

Anti-Virus / Anti Spam

Antivirus (or "anti-virus") software is a class of program that searches your hard drive and floppy disks for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets.

Anti-Spam software blocks unsolicited commercial email (UCE). Such "junk" email, commonly referred to as "spam," is generally advertising based and sent wide-scale to a mailing list or newsgroup.

Viruses, spam, and other harmful or unwanted content have a significant impact on companies' bandwidth, storage and email processing costs, while also reducing productivity. More than 90% of today's viruses enter networks through email. Most anti-virus solutions only detect 'known' virus through the use of signature files. These solutions provide no protection against new threats that spread rapidly through the Internet. Now both known and unknown viruses and spam can be stopped before it reaches your network through proprietary predictive technology. Anti-virus/anti-spam service acts as your first and strongest line of defense by scanning e-mail and eliminating threats such as viruses, spam, and unwanted content before it reaches its intended destination.

ATM (Asynchronous Transfer Mode)

ATM is a network technology that decreases the number of access lines you need, greatly simplifying technology management.

ATM transfers data in fixed-size cells. Because the cells are always the same size, ATM can transmit various types of data - voice, video, and so on - without any one type blocking the line.

When transferring data, ATM creates a fixed channel between two points. (This is different from TCP/IP, which divides the data into packets, with each packet taking a different route to its destination.) ATM's fixed-channel method can reduce overall costs and make it easier to track data usage across the network.

At the heart of each of IDC Global's network technology solutions is our proprietary ATM (Asynchronous Transfer Mode) Network Fabric. This network fabric is one of IDC Global's key differentiators and is fundamental to the Quality Of Service and high availability provided to IDC Global customers.

Business Continuance

Business continuance (sometimes referred to as *business continuity*) describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.

Although business continuance is important for any enterprise, it may not be practical for any but the largest to maintain full functioning throughout a disaster crisis. According to many experts, the first step in business continuity planning is deciding which of the organization's functions are essential, and apportioning the available budget accordingly. Once the crucial components are identified, failover mechanisms can be put in place. New technologies, such as disk mirroring over the Internet, make it feasible for an organization to maintain up-to-date copies of data in geographically dispersed locations, so that data access can continue uninterrupted if one location is disabled.

According to a recent Gartner Group document, a business continuance plan should include: a disaster recovery plan, which specifies an organization's planned strategies for post-failure procedures; a *business resumption plan*, which specifies a means of maintaining essential

services at the crisis location; a *business recovery plan*, which specifies a means of recovering business functions at an alternate location; and a *contingency plan*, which specifies a means of dealing with external events that can seriously impact the organization. Business continuance has become an increasingly common area of concern since the September 2001 World Trade Center disaster, in which an unforeseen incident created a sudden and severe threat to crucial functions for a number of companies.

CPE (Customer Premise Equipment)

The terminating equipment, such as a router, located at the customer's, or end user's, location connecting the data circuit with the customer's network.

DS1 (T1)

The DS1 (T1) is the most commonly used digital line in the United States. A DS1 is a high-speed data link protocol that has been a standard in the telecommunications industry for more than three decades. A full DS1 transfers data at 1.544 Mbps symmetrically, and is ideal for customers who need a high-speed, reliable connection to the Internet or as one link in their Virtual Private Network (VPN) or Private Wide Area Network.

DS3

A DS3 connection is very similar to a DS1 in that it utilizes the same stable technology, follows a similar provisioning and installation process and is subject to the same in depth management and monitoring from IDC Global. In fact, the biggest difference between a DS1 and a DS3 is the size of the "pipe," or the amount of bandwidth. As stated above, a DS1 transfers data at a rate of 1.544 Mbps. A DS3, in comparison, carries 28 DS1 signals, transferring data at a rate of 45 Mbps. A DS3 is a solution for companies that require larger amounts of highly available, dedicated bandwidth.

DSL (Digital Subscriber Line)

DSL stands for "Digital Subscriber Line," a broadband technology that uses existing telephone lines and digital coding to create a connection to the Internet from your computer. This link can transmit voice, video and data information at very high speeds.

DSL service providers use the same copper-based lines that let you make and receive telephone calls. To send data at high speeds carriers use these copper telephone lines' at higher frequencies to process data vs. voice. DSL modems are hooked up at both ends of a telephone line -- one at the home office or business and the other in the nearest telephone company switching station. The modems digitally divide your telephone line to transfer data over the copper circuit

ADSL: ADSL is a technology used for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides a continuously available, "always on" connection. ADSL is asymmetric in that it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. This recognizes that people tend to be more of a consumer of data than a producer. A slower *upstream* (upload) speed, 384K, is traded off for a faster *downstream* (download) speed, 1.54Kbps. This type of service is generally for those who mainly use the Internet for browsing and e-mail.

SDSL: SDSL, like ADSL, is also a technology used for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Also providing an

"always on" connection, the difference with SDSL is that it is symmetrical. This means that both the upstream and downstream speeds are the same. An individual who signs up for SDSL will have the ability to upload to and download from the Internet at the same speed (192K, 384K, 768K, 1.1M, 1.5M). This type of service is generally for those who require voice or video capabilities in addition to Internet browsing and e-mail.

