APPENDIX 303A
IST Term Listing

This glossary of terms is not intended to be a comprehensive list. It focuses primarily on terms that relate to networks, network security, communications, and communication devices used on the Internet. An additional source of definitions can be found at http://whatis.techtarget.com/.

Term **Discussion**

Access Control List
An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Windows NT, Novell's Netware, Digital's OpenVMS, and UNIX-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.

Account Lockout
This feature is available in most current network operating systems. After a specified number of logon attempts, the account is locked out and it usually requires a network administrator to unlock the account.

Administrator Account
This account manages the workstation's user account, policies and resources. This account cannot be locked out or disabled. The Administrator account also controls files owned by other users.

Alpha Test
The first stage of testing a new software product, carried out by the developer's staff.

Anonymous FTP
Using the Internet's File Transfer Protocol (FTP), anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available. If someone tells you to use anonymous FTP and gives you the server name, just remember to use the word "anonymous" for your user ID. Usually, you can enter anything as a password.

API -Application Programming Interface
Software that allows a specific front-end program development platform to communicate with a particular back-end database engine, even when the front end and back end were not built to be compatible.

Applet
An applet is a little application program. Prior to the World Wide Web, the built-in writing and drawing programs that came with Windows were sometimes called "applets." On the Web, using Java, the object-oriented programming language, an applet is a small program that can be sent along with a Web page to a user. Java applets can perform interactive animations, immediate calculations, or other simple tasks without having to send a user request back to the server.

Application
A computer program or set of programs that perform the processing of records for a specific function.

Archie

Archie is a program that allows you to search the files of all the Internet FTP servers that offer anonymous FTP access for a particular search string. Archie is actually an indexing spider that visits each anonymous FTP site, reads the entire directory and file names, and then indexes them in one large index. A user can then query Archie, which checks the query against its index. To use Archie, you can Telnet to a server that you know has Archie on it and then enter Archie search commands. However, it's easier to use a forms interface on the Web called ArchiePlex.

Auditing policies

A critical component of security monitoring controls. Auditing measures the system status against a pre-determined system setting and either will not permit a change or audit and send notifications of the change.

Authentication

The process of proving the claimed identity of an individual user, machine, software component or any other entity.

Bandwidth

The transmission capacity of a computer channel or communications line.

Bastion Host

A computer system that must be highly secured because it is vulnerable to attack, usually because it is exposed to the Internet and is a main point of contact for users of Internal networks. A web page server is an example of a bastion host. It gets its name from the highly fortified projections on the outer walls of medieval castles.

BDC - Back Up Domain Controllers

After a domain has been created, the entire account database is mirrored on each BDC. The PDC (see definition of PDC – primary domain controller) updates a BDC with changes usually at a minimum of every 5 minutes.

Callback security

A feature of remote access servers or software. When a user dials into a remote access facility, the server disconnects the session, and then calls the client back at a preset telephone number or at a number provided during the initial call.

CHAP – Challenge Handshake Authentication Protocol

CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works:

After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it to its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.

Communications Protocol

A convention—a set of rules and procedures—for completing a communications systems task.

Corporate Security Policy

Defines the assets of a corporation, risks to those assets, owners of these assets and how to protect those assets. It includes creating security awareness among employees and having senior management support. It also defines the framework under which the entire corporation treats and reacts to attacks on its resources.

CRC – Cyclic Redundancy Check

An error-checking procedure for data transmission. The sending device performs a complex calculation, generating a number based upon the data being transmitted, and sends that number to the receiving device. The receiving device performs the same calculation after transmission. If the results match, the transmission succeeds. If the numbers don't match, it means the message was received in an altered state, and the data may be incorrect.

De-militarized Zone

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the war in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

Denial of service attack

A denial of service attack is aimed at preventing owners of a computer system from using it. It attempts to prevent the use of a system either by using all available processor resources, memory resources, network resources or by shutting down the system. A typical denial of service attack is to send a flood of e-mail messages to a mail server. If the mail server is inside a critical network, the traffic will either close down or severely slow it down.

DES - Data encryption Standard

A standardized encryption method widely used on the Internet.

