Protocol

X.21bis is an ITU-T standard that defines the physical layer protocol for communication between DCE and DTE in an X.25 network.

ITU-T Specification: X.25

X.25
Networking, Protocol

X.25, an ISO and ITU-T protocol for wide area network (WAN) communications, is a packet-switched data network protocol which defines the exchange of data as well as the control of information between a user device, called Data Terminal Equipment (DTE), and a network node, called Data Circuit Terminating Equipment (DCE). X.25 specifies LAPB, a data-link-layer protocol, and PLP, a network-layer protocol. Frame Relay has, to some degree,

Y

Y Windows *Software*
The Y Windows, also known as Y Window System, is a windowing system, consisting of a window server and a client library for writing applications, written by Mark Thomas. It is intended to be a successor to the X Window System. It differs from the X Window System in having an integrated widget set and ground-up support for things like an alpha channel, which allows transparent or translucent windows.

Yacc *Software*
See Yet Another Compiler Compiler.

YafRay *Software*
See Yet Another Free Raytracer.

Yagi Antenna *Wireless*
Yagi Antenna is an antenna type that radiates in only a specific direction. Yagi antennas are used only in point-to-point situations.

Yellow Alarm *Telecom*
Yellow alarm, also known as Remote Alarm Indication (RAI), is an indication provided to a source device indicating a signal failure condition at a sink device. An incoming yellow alarm indicates that the T1 network element connected to the T1 interface has a problem with the signal it is receiving from the T1 interface.

Yellow Pages protocol *Networking, Protocol*
The Yellow Pages (YP) protocol, now known as Network Information Service (NIS), is a directory service used for name lookup and general table enumeration. Each YP database consists of key-value pairs, maps, and domains. YP defines a set of key-value pairs as a map. Each map belongs to a domain that is a category of maps. This hierarchy of key-value pairs, maps, and domains provides a generic structure for modeling a database of information. An optional component to a YP server database implementation is the YP binder (YPbind) server. YP uses YP-binder servers to provide addressing information about YP database servers to potential clients.
Sun Protocol

Yersinia *Security*
Yersinia is a tool for performing layer 2 attacks, helping the pen-tester in his daily work checking the robustness of layer 2 protocols configuration. Yersinia can manipulate layer 2 network protocol and allow an attacker foil switches by injecting spurious Spanning Tree Protocol, DHCP, VLAN Trunking protocol and other messages into a network.

Yet Another Compiler Compiler *Software*
Yacc, abbreviated from “Yet Another Compiler Compiler”, is a Unix system tool program for generating C or C++ code for a parser. Yacc is a command-line tool that accepts a grammar description (in a text file) as input and generates the code for a parser for that grammar as output. Parsers are useful in many systems other than just compilers, such as for reading the contents of a configuration file stored in a system’s flash memory. Yacc was developed by Stephen C. Johnson at AT&T for the Unix operating system. Later compatible programs were written, such as Berkeley Yacc, GNU bison, MKS yacc and Abraxas yacc. Each offers slight improvements and additional features over the original Yacc, but the concept has remained the same. Yacc has also been rewritten for other languages, including Ratfor, EFL, ML, Ada, Java, and Limbo.

Yet Another Free Raytracer *Software*
YafRay, abbreviated from “Yet Another Free Raytracer”, is an open source ray tracing program that uses an XML scene description language. It has recently been integrated into, and is often used to render scenes made in, the 3D modelling software Blender.

Ymodem *Networking, Protocol*
YMODEM is a protocol for file transfer used between modems. YMODEM was developed by Chuck Forsberg as the successor to XMODEM and MODEM7. The original YMODEM was essentially the same as XMODEM except that it sent the file’s name, size, and timestamp in a regular XMODEM block before actually transferring the file. Sending the file size solved XMODEM’s problem of superfluous padding at the end of the file.

Ypgrab *Security*
Ypgrab is a tool for extracting password tables from Network Information System (NIS) hosts.

Z

Z88DK *Software*

Z88DK is a Small-C-derived cross compiler for a long list of Z80 based computers. The name is derived from that it was originally developed to target the Cambridge Z88. Z88DK is much developed from Small-C and accepts many features of ANSI C with the notable exception of multi-dimensional arrays and function pointers.

Zap *Security, Software*

Zap is a tool for cleaning log files on UNIX systems.

ZBTSI *Telecom*

See Zero Byte Time Slot Interchange.

ZDO *Wireless*

See ZigBee Device Object.

Zero Byte Time Slot Interchange *Telecom*

Zero Byte Time Slot Interchange (ZBTSI) is a technique used to ensure pulse density for clear channel capability. ZBTSI is applied to a DS1 frame to ensure that pulse density requirements are met, where bits 2 through 193 of each frame are scrambled to minimize the occurrence of all-zero octets.

Zero Code Suppression *Networking*

Zero Code Suppression is a line coding scheme used for transmission clocking. Zero line suppression substitutes a 1 in the 7th bit of a string of eight consecutive zeros.

