10BaseT – Ethernet specification for unshielded twisted pair cable (category 3, 4, or 5), transmits signals at 10 Mbps (megabits per second) with a distance limit of 100 meters per segment.

100BaseT – Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 100 Mbps (megabits per second) with a distance limit of 100 meters per segment.

1000BaseTX – Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 1 Gbps (gigabits per second) with a distance limitation of 220 meters per segment.

Access List – is kept by routers to control access to or from the router for a number of services. For example, the list can prevent packets with a certain IP address from leaving a particular interface on the router.

Access Point (AP) – is a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.

ARP (Address Resolution Protocol) – is a portion of the TCP/IP protocol that maps an IP address to the physical address (Ethernet Address) of the device that it is on, helping to identify devices on an Ethernet LAN.

Asynchronous PPP – is 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 – is 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) – is a broadband transmission system using 53-octet packets over a cell-switched network at speeds up to 2.2 GBPS.

Authentication – is a procedure that establishes the legitimacy of users and machines and defines the parameters of the sessions they establish. It is 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.

Authorization – is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular.

B channel – is a 56-kbps or 64-kbps channel that carries user data on a line using ISDN D-channel signaling.

Backbone – is the part of the communications network intended to and designed to carry the bulk of traffic. It provides connectivity between subnetworks in an enterprise-wide network.

Backplane – is the communication channels of a single device's architecture, such as in a hub, switch or concentrator.

BGP (Border Gateway Protocol) – is an interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined by multiple RFCs. BGP Version 4 is the predominant interdomain routing protocol used on the Internet. BGP4 supports CIDR and uses route aggregation mechanisms to reduce the size of routing tables.

BRI (Basic Rate Interface)-- is an ISDN subscriber line, consisting of two 64 kbit/s B channels, or "bearer" channels, and one 16 kbit/s D channel, used for both data and signaling purposes.

Bridging – network bridging describes the action taken by network equipment to allow two or more communication networks or segments to create an aggregate network within the same subnetwork. It operates primarily on OSI layer 2. As a comparison, routing operation at layer 3 and connects separate networks.

Bridge table – identifies destination addresses known to exist in a network. It is built dynamically by a learning bridge as it passes data in a network.

Bridging vs. Routing – Bridging is the process of passing packets to another network segment without regard to the network operating system. Bridged packets are passed to the data link layer (layer 2) of the OSI model, as opposed to routed packets, which are delivered to the network layer (layer 3). In an environment where diverse network operating systems exist, a bridge can move data between the networks, but cannot deliver packets all the way up through the network. Routing delivers packets to discreet IP addresses in the network.

Broadcast Domain – is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by VLANs or routers because routers do not forward broadcast frames.

Broadcast Storm – is an undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Category 5 cabling – is one of five grades of UTP cabling described in the EIA/TIA-586 standard. Category 5 cabling can transmit data at speeds at 100 Mbps, 1 Gbps and higher. Compare with Category 1 cabling, Category 2 cabling, Category 3 cabling, and Category 4 cabling.

Channels – is a portion of a telephony 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 in-band signaling.
- B channel - a 56-kbps or 64-kbps channel that carries user data on a line using ISDN D-channel signaling.
- D channel - carries WAN synchronization information on a line using ISDN D-channel signaling.

CHAP (Challenge Handshake Authentication Protocol) – is a security protocol that 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.

CIDR (Classless InterDomain Routing) – is a technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes together in order to cut down on the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity.

Circuit – is a connection between endpoints over a physical medium.

Circuit-level Inverse Multiplexing – is a method of inverse multiplexing in which the inverse mux slices the data stream into equal portions, and transmits each portion over an available circuit. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order.

COS (Class of Service) – is an indication of how an upper-layer protocol requires that a lower-layer protocol treat its messages. COS definitions are used by subarea nodes to determine the optimal route to establish to given session. A COS definition comprises a virtual route number and a transmission priority field. It is also called TOS (type of service).

CO (Central Office) – is the local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.

Codec (COder/DECoder) – is a device that encodes analog data into a digital signal for transmission over a digital medium.

CPE (Customer Premises Equipment) – is terminal equipment located on the customer premises which connects to the telephone network.

CSMA/CD (Carrier Sense Multiple Access Collision Detect) – is a media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. CSMA/CD access is used by Ethernet and IEEE 802.3.