Digital certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys.

Digital Signature

A digital signature (not to be confused with a digital certificate) is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Directory Replication

Any process that utilizes directory replication makes an exact copy of a file contents and places it on another server.

DNS – Domain name system

The DNS is a static, hierarchical name service used with TCP/IP hosts, and is housed on a number of servers on the Internet. Basically, it maintains a database for figuring out and finding (or resolving) host names and IP addresses on the Internet. This allows users to specify remote computers by host names rather than numerical IP addresses. The advantage of the DNS is that you don't have to remember numerical IP addresses for all the Internet sites you want to access.

Domain

A group of computers containing domain controllers that share account information and have one centralized accounts database. The four domain models – single domain, complete trust, master domain, and multiple-master domain-represent various stages of growth and decentralization.

Domain controller

Authenticates users and grants them access to other resources within the network.

Encryption

The process of enciphering or encoding data so that it is inaccessible to unauthorized users.

Ethernet

A standard and probably the most popular connection type for LANs. It was first developed by Xerox, and later refined by Digital, Intel and Xerox (see also "DIX"). In an Ethernet configuration, computers are connected by coaxial or twisted-pair cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm.

Event Log

Network operating system services that records system, security, and applications events in the Event Log files.

Event Viewer

A tool used to review logged and audited events. It can be a tool within the operating system or an application designed to do this.

Extranet

The part of a company or organization’s internal computer network that is available to outside users, for example, information services for customers.

Finger

Finger is a program that tells you the name associated with an e-mail address. It may also tell you whether they are currently logged on at their system or their most recent logon session and possibly other information, depending on the data that is maintained about users on that computer. Finger originated as part of BSD UNIX. To finger another Internet user, you need to have the finger program on your computer or you can go to a finger gateway on the Web and enter the e-mail address. The server at the other end must be set up to handle finger requests. A ".plan" file can be created for any user that can be fingered. Commonly, colleges, universities, and large corporations set up a finger facility.

Firewall

A combination of devices and software that form a barrier between a secure network and an open environment. Firewalls examine incoming and outgoing communications on a network and determine if the traffic is permissible. Unauthorized communications are not permitted.

FTP - (file transfer protocol)

FTP is a method of transferring files over any network. It is used extensively over the Internet. Typical FTP servers are established for the purpose of giving open access to information. Critical files should never be installed on an FTP server. FTP servers typically should be placed outside a critical network.

Gopher

Gopher is an Internet application protocol in which hierarchically-organized file structures are maintained on servers that themselves are part of an overall information structure. Gopher provided a way to bring text files from all over the world to a viewer on your computer. Popular for several years, especially in universities, Gopher was a step toward the World Wide Web's Hypertext Transfer Protocol (HTTP). With hypertext links, the Hypertext Markup Language (HTML), and the arrival of a graphical browser, Mosaic, the Web quickly transcended Gopher. Many of the original file structures, especially those in universities, still exist and can be accessed through most Web browsers (because they also support the Gopher protocol). Gopher was developed at the University of Minnesota, whose sports teams are called "the Golden Gophers."

Group accounts

Accounts used for grouping together users who perform the same task or require access to the same resources. Group accounts eliminate the administrative headaches that would be created by granting resources to users on a per user basis.

Groups (Global)

Created on domain controllers and used to assign local permissions to domain users. The sole purpose of a global group is to gather users together at the domain level so that they can be placed in appropriate local groups. (see also local groups).

Groups (Local)

Local groups are defined on each machine and may have both user accounts and global groups as members but cannot contain other local groups.

Guest Account

Typically, this account is built into the operating system. It is designed for one time or occasional users. The problem with guest accounts is that they provide no audit trail or user accountability. They should rarely, if ever, be enabled.

HTML - Hyper Text Markup Language

The language in which World Wide Web documents are formatted. It defines fonts, graphics, hypertext links, and other details.

HTTP - Hypertext Transfer Protocol

The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol.

IMAP – Internet message Access Protocol

A standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail.

Intranet

A private network that uses Internet software (Web browsers, gophers, etc.) and standards (TCP/IP, FTP, HTML, etc.).

