

**Angle**

The field of view, relative to a standard lens within a 35mm still camera, expressed in degrees, e.g. 30°. Practically, this is the area of a scene that a lens covers or sees; where, the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than a normal or telephoto lens with a longer focal length.

**API**

Application Programming Interface.

**ARP**

Address Resolution Protocol. This is the protocol used for mapping an Internet Protocol address (IP address) to a physical machine address that is recognizable to the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. Here is how ARP works:

When an incoming packet destined for a host machine arrives at a LAN gateway, the gateway requests the ARP program to find a physical host (or MAC address) that matches the packet IP address. If a positive match is found within the ARP cache, the packet data is formatted to the appropriate packet length and sent to the machine with the matching address. If a matching entry is not found for the IP address, ARP then broadcasts an IP address query to all machines on the LAN. The machine recognizing this IP address sends a reply to confirming it as its own. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

**Aspect Ratio**

A ratio of width to height, an aspect ratio of 9:16 is used in high-definition television (HDTV).

**Autofocus (AF)**

System by which the camera lens automatically focuses on a selected part of the picture subject.

**Automatic iris**

A lens controlled by a mechanism coupled to the shutter release in the camera body. The diaphragm closes to any preset value before the shutter opens and returns to the fully open position when the shutter closes.

**Bitmap**

A bitmap defines a display space and the color for each pixel or "bit" in the display space. GIF and a JPEG are examples of graphic image file types that contain bit maps. A bit map does not need to contain a bit of color-coded information for each pixel on every row. It only needs to contain information indicating a new color as the display scans along a row. Thus, an image with much solid color will tend to require a small bit map. Because a bit map uses a fixed 'raster' method for specifying an image, a user cannot immediately rescale the image without losing definition. Conversely, a vector graphic image is designed to be quickly rescaled. When an artist is satisfied with an image, it is typically created using vector graphics and then converted to (or saved as) a raster graphic file, or bit map.

**BOOTP**

BOOTP (Bootstrap Protocol) is a protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted or initiated without user involvement. The BOOTP server, managed by a network administrator, automatically assigns the IP address from a pool of addresses for a certain duration of time. BOOTP is the basis for a more advanced network manager protocol, the Dynamic Host Configuration Protocol (DHCP).

**CCD – Charge Coupled Device**

The light-sensitive image device within most modern cameras, this is a large-scale integrated circuit containing hundreds of thousands of photo-sites (pixels) that convert light energy into electronic signals. Its size is measured diagonally and can be 1/4", 1/3", 1/2" or 2/3". CCD stands for Charge Coupled Device, which is the new age imaging device, replacing the old image tube. When first invented in the 1970s, it was initially intended to be used as a memory device. Most often used in cameras, but also in Telephone, fax machines, scanners, etc.

**CCTV**

Closed Circuit Television, also known by the acronym CCTV, is a private video system within a building (or complex) used to visually monitor a location for security or industrial purposes. A CCTV system can be recorded and viewed on-site or viewed remotely through the use of telephone lines.

**Chap**

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:

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

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because the server can request authentication at any time, CHAP provides greater security than PAP. RFC1334 defines both CHAP and PAP.

### **CIF**

CIF (Common Intermediate Format) refers to video resolution 352 x 288 pixels (PAL) and 352 x 240 pixels (NTSC).

### **Client/Server**

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although programs within a single computer can use the client/server concept, it is more relevant in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common.

For example, to check your bank account from your computer, a client program in your computer will need to forward your enquiry to a server at the bank. The bank's server program responds by forwarding that query – via its own client program – to a database running on another server at yet another bank. Your balance information is returned to the requesting data client at your bank, that in turn serves it back to the client in your personal computer. Your huge bank balance is subsequently displayed on the screen.

The client/server model is one of the founding concepts of network computing. Most business applications written today use the client/server model—as does the Internet's main program, TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the 'monolithic' centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing.

In the usual client/server model, one server, sometimes called a daemon, is activated and awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, your Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet. Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet.