CSU (Channel Service Unit) – is a device used to connect a digital phone line coming in from the phone company to network access equipment located on the customer premises. A CSU may also be built into the network interface of the network access equipment.

D channel – is a channel that carries WAN synchronization information on a line using ISDN D-channel signaling.

Data Encryption – is accomplished by applying a special scrambling code that makes the data unreadable to anyone who does not have a decryption key. The message or information (plaintext) is encrypted using an encryption algorithm, turning it into unreadable information (ciphertext.) This is done with an encryption key. Authorized personnel with access to this key can unscramble it.

Data Link Layer – is Layer 2 of the OSI reference model. This layer provides reliable transit of data across a physical link. The data link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE has divided this layer into two sublayers: the MAC sublayer and the LLC sublayer.

DCE (Data Circuit-Terminating Equipment) – 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.

DHCP (Dynamic Host Configuration Protocol) – 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 Option 82 – is the DHCP Relay Agent Information Option. It allows a DHCP Relay Agent to insert circuit specific information into a request that is being forwarded to a DHCP server. It is used mainly to assign the same IP address to the same computing device.

DHCP Relay – allows DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers. DHCP relay agents are installed on these subnets and forward DHCP information.

DVMRP (Distance Vector Multicast Routing Protocol) – is an internetwork gateway protocol, largely based on RIP, that implements a typical dense mode IP multicast scheme. DVMRP uses IGMP to exchange routing datagrams with its neighbors.

DNS (Domain Name System) – is 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. DNS maintains a database of network numbers and corresponding domain names. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the user name corresponding to the host number.

DTE (Data Terminal Equipment) – is equipment to which DCE (Data Communications Equipment) is connected, such as personal computers or data terminals. DTE often refers to application equipment, such as a videoconference terminal or LAN bridge or router, while DCE refers to equipment such as network access equipment.

Dual Homing – is a network topology in which a device is connected to the network by way of two independent access points (points of attachment). One access point is the primary connection, and the other is a standby connection that is activated in the event of a failure of the primary connection.

E1 PRI line – is an ISDN line that consists of 32 64 kbps channels. This type of line uses 30 B channels for user data, 1 64 kbps D channel for ISDN D-channel signaling, and one framing channel. The B channels can be all switched, all nailed up, or a combination of switched and nailed up.

Encapsulation – is the process of placing one protocol inside of another. Usually implies that the encapsulated protocol was not originally intended by its designers to be carried by the encapsulating protocol.

Ethernet – is a local area network specification for a transmission system including Layers 1 and 2 of the OSI 7-layer model using the CSMA/CD access method. It operates over copper, coaxial, fiber, wireless at speeds from 10 Mbps to multi-Gbps rates.

Fast Ethernet – is an Ethernet standard that supports 100 Mbps using category 5 twisted pair or fiber optic cable.

Fiber Optic Cable – is a cable, consisting of a center glass core surrounded by layers of plastic that transmits data using light rather than electricity. It has the ability to carry more information over much longer distances.

- Multi-mode -- is a type of optical fiber mostly used for communication over short distances
- Single-mode is an optical fiber designed to carry only a single ray of light (mode) over long distances

Filter – is 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.

Firewall – is 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, part of a proprietary operating system, purpose built device or network appliance. A firewall by itself does not perform the routing function.

Frame Relay – is a form of packet switching, but using smaller packets and less error checking than traditional forms of packet switching (such as X.25). It is an international standard for efficiently handling high-speed, bursty data over wide area networks at fees less than traditional leased lines.

Fractional T1 line – is a communication line that contains both switched and nailed-up channels. T1 PRI and ISDN BRI lines can also be fractional T1 lines.

Framing – at the physical and data link layers of the OSI model, bits are fit into units called frames. Frames contain source and destination information, flags to designate the start and end of the frame, plus information about the integrity of the frame. All other information, such as network protocols, and the actual payload of data, is encapsulated in a packet, which is encapsulated in the frame.

FTP (File Transfer Protocol) – is standard method of point-to-point transfer of text and binary files between IP connected hosts.

Gateway – is a point of entrance to and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture. In OSI terms, a gateway is a device that provides mapping at all seven layers of the OSI model. A gateway can be thought of as a function within a system that enables communications with the outside world.

Gigabit Ethernet – is an Ethernet protocol that transmits at 1 Gbps (gigabits per second) over copper, Coax and fiber.

