CS610 - Computer Network Glossary By www.virtualians.pk

10Base-T : An IEEE standard (802.3) for operating 10 Mbps Ethernet networks with twisted-pair cabling and a wiring hub, referred to as a 10Base-T hub.

3PC : Third Party Connect Protocol

Analog Data : Data that can have any value in a range and that can change continuously; the time of day represented by clock hands, or the temperature represented by a liquid thermometer are examples of analog data.

APP : Ascend Password Protocol

APP server : The APP Server utility lets users respond to token password challenges received from a remote network access server (NAS). Network access servers offer a complex security algorithm that forces a user to have possession of a security card that can generate a password. When a user on the LAN starts an application that requires a connection to a host on a secure network, the Pipeline initiates the call, and after the initial session negotiation, the remote NAS returns a password challenge. The user has 60 seconds to obtain and enter the current dynamic password from the security card.

ARP (Address Resolution Protocol) : Address Resolution Protocol. This portion of the TCP/IP protocol maps an IP address to the physical address (Ethernet Address) of the PC that it is on, helping to identify PCs on an Ethernet LAN. See also Ethernet, TCP/IP, and proxy ARP.

asynchronous PPP : One of the modes in which the point-to-point protocol is utilized. Asynchronous means that the characters which form data packets are sent at irregular intervals. There is no clocking signal to time transmission. Asynchronous PPP is commonly used in lower-speed transmission and less-expensive transmission systems.

Asynchronous Transmission : A mode in which the sending and receiving serial hosts know where a character begins and ends because each byte is framed with additional bits, called a start bit and a stop bit. A start bit indicates the beginning of a new character; it is always 0 (zero). A stop bit marks the end of the character. It appears after the parity bit, if one is in use.

ATM : Asynchronous Transfer Mode

AUI (Autonomous Unit Interface or Auxiliary Unit Interface) : This refers to the 15-pin D connector and cables that connect single and multiple channel equipment in an Ethernet transceiver.

Authentication : Authentication is a procedure that establishes the legitimacy of users and defines the parameters of the sessions they establish. As such, authentication can be thought of as a security measure that controls and defines network access. It is always the first part of a session; the range of authentication parameters that can be set depend upon the specific authentication system employed.

auto-reconnect : An automatic reconnection of a link that has been lost. The software used to manage the connection notes the lost connection and re-establishes it.

backbone : The part of the communications network intended to and designed to carry the bulk of traffic. Provides connectivity between subnetworks in an enterprise-wide network.

backbone router : Routers designed to be used to construct backbone networks using leased lines. Typically do not have any built-in digital dial-up WAN interfaces. Typical manufacturers include Cisco, Wellfleet, 3Com, CrossCom, and so on.

Bit : Binary digit. The smallest unit of information a computer can process, representing one of two states (usually indicated by "1" and "0").

bridge : A device or setup that connects and passes data, voice, or video between two network segments based on the destination field in the packet header. Ascend units are learning bridges, because they pass all packets to the next network segment (the ISDN line) and build a table identifying the destination addresses that are local and remote. After learning the addresses on both sides of a network, the bridge passes only packets for the remote network. (See router.)

channels : A portion of a line's bandwidth. A line contains a fixed number of channels. Each line can contain switched channels only, nailed-up channels only, or a combination of switched and nailed-up channels. A line can have these types of channels: DS0 - a 64-kbps channel on a line using inband signaling. For information on inband signaling, see the entry for Inband signaling. B channel - a 56-kbps or 64-kbps channel that carries user data on a line using ISDN D-

channel signaling. For information on ISDN D-channel signaling, see the entry for ISDN D-channel signaling. D channel - carries WAN synchronization information on a line using ISDN D-channel signaling. For information on ISDN D-channel signaling, see the entry for ISDN D-channel signalling.

CHAP : Challenge Handshake Authentication Protocol. This security protocol allows access between data communications systems prior to and during data transmission. CHAP uses challenges to verify that a user has access to a system.

codec (COder/DECoder) : A device that encodes analog data into a digital signal for transmission over a digital medium.