Other program relationship models included master/slave, with one program being in charge of all other programs, and peer-to-peer, with either of two programs able to initiate a transaction.

### **Coax cable**

Coax cable is the standard means of transmitting video in a CCTV system. Coax is the same type of cable used by cable companies to send television into the home.

### **Control unit**

If a CCTV system has more than one camera, there must be a way to control each video signal going to the VCR and the monitor. There are three basic types of Video Control Units, Multiplexor, Switch and Quad.

### **DHCP**

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses in an organization's network.

Using the Internet's set of protocols (TCP/IP), each machine that connects to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered.

DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It is especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DHCP is an alternative to another network IP management protocol, BOOTP (Bootstrap Protocol). DHCP is a more advanced protocol, but both configuration management protocols are commonly used. Some organizations use both protocols, but understanding how and when to use them in the same organization is important. Some operating systems, including Windows NT, come with DHCP servers. A DHCP or BOOTP client is a program that is located in (and perhaps downloaded to) each computer so that it can be configured.

### **DNS**

The domain name system (DNS) is the way that Internet domain names are located and translated into IP (Internet Protocol) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. There is probably a DNS server within close geographic proximity to your access provider that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

### **Domain Server**

A tool to authenticate and authorize computers/users on a network. It is used in most corporate networks.

### **Ethernet**

Ethernet is the most widely installed local area network technology. Now specified in a standard, IEEE 802.3, 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. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

Fast Ethernet or 100BASE-T10 provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second).

### **Field**

In video, this is one vertical sweep of a raster scan. In 1:1, 2:1 and 4:1 interlaced video, one, two, and four fields respectively make up a video frame.

### **Firewall**

A firewall works as a gateway between a Local Area Network and the Internet, and will ensure that only authorized users have access through the firewall. A firewall, which can be either a service running on a computer or a standalone device/box, can also be used to filter information and restrict access to certain sites or functions.

### **FTP (File Transfer Protocol)**

FTP (File Transfer Protocol), a standard protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their computer of origin to a publicly accessible computer server for everyone on the Internet. FTP is also commonly used to download programs and other files to your computer from other servers.

As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to log on to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

FTP is usually provided as part of a suite of programs that come with TCP/IP.

### **Frame**

A frame is a complete video picture. In the 2:1 interlaced scanning format of the RS-170 and CCIR formats, a frame is made up of two separate fields of 262.5 or 312.5 lines interlaced at 60 or 50 Hz to form a complete frame which appears at 30 or 25 Hz. In video cameras with a progressive scan, each frame is scanned line-by-line and not interlaced; most are also presented at 30 and 25 Hz.

### **GIF (Graphics Interchange Format)**

A GIF (some people say "DJIF" and others say "GIF" with a hard G) is one of the two most common file formats for graphic images on the World Wide Web. The other is the JPEG.

On the Web and elsewhere on the Internet (for example, bulletin board services), GIF has become a de facto standard image format. CompuServe owns the format, and companies commercially developing products exploiting the format

need to buy a license. Ordinary Web users and businesses publishing GIF images on their Web sites do not need a license.

Technically, a GIF uses the 2D raster data type, is encoded in binary, and uses LZW compression. There are two versions of the format, 87a and 89a. Version 89a (July, 1989) allows for the possibility of an animated GIF, which is a short sequence of images within a single GIF file. A GIF89a can also be specified for interlaced presentation.

An Internet committee has developed a patent-free replacement for the GIF, the PNG format, and major browsers will soon be supporting it.

### **HTML (Hypertext Markup Language)**

HTML (Hypertext Markup Language) is the set of "markup" symbols or codes inserted in a file intended for display on a World Wide Web browser. The markup tells the Web browser how to display a Web page's words and images for the user.

### **HTTP (Hypertext Transfer Protocol)**

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol relative to the TCP/IP suite of protocols, which are the basis for information exchange on the Internet.