HDLC (High-level Data Link Control) – is a synchronous, bit-oriented Link Layer protocol for data transmission. Frame Relay is an example of an HDLC-based packet protocol.

Host – is a computer on a network.

HSRP (Hot Standby Router Protocol) – provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of the standby routers inherits the lead position and the Hot Standby group address.

Hub – is a hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat but merely split signals sent through them).

ICMP (Internet Control Message Protocol) – is an error reporting mechanism that is an integral part of the IP suite. Gateways and hosts use ICMP to send reports of datagram problems back to the sender. ICMP also includes an echo request/reply function that tests whether a destination is reachable and responding. Ping is a type of ICMP.

IDRP (Inter-Domain Routing Protocol) – dynamically exchanges policies between autonomous systems. IDPR encapsulates inter-autonomous system traffic and routes it according to the policies of each autonomous system along the path.

IEEE (Institute of Electrical and Electronics Engineers) – is a professional association dedicated to advancing technological innovation.

IEEE 802.1 – is a specification that describes an algorithm that prevents bridging loops by creating a spanning tree.

IEEE 802.1X – port-based network access is a standard designed to enhance 802.11 WLAN security as well as switch access. 802.1X provides an authentication framework, allowing a user to be authenticated by a central authority.

IEEE 802.3 – is a LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet and gigabit Ethernet

IEEE 802.3af – is a Power over Ethernet (PoE) standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

IEEE 802.3at – is a Power over Ethernet standard also known as **PoE+** or **PoE plus**, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power. Some vendors have announced products that claim to be compatible with the 802.3at standard and offer up to 51 W of power over a single cable by utilizing all four pairs in the Category 5 cable.

IEEE 802.11a – provides specifications for wireless ATM systems. 802.11a is also used in wireless hubs. Networks using 802.11a operate at radio frequencies between 5.725 GHz and 5.850 GHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings.

IEEE 802.11b – is a WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference.

IEEE 802.11g – offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

IEEE 802.11n – was designed to improve network throughput over 802.11a and 802.11g with a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s with the use of four spatial streams at a channel width of 40 MHz. 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements.

IETF (Internet Engineering Task Force) – is an international organization whose purpose is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. It consists dozens of working groups responsible for developing Internet standards.

IGMP (Internet Group Management Protocol) – is used by IP hosts to report their multicast group memberships to an adjacent multicast router.

IRDP (ICMP Router Discover Protocol) – enables a host to determine the address of a router that it can use as a default gateway.

IGP (Interior Gateway Protocol) – used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

In-band Signaling – is a type of signaling in which a line uses 8 kbps of each 64 kbps channel for WAN synchronization and signaling. The remaining 56 kbps handle the transmission of user data. Another term for in-band signaling is robbed-bit signaling. Robbed-bit refers to the 8 kbps of each channel used for signaling. T1 access lines containing one or more switched channels, and Switched-56 lines use in-band signaling.

Inverse ARP (Inverse Address Resolution Protocol) – is a method of building dynamic routes in a network. It allows an access server to discover the network address of a device associated with a virtual circuit.

Intranet – is a network internal to an organization that uses Internet protocols.

Internet – is the global network of networks used to exchange information using the TCP/IP protocol. It allows for electronic mail and the accessing ad retrieval of information from remote sources.

Interoperability – interoperable devices are compatible with the devices and services of multiple vendors, and can be integrated into a generic network containing a wide range of vendor products. Interoperability is a significant factor among expansion considerations, since any device must have the versatility to function in an expanding network structure. The technical elements of interoperability may include a bundle of protocols and a flexible architecture to accommodate upgrades.

Inverse Multiplexing – an inverse mux is an electronic device that enables two or more signals to pass over a single communications circuit, whether analog or digital. It allows individually dialed channels across a network to be combined into a single, higher-speed data stream. Each end of the connection uses an inverse mux.

IP (Internet Protocol) – is the Network Layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP Address – is an address that uniquely identifies each host on a network or internet.