Zero Day *Security*

See 0-day.

Zero Day *Security*

A zero-day means the first day when a security vulnerability is discovered.

Zero Insertion Force socket *Hardware*

Zero Insertion Force (ZIF) socket is a chip socket that allows one to insert and remove a chip without special tools.

Zero-Day Exploit *Security*

A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. Ordinarily, after someone detects that a software program contains a potential exposure to exploitation by a hacker, that person or company can notify the software company and sometimes the world at large so that actions can be taken to repair the exposure or defend against its exploitation. Given time, the software company can repair and distribute a fix to users.

Zero-Dispersion Slope *Telecom*

Zero-dispersion slope, in a single-mode optical fiber, refers to the rate of change of dispersion, with respect to wavelength, at the fiber's zero-dispersion wavelength.

Zeroization *Security*

Zeroization is the process of removing or eliminating the key from a cryptographic program or device.

ZIF Socket *Hardware*

See Zero Insertion Force socket.

ZigBee *Wireless, Protocol*

ZigBee, defined in the IEEE 802.15.4, is the technology used in the low data rate Wireless Personal Area Network (WPAN) for home control, building automation industrial automation. ZigBee covers up to 330 feet (about 100 meters) in the bandwidth of 20 to 250 kbps.

IEEE Specification: IEEE 802.15.4

ZigBee Device Object *Wireless*

ZigBee Device Object (ZDO), a protocol in the ZigBee protocol stack, is responsible for overall device management, and security keys and policies. The ZDO is like a special application object that is resident on all ZigBee nodes. ZDO has its own profile, known as the ZigBee Device Profile (ZDP), which the application end points and other ZigBee nodes can access.

Zimmermann Telegram *Telecom*

The Zimmermann Telegram was a telegram dispatched by the Foreign Secretary of the German Empire, Arthur Zimmermann, on January 16, 1917, to the German ambassador in Mexico, Heinrich von Eckardt, at the height of World War I. It instructed the ambassador to approach the Mexican government with a proposal to form an alliance against the United States. It was intercepted and decoded by the British and its contents hastened the entry of the United States into the war.

ZIP File Format *Software*

The ZIP file format is a popular data compression and archival format. A ZIP file contains one or more files that have been compressed or stored. The ZIP format was originally designed by Phil Katz for PKZIP. However, many software utilities other than PKZIP itself are now available to create, modify or open ZIP files, notably WinZip, BOMArchiveHelper, PicoZip, Info-ZIP, WinRAR, IZArc and 7-Zip. ZIP files generally use the file extensions ".zip" or ".ZIP" and the MIME media type application/zip.

ZIP Storm *Networking*

ZIP Storm refers to the broadcast storm that occurs when a router running AppleTalk propagates a route for which it currently has no corresponding zone name. The route is then forwarded by downstream routers, and a ZIP storm ensues.

ZipGenius *Software*

ZipGenius is a freeware file archiver designed for Microsoft Windows users, developed by M.Dev Software. It uses, e.g., 7-Zip format, and can also handle a number of other archive formats. It is a freeware product and is presented in two editions: STANDARD and SUITE. While the suite edition includes optional

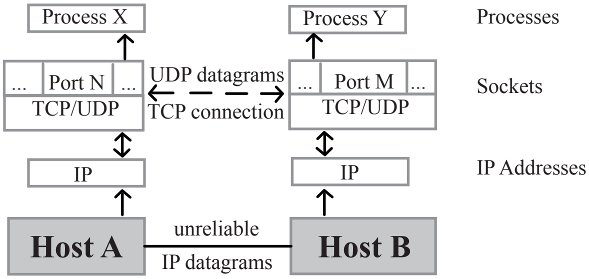
Appendix I
TCP and UDP Port Numbers

TCP and UDP are both transport protocols above the IP layer, which are interfaces between IP and upper-layer processes. TCP and UDP protocol port numbers are designed to distinguish multiple applications running on a single device with one IP address from one another.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine, and to make sure replies get routed to the correct application on the source computer. This is accomplished through the use of the TCP or UDP "port numbers". In the TCP and UDP header, there are "Source Port" and "Destination Port" fields which are used to indicate the message sending process and receiving process identities defined. The combination of the IP address and the port number is called "socket".

There are three port ranges defined by IETF IANA: The Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

- The Well Known Ports are in the range of 0 to 1023, which are assigned by the IANA. In most cases, they can only be used by system (or root) processes or by programs executed by privileged users.
- The Registered Ports are in the range of 1024 to 49151, which are not controlled by IANA. They are commonly used by ordinary user processes or programs executed by ordinary users.
- The Dynamic and/or Private Ports are in the range of 49152 to 65535, which are typically used as source port by a TCP or UDP client, to communicate with a remote TCP or UDP server, using a well-known port as destination port.