Essential concepts that are part of HTTP include the principal idea that files can contain references to other files whose selection elicit additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an HTTP daemon—a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address indicated by the URL. The HTTP daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned. Default TCP port is 80.

### **Hub**

In its traditional sense, a hub is the central part of a wheel where the spokes come together. The term has since developed and is now familiar to frequent fliers who travel through airport "hubs" to connecting flights from one point to another. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded to one or more other directions. A hub usually includes a switch of some kind and in this sense a "switch" is often considered a hub as well. The main distinction between these two devices is that, whereas a hub is simply a device for joining several data streams together, a switch is a more complex device that additionally determines how and where the data is forwarded. With reference to its switching capability, a hub can also be regarded as a router.

1. In describing network topologies, a hub topology consists of a backbone (main circuit) to which a number of outgoing lines can be attached ("dropped"), each providing one or more connection ports for devices to attach to. For Internet users not connected to a local area network, this is the general topology used by your access provider. Other common network topologies are the bus network and the ring network. (Either of these could possibly feed into a hub network, using a bridge.)
2. As a network product, a hub may include a group of modem cards for dial-in users, a gateway card for connections to a local area network (for example, an Ethernet or a Token Ring), and a connection to a T-1 line (the main line in this example).

### **Image compression**

Image compression minimizes the size of a graphics file (in bytes) without seriously degrading the quality of the image. The reduction in file size for a small and acceptable degradation in image quality allows more images to be stored within a limited disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages.

There are several different ways in which image files can be compressed. For Internet use, the two most common compressed graphic image formats are the JPEG format and the GIF format. The JPEG method is more often used for photographs, while the GIF method is commonly used for line art and other images in which geometric shapes are relatively simple.

Other promising techniques for image compression include the use of fractals and wavelets. And, although these methods have not yet gained widespread acceptance for use on the Internet, both formats do offer significantly higher compression ratios than either JPEG, or GIF. Another new image standard that may in time supersede the popular GIF format is PNG (Portable Network Graphics) format.

A text file or program can be compressed without the introduction of errors, but only to a certain point. This is called 'lossy compression'. And, beyond this point, errors are introduced. In text and program files, it is crucial that the compression process does not cause loss of data, because a single error may seriously damage the meaning of a text file, or prevent a program from running. In image compression, a small loss in quality is usually not noticeable. There is no 'critical point' up

to which compression works perfectly and beyond which point it becomes impossible. But when tolerance for some data loss is acceptable, the compression factor may be greater than it might otherwise be for compression with zero tolerance loss. For this reason, graphic images can be compressed more than text files or programs.

### **IP (Internet Protocol)**

The Internet Protocol (IP) is the method by which data is sent from one computer to another over the Internet. Each computer (known as a host) on the Internet has at least one 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 contain both the sender's Internet address and the receiver's address. Any given data packet is initially sent to a gateway computer. This gateway computer will only be familiar a very small part of the Internet. If this first gateway does not recognize the destination address, the computer forwards the packet to an adjacent gateway. The packet continues to be forwarded to other gateways over the Internet until the destination address is recognized within the gateway's immediate neighborhood or domain. That gateway then forwards the packet directly to the computer synonymous with the destination address. Because a message is divided into a number of packets, each packet may take a different route if necessary across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol, which means that there is no established connection between the end points that communicate. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (TCP is a connection-oriented protocol that keeps track of the packet sequence in a message. This ensures that the data packets are always kept in the correct order.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer. The most widely used version of IP today is Internet Protocol Version 4 (IPv4).

However, IP Version 6 (IPv6) is also slowly beginning to be supported. IPv6 provides for much longer addresses and therefore affords the possibility of supporting many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

### **IP Masquerading**

A computer running IP Masquerading server software allows one or more computers in a network without assigned IP addresses to communicate with the Internet, via the server's assigned IP address. In this way, all outgoing traffic from the LAN is made to seem like it came from a single host. The masquerading host acts as a router to the hosts on the LAN, but behaves as a single host to the rest of the Internet.