> An IP address has a length of 32 bits, and is divided into four 8-bit parts, each separated by a period, as in 149.122.3.30. This kind of notation is called dotted decimal notation. Each part can consist of a number between 1 and 255.
>
> An IP address consists of a network number and a host number. IP addresses come in three types: Class A, Class B, and Class C. The class of an IP address determines which portion of the address belongs to the network number and which portion belongs to the host number. The first bits of the IP address identify the class. The Internet's Network Information Center (NIC) determines the type of class assigned a network.
>
> A Class A address starts with 0 as the class identifier, followed by 7 bits for the network number and 24 bits for the host number. Therefore, the first number in dotted decimal form is the network number; the next three numbers make up the host number. For example, in the IP address 127.120.3.8, the network number is 127 and the host

number is 120.3.8. This type of address is used by the largest organizations, because this scheme allows for over 16 million different host numbers. However, it also limits network numbers to a total of 128.

A Class B address starts with binary 10 as the class identifier, followed by 14 bits for the network number and 16 bits for the host number. Therefore, the first two dotted decimal numbers comprise the network number, and the second two dotted decimal numbers comprise the host number. For example, in the IP address147.14.86.24, the network number is 147.14 and the host number is 86.24. More network numbers are available, but fewer hosts (approximately 65,000).

A Class C address starts with binary 110 as the class identifier, followed by 21 bits for the network number and 9 bits for the host number. Therefore, the first three dotted decimal numbers comprise the network number, and the last dotted decimal number comprises the host number. For example, in the IP address 225.135.38.42, the network number is 225.135.38 and the host number is 42. Many network numbers are available, but only 254 hosts per network number. The numbers 0 and 255 are reserved.

You can tell the type of class an IP address falls into by looking at the first 8-bit portion of the dotted decimal form of the address. Class A addresses begin with a number between 0 and 127. Class B addresses begin with a number between 128 and 223. Class C addresses begin with a number between 192 and 233.

A Class D address is a group of IP addresses from 224.0.0.0 to 239.255.255.255 and is used for multicast routing.

In addition to an IP address, you can use a symbolic name provided by Domain Name Services (DNS) to designate an Internet address.

IP Filters – examine a TCP/IP/UDP data packets' source addresses, destination addresses, IP protocol type, port, or any combination.

IP Multicast – is a routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address.

IPSec (Internet Protocol Security) – is a technology protocol suite for securing IP communications by authenticating and/or encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IP Subnet – is a way to subdivide a network into smaller networks, so you can have a greater number of computers on a network with a single IP address. The IP subnet is a number that you append to the IP address. For example, 195.112.56.75/14, 195.112.56.75/15, and 195.112.56.75/16 are all IP addresses with subnets of 14, 15, and 16.

IPCP (Internet Protocol Control Protocol) – is responsible for configuring, enabling and disabling the IP protocol modules on both ends of a point-to-point link. The IPCP is tied to PPP, and is activated only when PPP reaches the network layer protocol phase. If IPCP packets are received prior to this phase, they should be discarded. Elements of IPCP include packet encapsulation, code fields and timeouts.

ISDN (Integrated Services Digital Network) – is a system that provides simultaneous voice and high-speed data transmission through a single channel to the user's premises. ISDN is an international standard for end-to-end digital transmission of voice, data, and signaling.

ISDN BRI line – is the Basic Rate Interface line that uses two B channels for user data, and one 16-kbps D channel for ISDN D-channel signaling. Both B channels can be switched, both channels can be nailed up, or one channel can be switched and the other nailed up. A line of this type can connect to standard voice service, Switched-56 data service, or Switched-64 data service.

ISDN D-channel Signaling – is a type of signaling in which a D channel handles WAN synchronization and signaling, and the B channels carry the user data. Another term for ISDN D-channel signaling is out-of-band signaling. T1 PRI, E1 PRI, and ISDN BRI lines use ISDN D-channel signaling.

ISP (Internet Service Provider) – is a company that provides access to the Internet. By establishing Points of Presence (POPs) containing remote access servers and additional devices, as well as a suite of user software packages, the Internet Service Provider acts as a commercial Internet on-ramp. Providers typically charge a monthly fee and supply technical support and advice to customers.

IXC (Interexchange Carrier) – is a legal and regulatory term for a telecommunications company, commonly called a long-distance telephone company.

Jumbo Frames – are Ethernet frames with more than 1500 bytes (the standard) of payload. Conventionally, jumbo frames can carry up to 9000 bytes of payload.