IP - Internet Packet

The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.

IPX/SPX

(Internet work Packet Exchange/Sequenced Packet Exchange) Protocol used to connect Novell networks.

ISDN - Integrated Service Digital Network

A communications service that encodes voice, data, facsimile, image, and video communications digitally so that they can be transmitted through a single set of standardized interfaces.

Land Attack

A denial of service attack in which the source and destination SYN (see definition of SYN) packets have the same address and the same port. This attack forces the computer to operate more slowly while trying to respond to packets sent to itself.

Latency

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

Logon scripts

Scripts are used to start applications or send environment variables for specific users or computers upon logon.

Nbstat

Tool used to display the contents of a remote computer's Net BIOS name table. The information listed in the Net BIOS name table can be used to determine the Domain name or workgroup the machine is in and the currently connected users. The information may also be used to uncover the Administrator's account due to the fact that account Station IDS are displayed in the name cache.

Net BIOS

Protocol used when Microsoft networking is required in a large multi-segment network. Net BIOS has many similarities to NetBEUI except for the fact that it can be routed with either the TCP/IP or NWLink protocols in a form known as an encapsulated protocol.

NetBEUI - (Net BIOS Extended User Interface)

The built-in protocol of Microsoft networking supports communication in a Microsoft-only environment when the network is small and composed of a single network segment. NetBEUI is a non-routable protocol, meaning that its packets contain no routing information and cannot pass through routers into other network segments.

Netstat

Tool used to display the status of the TCP/IP stack including what ports are open and what connections are active.

Network DDE

Service that provides a network transport as well as secured for DDE (Dynamic Data Exchange) Conversations.

NOS – Network Operating System

Software that controls the execution of network programs and modules.

NTFS - (New Technology File System)

The file system exclusive to Windows NT 4.0 Utilizes Windows NT File and Directory Security features so it is more secure than the File allocation Table File System (FAT) found in Windows 98, 95 and DOS systems.

Nwlink

Microsoft's implementation of the IPX protocol that allows connectivity between the Windows NT and the Novell NetWare Environment.

OFX - Open Financial Exchange

Open Financial Exchange is a unified specification for the electronic exchange of financial data between financial institutions, business and consumers via the Internet. Open Financial

Exchange, which supports transactional Web sites, thin clients and personal financial software, streamlines the process financial institutions need to connect to multiple customer interfaces, processors and systems integrators. By making it more compelling for financial institutions to implement online financial services, Open Financial Exchange will help accelerate the adoption of online financial services by financial institutions and their customers.

OLE – Object Linking and Embedding

A Microsoft Windows capability in which an object from one application can be referenced from within another application.

OSI - Open Systems Interconnection

Standards for the exchange of information among systems that are "open" to one another by virtue of incorporating International Organization for Standardization (ISO) standards. The OSI reference model segments communications functions into seven layers. Each layer relies on the next lower layer to provide more primitive functions and, in turn, provides services to support the next higher layer.

Out of-Band Attacks

Service attacks where data is sent out the normal expected band that has been shown to affect Windows NT. This attack may cause Windows NT to have trouble handling any network operations.

Packet Filtering

The action a device takes to selectively control the flow of data to and from a network. Pack filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network or vice versa). To accomplish packet filtering, you set up a set of rules that specify what types of packets (for example, those to or from a particular IP address or port) are to be allowed and what types are to be blocked. Packet filtering may occur in a router, in a bridge or on an individual host computer.

PAP – Password Authentication Protocol

One of the many authentication methods that can be used when connecting to an ISP. PAP allows you to login automatically, without having to use a terminal window to type in your username and password. One warning about PAP: passwords are sent over the connection in text format, which means there is no protection if someone is "listening-in" on your connection.

PDC - Primary Domain Controller

The central server in the network that maintains the security database for that domain.

Performance Monitor

Tools configured to monitor system performance in Windows NT. It gathers vital information on system statistics and provides the information graphically. It can also be configured to send alerts when a hacker may be attempting to compromise security.