One drawback with masquerading, apart from the additional processing power it demands, is that it only works transparently when the inner 'LAN users' are users of net services and not providers. However, it is possible to direct incoming requests for a certain port to a special host on the inner net interface; for example: it can be arranged for all requests to port 80 to be redirected to a specific host on the LAN. Load balancing is another variation of this method, whereby incoming requests can be distributed among several hosts.

### **IP Multicasting**

IP multicasting is an extension of Link Layer multicast to IP Internets. Using IP Multicasts, a single datagram can be addressed to multiple hosts without sending it to all. In the extended case, these hosts may reside in different address domains. This collection of hosts is called a multicast group. Each multicast group is represented as a 'Class D' IP address. An IP datagram sent to the group is delivered to each group member with the same 'best effort' delivery as that provided for unicast IP traffic. The sender of the datagram does not itself need to be a member of the destination group.

Forwarding of IP Multicast datagrams is accomplished either through static routing information or via a multicast routing protocol. Devices that forward IP multicast datagrams are called multicast routers. They may or may not also forward IP unicasts. Multicast datagrams are forwarded on the basis of both their source and destination addresses.

### **JPEG (Joint Photographic Experts Group)**

To create a JPEG (pronounced JAY-peg) graphic image a level of compression must be chosen from a suite of compression algorithms. When creating or converting a JPEG image from another format, you are asked to specify the quality of image you want. Since the highest quality results in the largest file, you can make a trade-off between image quality and file size. Officially, the JPEG file format is ISO standard 10918. The JPEG scheme includes 29 distinct coding processes although a JPEG implementer may not use them all.

Along with the Graphic Interchange Format (GIF) file, the JPEG is a file type supported by the World Wide Web protocol, usually with the file suffix of '.jpg'. You can create a progressive JPEG that is similar to an interlaced GIF.

### **Monitor**

A monitor is very similar to a standard television set, however, it lacks the electronics to pick up regular television.

Monitors are available in both monochrome and color versions.

### **MPEG (Moving Picture Experts Group)**

MPEG (pronounced EHM-pehg), the Moving Picture Experts Group, develops standards for digital video and digital audio compression. It operates under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, each designed for a different purpose.

To use MPEG video files, you need a personal computer with sufficient processor speed, internal memory, and hard disk space to handle and play the typically large MPEG file (which has a file name suffix of .mpg). You also need an MPEG viewer, or client software that plays MPEG files.

(Note that .mp3 file suffixes indicate MP3 (MPEG-1 audio layer-3) files, not MPEG-3 standard files.) You can download shareware or commercial MPEG players from a number of sites on the Web.

### **Multiplexers**

These units are high-speed switches that provide full-screen images from up to 16 cameras. Multiplexers can playback everything that happened on any one camera without interference from the other cameras on the system.

### **ODBC**

Open Database Connectivity (ODBC) is a standard or open application programming interface (API) for accessing a database. By using ODBC statements in a program you can access files in a number of different databases; including, Access, dBase, DB2, Excel, and Text. In addition to the ODBC software, a separate module or driver is needed for each database to be accessed. The main proponent and supplier of ODBC programming support is Microsoft.

ODBC is based on and closely aligned with the Open Group standard Structured Query Language (SQL) Call-Level Interface. It allows programs to use SQL requests that will access databases without having to know the proprietary interfaces to the databases. ODBC handles the SQL request and converts it into a request the individual database system understands.

ODBC was created by the SQL Access Group and first released in September, 1992. Although Microsoft Windows was the first to provide an ODBC product, versions now exist for UNIX, OS/2, and Macintosh platforms as well.

In the newer distributed object architecture called CORBA, the Persistent Object Service (POS) is a superset of both the Call-Level Interface and ODBC. When writing programs in the Java language and using the Java Database Connectivity (JDBC) application program interface, you can use a product that includes a JDBC-ODBC "bridge" program to reach ODBC-accessible databases.