LAN (Local Area Network) – is a network that interconnects devices over a geographically small area, typically in one building or a part of a building. The most popular LAN type is Ethernet, a 10 Mbps standard that works with 10BaseT, 10Base2, or 10Base5 cables. When you interconnect a single computer to the Pipeline with the crossover cable in your package, you are creating a two-node Ethernet network.

LAN Switch – a device that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches are often categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multilayer switches are an intelligent subset of LAN switches. Compare with multilayer switch.

Layer – is a term used to describe a group of communication functions and the protocols implemented to perform them as defined by a network standards organization, most often referring to a group of functions as described by the OSI 7-Layer Model designated by the ISO.

Leased Line – is a circuit rented for exclusive use twenty-four hours a day, seven days a week from a telephone company. The connection exists between two predetermined points and cannot be switched to other locations.

LEC (Local Exchange Carrier) – is a regulatory term in telecommunications for the local telephone company.

Link Aggregation – is a general term to describe various methods of combining multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails. It is also referred to as trunking.

Link State Routing – is a routing protocol that takes link loading and bandwidth when selecting between alternate routes.

LLC (Logical Link Control) – is a data communication protocol layer is the upper sublayer of the data link layer (layer 2). It provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and to be transported over the same network medium. It can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

Load Balancing – in routing, the ability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the utilization of network segments, thus increasing effective network bandwidth.

MAC (Media Access Control) – is a sublayer of the data link layer (layer 2). The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

MAC Address – standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. It is also known as a hardware address, a MAC-layer address, or a physical address.

Mesh – is a network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections strategically placed between network nodes.

MIB (Management Information Base) – is an SNMP specification of the data objects and data structures that the Agent is responsible for knowing and reporting to the Console on demand.

Modem (MOdulator/DEModulator) – takes digital data from a DTE, translates (or modulates) the 1s and 0s into analog form, and sends the data over the channel. The receiving modem demodulates the analog signal into digital data and sends it to the DTE to which it is attached.

MP (Multilink PPP) – is a standard for inverse multiplexing, a method of combining individually dialed channels into a single, higher-speed data stream. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

MPP (Multichannel Point-to-Point Protocol) – A protocol that extends the capabilities of MP to support inverse multiplexing, session management, and bandwidth management. MPP allows you to combine up to 30 individual channels into a single high-speed connection.

MTU (Maximum Transfer Unit) – is the size (in bytes) of the largest protocol data unit that the layer can pass onwards.

Multicast – is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source.

Multicast Group – is a dynamically determined group of IP hosts identified by a single IP multicast address.

Multicast Router – is a router that sends IGMP query messages on their attached local networks. Host members of a multicast group respond to a query by sending IGMP reports noting the multicast groups to which they belong. The multicast router takes responsibility for forwarding multicast datagrams from one multicast group to all other networks that have members in the group.

MOSPF (Multicast OSPF) – is an intradomain multicast routing protocol used in OSPF networks. Extensions are applied to the base OSPF unicast protocol to support IP multicast routing.

Network Address Translation (NAT) – is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.

Network Layer – is layer 3 of the OSI reference model. This layer provides connectivity and path selection between two end systems. The network layer is the layer at which routing occurs.

NMS (Network Management System) – is responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

OSI (Open Systems Interconnection) – is a reference model used to describe layers of a network and the types of functions expected at each layer. The OSI model is used as a standard, letting developers of networks and communication systems rely on the presence of certain functions at certain places in a standard system. Top to bottom, the seven layers are:

- application
- presentation
- session
- transport

- network
- data link
- physical

The physical and data link layers have to do with hardware, wires, signals on wires, and basic addressing functions, such as media access control (MAC). In the network layer, information from different networking protocols is distinguished, which is where the internet protocol (IP) functions. In the transport layer, data is packaged for transport in a size and organization appropriate for its intended environment. This is where transport control protocol (TCP) works. The session, presentation, and application layers keep information streaming in and convert it to a usable format.

OSPF (Open Shortest Path First) – is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks.

PAP (Password Authentication Protocol) – is a security protocol that uses password protection to allow access to a network or host.

PBX (Private Branch Exchange) – is an internal telephone network, such as those used in large offices, in which one incoming number directs calls to various extensions and from one office to another.

Ping – is the command invoked on many systems to send ICMP echo requests. Ping has several versions. The most sophisticated Pings send a series of ICMP echo requests, capture responses, and corollary statistics regarding data packet loss. The user can determine the length of the ICMP request and designate an interval between tries.