PING - (Packet InterNet Groper)

A standard TCP/IP network utility that sends packets from one machine to another in order to determine if there is a valid network route between them.

Ping-of- Death 2 attack

A variation on the original Ping-of -Death whereby multiple packets of either greater than 64 K in size or multiple 64 K fragmented packets are sent, crashing the receiving system.

Ping-of-Death attack

A security attack involving Ping. Issuing a Ping pack of larger than normal size set at 64 Kbytes causes the Ping-of-Death. This attack effectively takes the system off-line until it is rebooted.

POP3 – Post Office Protocol 3

The most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail.

Port

On computer and telecommunication devices, a *port* (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. The serial port supports sequential, one bit-at-a-time transmission to peripheral devices such as scanners and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.

2) In programming, a port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, HTTP, have ports with pre-assigned numbers. These are known as "well-known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA). Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number.

Port numbers are from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default and it does not have to be specified in the Uniform Resource Locator (URL).

3) In programming, to port (verb) is to move an application program from an operating system environment in which it was developed to another operating system environment so it can be run there. Porting implies some work, but not nearly as much as redeveloping the program in the new environment. Open standard programming interfaces (such as those specified in X/Open's UNIX 95 C language specification and Sun Microsystems's Java programming language) minimize or eliminate the work required to port a program. Also see portability.

PPP - Point-to-Point Protocol

Enables links between two points with no devices in between.

PPPMP - Point-to-Point Protocol Multilink Protocol.

An Internet standard allowing multiple protocols, such as NETBUI and IPX to be encapsulated within IP data grams and transmitted over public backbones such as the Internet.

PPTP - Point-to Point Tunneling Protocol

A Microsoft protocol under which remote users can connect to corporate networks through secure channels creating connections commonly referred to as Virtual Private Networks (VPNS). There are two implementations of PPTP today. One is a North American version featuring 128-bit encryption and the other is an exportable version with 40-bit encryption. (See also Virtual Private Networks).

Protocols

Languages used by computers. In order for two computers to talk to each other, they must use the same protocol.

Proxy server

A server between a client workstation on a network and the Internet. A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Key cryptography

Public key cryptography consists of a public key and a private key. The public key is given freely to anyone that needs it. The private key is kept secret by the owner of the key and is stored in the user's security file.

Public Key Infrastructure

Public Key Infrastructure (PKI) provides an encryption scheme offering privacy and user authentication. The concept uses a public key accessible by anyone, a private key for decrypting data encoded with your public key, and a pass code to protect your private key. Some experts believe PKI, when implemented properly, is more secure than your own signature.

PVC – Permanent virtual circuit

A software-defined logical connection in a frame relay network. A feature of frame relay, making it a highly flexible network technology is that users (companies or clients of network providers) can define logical connections and required bandwidths between end points and let the frame relay network technology worry about how the physical network is used to achieve the defined connections and manage the traffic.

Query language

A set of commands through which users can update, ask questions, and retrieve data from computer files.

RAID - (Redundant Array of inexpensive disks)

Enables a system to segment data and store pieces of it on several different drives, using a process known as data striping. The principal reason for implementing RAID is for fault tolerance.

RDB – Relational Database

A database in the form of tables which have rows and columns to show the relationships between items, and in which information can be cross-referenced between two or more tables to generate a third table. A query language is used to search for data. If data is changed in one table, it will be changed in all related tables. A database that has only one table is called a flat file database.

Registry

This is the database for windows NT. It contains all the system and program configuration parameters. It also contains the Security Access Manager and configuration data for applications, hardware and device drivers. It also houses data on user-specific profiles, desktop settings, software configurations and network settings.

Remote Access Service

A default service that enables users to connect over a phone line to a network and access resources as if they were at a computer connected directly to the network.

Replication

Creating and maintaining a duplicate copy of a database or file system on a different computer, typically a server. The term usually implies the intelligent copying of parts of the source database which have changed since the last replication with the destination. Replication may be one-way or two-way. Two-way replication is much more complicated because of the possibility that a replicated object may have been updated differently in the two locations in which case some method is needed to reconcile the different versions.