### **PPan**

The rotation of a camera along its vertical axis, i.e. moving a camera target sideways.

### **PAP**

PAP (Password Authentication Procedure) is a procedure used by PPP servers to validate a connection request. PAP works as follows:

1. After the link is established, the requestor sends a password and an id to the server.
2. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP. PAP protocol details can be found in RFC 1334.

### **PING**

Ping (Packet Internet or Inter-Network Groper) is a basic Internet program that lets you verify that a particular Internet address exists and can accept requests. The verb ping means the act of using the ping utility or command. Ping is used diagnostically to ensure that the host computer you are trying to reach is actually operating. A user is unable to send files to a host that cannot be 'pinged'. Ping can also be used to see how long it takes for an operative host to respond. Using ping, you can learn the number form of the IP address from the symbolic domain name (see "Tip").

Loosely translated, ping means 'to get the attention of' or 'to check for the presence of' another party online. Ping operates by sending a packet to a designated address and waiting for a response. The computer acronym was contrived to match the submariners' term for the sound of a returned sonar pulse.

Ping can also refer to the process of sending a message to all the members of a mailing list requesting an ACK (acknowledgement code). This is done before sending e-mail in order to confirm that all of the addresses are reachable.

Tip!

To find out the dot address (such as 205.245.172.72) for a given domain name, Windows users can go to their MS DOS prompt screen and enter: ping xxx.yyy where xxx is the second-level domain name like "microsoft" and yyy is the top-level domain name like "com").

### **PPP**

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. Your ISP (Internet Service Provider) should be able to provide a PPP connection that allows the ISP server to respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service.

PPP is a full-duplex protocol that can be used over various transmission media; including, twisted pair cable, fiber optic lines, or satellite. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection – that SLIP lacks. If a choice is possible, PPP should be preferred.

### **PPTP**

PPTP (Point-to-Point Tunneling Protocol) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. In this way a corporation can effectively use a WAN (Wide Area Network) as a large single LAN (Local Area Network). Consequently, a company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

PPTP, a proposed standard sponsored by Microsoft and other companies, and Layer 2.

Forwarding, proposed by Cisco Systems, are amongst the most foremost proposals likely to form basis for a new Internet Engineering Task Force (IETF) standard. With PPTP, which is an extension of the Internet's Point-to-Point Protocol (PPP), any PC user with PPP client support can use an independent ISP to securely connect to a server elsewhere in the user's company.

### **Proxy Server**

In an enterprise that uses the Internet, a proxy server acts as an intermediary between a workstation user and the Internet. This affords the enterprise with security, administrative control, and a caching service.

Any proxy server associated with a gateway server, or part of a gateway server, effectively separates the enterprise network from the outside network and the local firewall. It is the firewall server that protects the enterprise network from outside intrusion.

A proxy server receives requests for Internet services (such as a Web page request) from many users. If it a request passes filtering requirements, the proxy server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it is returned to the user without forwarding the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from another server over the Internet. When the requested page is returned, the proxy server forwards it to the user that originally requested it.

To the user, the proxy server is invisible; all Internet requests and returned responses appear to be returned directly from the addressed Internet server. (Note that in practice the proxy server is not quite invisible, as its IP address has must be specified as a configuration option within the Web browser, or other protocol program.)

The fundamental advantage of a proxy server is that its cache can serve all users. Internet sites that are frequently requested are most likely to be in the proxy's cache. This method of storing Web pages locally invariably improves user response times significantly.

The functions of proxy, firewall, and caching can be included in separate server programs or combined in a single package. Different computers use different server programs. For example, a proxy server may coexist in the same machine with a firewall server, or it may be installed on a separate server and forward requests through the firewall.

### **Quads**

A Quad displays images from up to four cameras on a single screen; where, the images from each camera take up approximately a quarter of the display area. Optionally, the visual information from each camera can be simultaneously recorded—but only in the small quad format at quarter-screen resolution.