POP (Point of Presence) – is access to an Internet service provider used to facilitate remote users' access to the range of applications and IP addresses in the internetwork.

PPP (Point-to-Point Protocol) – provides a standard means of encapsulating data packets sent over a single-channel WAN link. It is the standard WAN encapsulation protocol for the interoperability of bridges and routers. PPP is also supported in workstations, allowing direct dial-up access from a personal computer to a corporate LAN or ISP. Using PPP ensures basic compatibility with non-Ascend devices. Both the dialing side and the answering side of the link must support PPP.

PoE (Power-over-Ethernet) – is a means for delivering power to a remote device using the same cable lines used to deliver Ethernet data.

PoE Power Sourcing Equipment (PSE) – is a device such as a switch that provides or sources power on the Ethernet cable.

PoE Powered device (PD) – is a device powered by a PSE and consumes energy.

PRI (Primary Rate Interface) – is an ISDN service over a T1 link that provides 23 data channels "bearer" or "b" Channels" at 64 KBPS and one 16 KBPS control channel (or "D" channel).

Protocol – is a set of rules governing message exchange over a network or internetwork. An example of commonly used protocols are the TCP/IP (Transmission Control Protocol/Internet Protocol) suite.

PIM (Protocol-Independent Multicast) – is a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It does not include its own topology discovery mechanism, using routing information supplied by other traditional routing protocols such as OSPF, RIP and BGP. There are four variants of PIM:

- PIM Sparse Mode (PIM-SM)
- PIM Dense Mode (PIM-DM)
- Bidirectional PIM
- PIM Source-Specific Multicast (PIM-SSM)

Proxy ARP – is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network

Quality of Service (QoS) – refers to several related aspects of telephony and computer networks that allow the transport of traffic with special requirements including prioroties. QoS may agree on a traffic contract with the application software and reserve capacity in the network nodes

RADIUS (Remote Access DIalup User Service) – is a protocol by which users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, dialback, SLIP, and PPP.

Resource Reservation Protocol (RSVP) – is a Transport Layer protocol designed to reserve resources across a network for an integrated services Internet.

Repeater – is a device used in a network to strengthen a signal as it is passed along the network cable.

RARP (Reverse Address Resolution Protocol) – is a method for devices to ask a server for their IP address during bootstrap operations.

RFC (Request For Comments) – is an IETF document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs. The RFC series of documents is unusual in that the proposed protocols are forwarded by the Internet research and development community, acting on their own behalf, as opposed to the formally reviewed and standardized protocols that are promoted by organizations such as CCITT and ANSI. A complete list of RFCs can be found at http://www.internic.net/rfc/.

RIP (Routing Information Protocol) – teaches routers on a wide area network which routers have access to which addresses. This information is kept in a routing table on each router. As routers communicate with each other, they all update their routing tables to include each others' routing table information. In a large network environment, this exchange of information can keep the network connections up unnecessarily, and can result in very large routing tables on each router. You can apply a call filter to ignore RIP updates. You can also control how route information is propagated.

Router – is an interconnection device that can connect individual LANs. Unlike bridges, which logically connect at OSI layer 2, routers provide logical paths at OSI layer 3. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Routing – is a device or setup that finds the best route between any two networks, even if there are several networks to traverse. (Contrast with bridge).

Routing Table – is a list of destinations known to the router. Routing tables are built and used statically or dynamically via RIP and OSFP.

Serial Communication – is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus

SLIP (Serial Line IP) – is a protocol that enables a computer to send and receive IP packets over a serial link.

SMDS (Switched Multimegabit Data Service) – is a packet-based network service allowing the creation of high-speed data networks (up to 45 Mbit/s).

SMTP (Simple Mail Transfer Protocol) – is the standard protocol for exchanging mail over TCP/IP networks.

SNMP (Simple Network Management Protocol) – is a standard way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB). An agent can use a message called a traps-PDU to send unsolicited information to the manager. SNMP security is implemented using the community name sent with each request.

Star Topology – is a LAN topology in which each node on a network is connected directly to a central network hub or concentrator.

Star-Wired Ring – is a network topology that connects network devices (such as computers and printers) in a complete circle.

Subnet Mask and Subnetting – a mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

Switch – is an intelligent type of hub, in that it sends packets only to the intended ports, rather than all computers on the network.