Rlogin

Rlogin is very similar to telnet and is available on many Unix and Non-Unix machines. Rlogin allows you to be on a local machine and to sign on to a remote machine (just like telnet). Rlogin may also require a password to allow system access. However, if it was set up in its default mode, chances are high that a password is not required.

Router

On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

SAM - Security Access Manager

A data base that maintains all user, group, and workstation accounts in a secure database.

Server Alerts

Used to send notification messages to users or computers. Server alerts are generated by the system, and relate to server and resources use. They warn about security and access problems and server shutdown because of power loss when the UPS service is available.

Share

Created by granting a particular resource a share name. This name is what other users or devices recognize as the entity with which they have permission to access. Shares can be set up on files, folders, directors or server services, such as printing.

Share-level security

Used to give other users access to a local hard drive via the network. The four types of share permissions are No Access, Read, Change, and Full Control.

SLIP - serial line Internet Protocol

An older protocol used to carry TCP/IP over low-speed serial lines.

SMB - Server Message Block

Services that form the backbone of Microsoft networking in the Windows NT environment. All file and printer sharing in Windows NT operate using the SMB services.

SMTP – Simple Mail Transfer Protocol

A TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server.

SNMP - Simple Network Management Protocol

An Internet standard for monitoring and configuring network devices. An SNMP network is composed of management systems and agents.

SPAMMING

An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn’t ask for it.

SSL - Secure Sockets Layer

SSL (Secure Sockets Layer) is a program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. Netscape's SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. This standard was offered free to the Internet community and is now widely used as part of the protocol for transmitting confidential data over the Internet.

SYN

A segment used in the start of a TCP connection to enable both devices to exchange information defining characteristics about the session. It is also used to synchronize the target and destination devices.

SYN flood attack

A SYN is a TCP request that can be sent to a server. When a flood of SYN requests are sent to a single server, the server can only respond with a reset to all further connection requests.

System Alerts

Critical security controls that help perform real-time monitoring of system resources, administrator and user activities. Alerts are configured in the network operating system typically the network administrator.

T1

A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T-1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet.

TCP/IP (Transmission Control Protocol/Internet Protocol)

An industry-standard suite of protocols designed for local and wide-area networking. Widely used for Internet communications.

Telnet

The Internet standard protocol to connect to remote terminals. Telnet clients are available for most platforms. When you Telnet to a UNIX site, for example, you can issue commands at the prompt as if you were directly at the machine.

Trojan Horse

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse can be considered a virus if it is widely redistributed. The term comes from Homer's Iliad. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

Trust relationship

A secure communications channel is established between domain controllers. Only servers with proper access rights can send and receive information across this channel. There are two types of trust relationships. The trusting domain which allows another domain to access its resources and the trusted domain-users in the trusted domain can access resources in a trusting domain.

APPENDIX 303A
IST Term Listing

UNIX

A Multitasking Operating System developed in 1969. There are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.

Untrusted Network

Any network in which secure communications have not been established between domain controllers. The largest untrusted network is the Internet.

UPS Uninterruptible power supply

A power system that provides short term power to critical computers so that in the event of a full power outage, the equipment can continue to operate until it can be safely shut down.

VPN - Virtual Private Network

A combination of software and hardware components that use public networks to create what appears to be a private network. A VPN-based remote access connection typically begins with a data connection to an Internet Service Point of Presence Server. From there, the data flows through a VPN session over the Internet (or other IP network) and ends at the corporate network gateway. All of the data that traverses the Internet is encrypted and authenticated providing the necessary security.

WAIS

Wide-area information servers (WAIS) is an Internet system in which specialized subject databases are created at multiple server locations, kept track of by a directory of servers at one location, and made accessible for searching by users with WAIS client programs. The user of WAIS is provided with or obtains a list of distributed databases. The user enters a search argument for a selected database and the client then accesses all the servers on which the database is distributed. The results provide a description of each text that meets the search requirements. The user can then retrieve the full text.

Whois

An Internet program (related to Finger) that lets you enter an Internet entity (such as domains, networks, and hosts) and display information such as a person's company name, address, phone number and email address.