### **Resolution**

Resolution is a measure of how clear and crisp an image appears on a monitor. As each piece of CCTV equipment included within a system contributes to the overall image quality, the resultant image can only be as clear as the piece of equipment with the lowest resolution. If you are using a high-resolution monitor together with a low-resolution camera, the monitor can only display low-resolution images. This observation becomes increasingly important when using the system for recording. The playback image quality from a tape is typically a half of that displayed within a normal monitor. So, be sure that the system can deliver the resolution your application demands before installing the system!

### **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 towards its final destination. Connecting between at least two networks, the router uses its understanding of the current state of the network to determine which way to send each information packet. A router can be located at any juncture of a network or gateway, including each Internet point-of-presence. A router is often included as part of a network switch.

A router creates and maintains a table of available network routes and their status. It uses this information together with distance and cost algorithms to determine the best route for any given packet. Typically, a packet may travel through a number of network points and several routers before arriving at its final destination.

An edge router is a router that interfaces with an asynchronous transfer mode (ATM) network. A brouter is a network bridge combined with a router.

### **RS-232**

RS-232C is a long-established standard ("C" is the current version) that describes the physical interface and protocol for relatively low-speed serial data communication between computers and related devices. An industry trade group, the Electronic Industries Association (EIA), originally defined it for teletype devices.

RS-232C is the interface that your computer uses to talk to and exchange data with your modem and other serial devices. Somewhere in your PC, typically on a UART (universal asynchronous receiver-transmitter) chip on your motherboard, the data from your computer is transmitted to an internal or external modem (or other serial device) from its Data Terminal Equipment (DTE) interface.

Since data in your computer flows along parallel circuits and serial devices can handle only one bit at a time, the UART chip converts the groups of bits in parallel to a serial stream of bits. As your PC's DTE agent, it also communicates with the modem or other serial device, which, in accordance with the RS-232C standard, has a complementary interface called the Data Communications Equipment (DCE) interface.

The RS-232 standard has a:

- maximum recommended range of 50 feet (15.2 meters),
- recommended baud rate maximum of 20Kb/s, that is frequently exceeded in practice.
- defined standard pinout for D-25 connector and D-9 connectors.

### **RS-422**

RS-422 defines its signal characteristics as a differential pair with no standard connectors or pin-out defined. The differential pair is one signal transmitted across two separate wires in opposite states; one inverted and one non-inverted. To determine the logical state of the signal, the receiver compares the difference in voltage between the two lines. The idea behind this is that if the transmission wires are exposed to electrical noise, both lines are affected equally.

Consequently, the voltage potential between the two lines remains unaltered. Twisted pair type wire is recommended to best the signal radiation common on both lines. RS-422 is normally used in a "4-wire" full duplex mode for point-to-point communication, but can handle up to 10 receivers per transmitter.

- Maximum recommended range of 4,000 feet.
- Maximum recommended baud rate of 10M b/s
- Well suited for noisy environments; differential signal provides common-mode noise rejection.
- Receiver input sensitivity of +/- 200mV.
- One transmitter can drive up to ten receivers.
- 100 ohm termination placed at receiver furthest from the transmitter.

### **RS-485**

RS-485 is an upgraded version of RS-422 with the added capability to allow up to 32 devices (transmitters and receivers) to share the same connection (multidrop or "2 wire" mode). This is achieved by use of tristate drivers, which are usually controlled by a programmable handshake line to ensure that only one driver is active at a time. This control must be taken into consideration by the software.

- Maximum recommended range of 4,000 feet.
- Maximum recommended baud rate of 10M b/s.
- Support full duplex "4-wire" or half duplex "2-wire" communication.
- 120 ohms termination placed at two furthest points of communication link for 60 ohm parallel termination.

### **RTP**

RTP is the Internet-standard protocol for the transport of real-time data, including audio and video. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part.

The data part of RTP is a thin protocol providing support for applications with real-time properties such as continuous media (e.g., audio and video), including timing reconstruction, loss detection, security and content identification.