Switched Circuit – is temporary connection between endpoints, established for the duration of a call, over which two parties exchange data. The circuit is disconnected when the call ends.

Synchronous Transmission – is a transmission mode in which the data moves in large blocks, called messages or frames. Both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins. Synchronization can take one of these forms: Each side can transmit a separate synchronizing signal, called a clock; each frame or message can contain synchronization information; in the latter method, each block of data starts with one or more control characters, usually eight bytes long, called a SYNC. The receiver interprets the SYNC as a signal that it can start accepting data. Synchronous transmission can be up to 20 percent faster than asynchronous transmission.

T1 Access Line – is a 1.544 mbps T1 line that provides 24 56 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 line – is a line that consists of 24 64 kbps channels. Two types of T1 lines are available: T1 access lines and T1 PRI lines.

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 signaling. The B channels can be all switched, all nailed up, or a combination of switched and nailed up. This type of PRI line is a standard in North America, Japan, and Korea. PRI stands for Primary Rate Interface. You can connect this type of line to standard voice, or Switched-56, Switched-64, Switched-384, Switched-1536, and MultiRate data services.

T3 – is a digital transmission link with a capacity of 45 Mbit/s, or 28 T1 lines.

TACACS (Terminal Access Concentrator Access Control Server) – is a simple query/response protocol that enables the devices to check a user's password, and enable or prevent access. A TACACS server supports only the basic password exchanges that PAP uses; it does not support CHAP.

TCP/IP (Transmission Control Protocol/Internet Protocol) – is a family of protocols that defines the format of data packets sent across a network, and is the communications standard for data transmission between different platforms. The TCP/IP family consists of the following protocols and services.

Transport Protocols - these protocols control data transmission between computers:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- Routing protocols - these protocols control addressing and packet assembly, and determine the best route for a packet to take to arrive at its destination:
- IP (Internet Protocol)

- ICMP (Internet Control Message Protocol)
- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- Gateway protocols - these protocols enable networks to share routing and status information:
- EGP (Exterior Gateway Protocol)
- GGP (Gateway-to-Gateway Protocol)
- IGP (Interior Gateway Protocol)

Network address services and protocols - these services and protocols handle the way that each computer on a network is identified:

- DNS (Domain Name System)
- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- User services - these services provide applications a computer can use:
- BOOTP (Boot Protocol)
- FTP (File Transfer Protocol)
- Telnet
- Miscellaneous services
- NFS (Network File System)
- NIS (Network Information Service)
- RPC (Remote Procedure Call)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- Telnet -- Terminal-to-remote host protocol governing the exchange of character-oriented terminal data. This protocol is used to link two computers in order to provide a terminal connection to the remote machine. Instead of dialing into the computer, you connect to it over the Internet using Telnet. When you issue a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were a terminal connected to it.

Topology (Physical and Logical) – The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information between workstations. Issues involving logical topologies are discussed on the Protocol chapter

Unicast – is the transmission of messages to a single network destination identified by a unique address.

The information at hand is provided as available at the time of printing. Beijer Electronics reserves the right to change any information without updating this publication. Beijer Electronics does not assume any responsibility for any errors or omissions in this publication.

UDP (User Datagram Protocol) – is one of the core members of the Internet protocol suite allowing computer applications to send *datagrams* to other hosts on an IP network without prior communications to set up special transmission channels or data paths.

UTP (Unshielded Twisted Pair) – is a cable with two pair of wires twisted two or more times per inch to help cancel out noise.

VLAN (Virtual LAN) – is a broadcast domain created by switches. Networks are subdivided into multiple VLANs by switch ports, MACs address, etc. to control broadcast domains.

Virtual Private Network (VPN) – is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP) and IPSec. Data is encrypted at the sending end and decrypted at the receiving end.

Virtual Router Redundancy Protocol (**VRRP**) – is a computer networking protocol that provides for automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

WAN (Wide Area Network) – is a data network typically extending a LAN outside a building or beyond a campus, over IXC or LEC lines to link to other LANs at remote sites. Typically, created by using bridges or routers to connect geographically separated LANs.

Wi-Fi (Wireless Fidelity) – is a term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard.

The information at hand is provided as available at the time of printing. Beijer Electronics reserves the right to change any information without updating this publication. Beijer Electronics does not assume any responsibility for any errors or omissions in this publication.