IDSL: IDSL is available for locations that are too far from the local phone company's central office for either ADSL or SDSL. IDSL is DSL at 144 kbps. IDSL uses ISDN transmission coding, bundling together both ISDN channels on one circuit. IDSL does not use any kind of dial up nor involve per-call fees. IDSL can still be a very satisfactory solution for data transmission compared to alternatives such as a dial-up modem.

Ethernet

Ethernet is the most widely installed local area network (LAN) technology. Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs.

Firewall

A firewall is a set of related programs, located at a network gateway server, which protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Frame Relay

Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and end-points in a wide area network (WAN). Frame Relay protocol places data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission. When an error is detected in a frame, it is simply "dropped" (thrown away). The end points are responsible for detecting and retransmitting dropped frames. However, the incidence of error in digital networks is extraordinarily small relative to analog networks. A Frame Relay network is provisioned through a permanent virtual circuit (PVC), which means that you see a continuous, dedicated connection without having to pay for a higher bandwidth leased line.

Gateway

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

High Availability

In information technology, high availability refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing." A widely-held but difficult-to-achieve standard of availability for a system or product is known as "five 9s" (99.999 percent) availability.

Since a computer system or a network consists of many parts in which all parts usually need to be present in order for the whole to be operational, much planning for high availability centers around backup and failover processing and data storage and access. For storage, a redundant array of independent disks (RAID) is one approach. A more recent approach is the storage area network (SAN).

Some availability experts emphasize that, for any system to be highly available, the parts of a system should be well designed and thoroughly tested before they are used. For example, a new application program that has not been thoroughly tested is likely to become a frequent point-of-breakdown in a production system.

HUB

In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. A hub usually includes a switch of some kind. (And a product that is called a "switch" could usually be considered a hub as well.) The distinction seems to be that the hub is the place where data comes together and the switch is what determines how and where data is forwarded from the place where data comes together. Regarded in its switching aspects, a hub can also include a router.

Intrusion Detection / Intrusion Prevention Systems (IDS/IPS)

Intrusion Detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment/scanning, which is technology developed to assess the security of a computer system or network

Intrusion Prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like intrusion detection systems, an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

IP (Internet Protocol)

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Network

In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

The most common topology or general configurations of networks include the bus, *star*, and Token Ring topologies. Networks can also be characterized in terms of spatial distance as local area networks (LAN), metropolitan area networks (MAN), and wide area networks (WAN).

Network Security

Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.

In a generic sense, security is "freedom from risk or danger." In the context of computer science, security is the prevention of, or protection against, access to information by unauthorized recipients and intentional but unauthorized destruction or alteration of that information.

This can be re-stated: "Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity."

OCx

Optical Carrier levels (OCx) carry higher bandwidths than DS3 and are a set of multiples of the base rate for Synchronous Optical Network (SONET). SONET, the American National Standards Institute's standard for synchronous data transmission on optical media, defines the base rate as 51.84 Mbps, each OCx level being a multiple of this data transfer rate. The following chart shows the varied OCx levels and their associated data transfer rates.

Optical Carrier Level	Data Transfer Rate
OC1	51.84 Mbps
OC3	155.52 Mbps
OC24	1.244 Gbps
OC48	2.488 Gbps
OC192	10Gbps
OC256	13.271 Gbps
OC768	40 Gbps

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. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.

Server

In general, a server is a computer program that provides services to other computer programs in the same or other computers.

The computer that a server program runs in is also frequently referred to as a server (though it may contain a number of server and client programs).

In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a *client* with requests for services from other programs and also as a *server* of requests from other programs.

Specific to the Web, a Web server is the computer program (housed in a computer) that serves requested HTML pages or files. A Web *client* is the requesting program associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers.

Switch

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN), a switch determines, from the physical device (Media Access Control or MAC) address in each incoming message frame, which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines, from the IP address in each packet, which output port to use for the next part of its trip to the intended destination.

Virtual Private Networks (VPN)

A Virtual Private Network (VPN) is a data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a “tunneling” protocol and security procedures. The idea behind a VPN is to provide similar capabilities to that of a private network, at a reduced cost, by using the shared public infrastructure in lieu of a private one. Because virtual private networks make it possible to have similar secure sharing of data through public resources many companies look at using a VPNs for both extranets and wide-area intranets.

Vulnerability

1) Any characteristic of a computer system that allows an individual to keep it from correctly operating, or that will allow unauthorized users take control of the system. 2) A design, administrative, or implementation weakness or flaw in hardware, firmware, or software. If exploited, a vulnerability could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

Vulnerability Management

The practice of identifying and removing weaknesses that can be used to compromise the confidentiality, integrity, or availability of a computer information asset. A vulnerability management is a preventative information security practice that identifies and removes weaknesses before they can be used to compromise a computer information asset.

Vulnerability Scanning/Assessment

The automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws,

testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.