CRC : A cyclic redundancy check (CRC) is a non-secure hash function designed to detect accidental changes to raw computer data, and commonly used in digital networks and storage devices such as hard disk drives.

crossover cable : A cable with wires that "cross over," so the terminating ends of the cable have opposite wire assignments. (Contrast with straight-through cable).

DBA (Dynamic Bandwidth Allocation) : Adding or subtracting bandwidth from a switched connection in real time without terminating the link. MPP and AIM support Dynamic Bandwidth Allocation based upon a set of parameters you specify.

DCE (Data Circuit-Terminating Equipment) : As defined in the RS-232 specification, equipment to which DTE (Data Terminal Equipment) is connected, often to enable access to network facilities. A DCE converts the format of the data coming from the DTE into a signal suitable to the communications channel. DCE often refers to equipment such as network access equipment, and DTE refers to application equipment, such as a videoconference terminal.

default gateway : When setting up the PC to operate with a Pipeline, the gateway setting (in the Network settings) must be set to the IP address of the Pipeline. Using the IP address of the Pipeline as the gateway, lets your computer know that you will use the Pipeline to access remote networks.

DHCP (Dynamic Host Configuration Protocol) : DHCP is a standards-based protocol for dynamically allocating and managing IP addresses. DHCP runs between individual computers and a DHCP server to allocate and assign IP addresses to the computers as well as limit the time

for which the computer can use the address. When the time expires on the use of the IP address, the computer must contact the DHCP server again to obtain an address.

DHCP spoofing : There are some cases where the DHCP server is on a remote network, and an IP address is required to access the network, but since the DHCP server supplies the IP address, the requester is at an impasse. To supply access to the network, when the Pipeline receives a DHCP Discover packet (a request for an IP address from a PC on the network), it responds with a DHCP Offer packet containing the configured (spoofed) IP address and a renewal time, which is set to a few seconds. The requester then has access to the DHCP server and gets a real IP address. (Other variations exist in environments where the APP server utility is running.)

digital data : Data that can have only a limited number of separate values. The time of day represented by a digital clock, or the temperature represented by a digital thermometer are examples of digital data; the digital values do not change continuously, but remain at one discrete value and then change to another, discrete value.

DNS (Domain Name System) : A TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a user name and a domain name in the format user name@domain name. The user name corresponds to the host number in the IP address. The domain name corresponds to the network number in the IP address. A symbolic name might be steve@crocker.com or joanne@cal.edu. The domain identifier is the last part of the domain name, and identifies the type of organization to which the host belongs.

domain identifier : The portion of a domain name that appears last and specifies the type of organization to which the host belongs. The Internet's Network Information Center (NIC) provides these domain identifiers

domain name : The portion of a symbolic name that corresponds to the network number in the IP address. In the symbolic name info@vu.edu.pk, the domain name is vu.edu.pk.

filter : A set of rules that define what packets may pass through a network. Filters can use destinations, sources or protocols to determine what to do with packets. One of the packet's headers must contain information that matches the information in the rules or the packet filter will discard it. See also Firewall, Secure Access Firewall, Secure Access Manager.

filtering : One type of filtering transmits a selected range of energy to suppress unwanted frequencies or noise. Another type of filtering removes specific characters received in a data communications channel. Filtering in a network is the assignment of parameters to block transmissions from one LAN to another. See Filter.

firewall : A hardware/software tool that allows a network administrator to determine what type of users can access the resources on the network. The firewall provides a mechanism to monitor and funnel data from authorized users (only) through the firewall to and from the network. A firewall may be a software program that runs on a UNIX or other platforms or it may be a part of a proprietary operating system. A firewall by itself does not perform the routing function. See also Filter, Secure Access Firewall, Secure Access Manager.

FR (Frame Relay) : A form of packet switching, but using smaller packets and less error checking than traditional forms of packet switching (such as X.25). Now a new international standard for efficiently handling high-speed, bursty data over wide area networks.

host : A computer on a network.

hybrid LAN : A hybrid network is one in which some links are capable of sending and receiving only analog signals while others handle digital signals only. Another definition is the division of a network into public and private sections.