Port No.	Protocol	Service Name	Aliases	Comment
1	TCP	tcpmux		TCP Port Service Multiplexer
2	TCP/UDP	compressnet		Management Utility
3	TCP/UPD	compressnet		Compression Process
7	TCP/UDP	echo		Echo
13	TCP/UDP	daytime		Daytime
19	TCP/UDP	chargen	ttytst source	Character generator
20	TCP	ftp-data		File Transfer
21	TCP	ftp		FTP Control
22	TCP	ssh		SSH remote login protocol
23	TCP	telnet		Telnet
25	TCP	smtp	mail	Simple Mail Transfer
37	TCP/UDP	Time		Time
39	UDP	RLP	resource	Resource Location Protocol
42	TCP/UDP	nameserver	name	Host Name Server
43	TCP	nicname	whois	Who Is
49	UDP	TACACS		TACACS: Login Host Protocol
53	TCP/UDP	domain	DNS	Domain Name Server
67	UDP	bootps	dhcps	Bootstrap Protocol Server
68	UDP	bootpc	dhcpc	Bootstrap Protocol Client
69	UDP	TFTP		Trivial File Transfer Protocol
70	TCP	gopher		Gopher
79	TCP/UDP	finger		Finger

80	TCP/UDP	http	www, http	World Wide Web
88	TCP/UDP	kerberos	krb5	Kerberos
101	TCP	hostname	hostnames	NIC Host Name Server
102	TCP	iso-tsap		ISO-TSAP Class 0
107	TCP	rtelnet		Remote Telnet Service
110	TCP	Pop3	postoffice	Post Office Protocol - Version 3
111	TCP/UDP	sunrpc	rpcbind portmap	SUN Remote Procedure Call
113	TCP	Auth	ident tap	Authentication Sevice
117	TCP	Uucp-path		UUCP Path Service
118	TCP	sqlserv		SQL Services
119	TCP	nntp	usenet	Network News Transfer Protocol
123	UDP	Ntp		Network Time Protocol
135	TCP/UDP	epmap	loc-srv	DCE endpoint resolution
137	TCP/UDP	netbios-ns	nbname	NETBIOS Name Service
138	UDP	netbios-dgm	nbdatagram	NETBIOS Datagram Service
139	TCP	netbios-ssn	nbsession	NETBIOS Session Service
143	TCP	Imap	imap4	Internet Message Access Protocol
158	TCP	pcmail-srv	repository	PC Mail Server
161	UDP	snmp	snmp	SNMP
162	UDP	snmptrap	snmp-trap	SNMP TRAP
170	TCP	Print-srv		Network PostScript
179	TCP	BGP		Border Gateway Protocol
194	TCP	irc		Internet Relay Chat Protocol
213	UDP	ipx		IPX over IP
389	TCP	ldap		Lightweight Directory Access Protocol
401	TCP/UDP	UPS		Uninterruptible Power Supply
443	TCP/UDP	https	MCom	Http protocol over TLS/SSL
445	TCP/UDP	CIFS		Microsoft-ds (CIFS)
464	TCP/UDP	kpasswd		Kerberos (v5)
500	UDP	isakmp	ike	Internet Key Exchange (IPSec)
513	TCP	login		Remote Login
513	UDP	who	whod	Database of who’s logged on, average load
514	TCP	cmd	shell	Automatic Authentication
514	UDP	syslog		
515	TCP	printer	spooler	Listens for incoming connections
517	UDP	talk		Establishes TCP Connection
520	TCP	efs		Extended File Name Server
520	UDP	Routing	router routed	RIPv.1, RIPv.2
521	UDP	Routing	router routed	RIPng
525	UDP	Timed	timeserver	Timeserver
526	TCP	Tempo	newdate	Newdate
530	TCP/UDP	Courier	rpc	RPC
531	TCP	conference	chat	IRC Chat

532	TCP	netnews	readnews	Readnews
533	UDP	Netwall		For emergency broadcasts
540	TCP	Uucp	uucpd	Uucpd
543	TCP	Klogin		Kerberos login
544	TCP	Kshell	krcmd	Kerberos remote shell
550	UDP	new-rwho	new-who	New-who
554	UDP	rtsp		Real Time Stream Control Protocol
556	TCP	remotefs	rfs rfs_server	Rfs Server
560	UDP	rmonitor	rmonitord	Rmonitor
561	UDP	monitor		
636	TCP	Ldaps	sldap	LDAP over TLS/SSL
749	TCP/UDP	kerberos-adm		Kerberos administration
750	UDP	Kerberos-iv		Kerberos version IV
1080	TCP/UDP	socks		socks
1812	TCP	RADIUS		RADIUS
1813	TCP	RADIUS		RADIUS accounting

www.javvin.com
Networking technology books, posters and guides, as well as software tools.

www.networkdictionary.com
Free online encyclopedia of computer networking and telecom technologies.

wiki.networkdictionary.com
Open site to share technology knowledge, documents and white papers.

blog.networkdictionary.com
Bring the latest hot topics of the industry to your desk.

Javvin