### **RTCP**

RTCP provides support for real-time conferencing of groups of any size within an intranet. This support includes source identification and support for gateways like audio and video bridges as well as multicast-to-unicast translators.

It offers quality-of-service feedback from receivers to the multicast group as well as support for the synchronization of different media streams.

### **Server**

In general, a server is a computer program that provides services to other computer programs in the same or other computers. A computer running a server program is also frequently referred to as a server. In practice, the server may contain any number of server and client programs. In the client/server programming model, a server is a program that awaits and fulfils requests from client programs in the same, or other, computers. Any given computer application may function as a client with requests for services from other programs and as a server receiving and managing requests from other programs. Specific to the Web, a Web server is the computer program 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.

### **SMTP**

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used for sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, is usually used with one of two other protocols, POP3 or IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server. Users generally use an e-mail application that utilizes SMTP for sending e-mail, with either POP3 or IMAP for receiving their messages from their local server. Most e-mail programs like Eudora allow you to specify both an SMTP server and a POP server. On UNIX-based systems, sendmail is the most widely used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server and also comes in a version for Windows NT. SMTP is usually implemented to operate over TCP port 25. The specification details for SMTP are included in RFC 821 of the Internet Engineering Task Force (IETF). Europe is X.400 is a widely used alternative to SMTP.

### **Sockets**

Sockets are a method for communication between a client program and a server program over a network. A socket is defined as "the endpoint in a connection." Sockets are created and used with a set of programming requests or "function calls" sometimes called the sockets application programming interface (API).

The most common socket, API, is the Berkeley UNIX C language interface for sockets. Sockets can also be used for communication between processes within the same computer.

This is the typical sequence of sockets requests from a server application in the "connectionless" context of the Internet, in which a server handles many client requests and does not maintain a connection longer than the time it takes to serve the immediate request:

```

socket()
|
bind()
|
recvfrom()
|
(wait for a sendto request from some client)
|
(process the sendto request)
|
sendto (in reply to the request from the client; e.g., send an HTML file)

```

The corresponding sequence of client sockets requests would be:

```
socket()
|
bind()
|
sendto()
|
recvfrom()
```

Sockets can also be used for "connection-oriented" transactions with a somewhat different sequence of C language system calls or functions.

### **SSL/TSL**

Secure Socket Layer. A tool that allows for secure communication when connecting to remote Web servers. By using trusted certificates, issued by third-party organizations like Verisign, the remote user can decide to trust information provided by the server.

### **Sharpness**

This is the control of fine detail within a picture, independent of content. At least, that's what it is supposed to mean. The feature was originally introduced into color TV sets that used notch filter decoders—which includes almost every color TV launched onto the market before the mid-1980's. The filter took away all high frequency detail in the black and white region of the picture. The sharpness control attempted to put some of that detail back in the picture. Although sharpness control was unnecessary on many expensive sets that included comb filters, manufacturers were reluctant to remove a popular control mechanism that consumers had seen on TV sets for years. With sharpness controls pretty much superfluous in high-end TVs, the only logical requirement for sharpness control nowadays is on a VHS machine. Notably, there is no sharpness control included on direct view sets designed for DTV.

### **Subnet and subnet mask**

A subnet (short for 'subnetwork') is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address.

Without the use of subnets, an organization would need multiple connections to the Internet—one for each of its physically disparate subnetworks. However, this would represent unwarranted use of the limited number of IP numbers the Internet has to assign. Moreover, it would also require that the Internet routing tables maintained on gateways outside the organization would need to manage the routing otherwise be handled within the organization.

The Internet is a collection of networks whose users communicate with each other. Each communication carries the address of the source and destination networks, along with the address of the machine that is associated with the user, or host computer, at either end. This address is called the IP address (Internet Protocol address). This 32-bit IP address has two parts: one part that identifies the network (with the network number) and the other part that identifies the specific machine or host within the network (with the host number). An organization may use some of the bits in the machine or host part of the address to identify a specific subnet. Effectively, the IP address then contains three parts: the network number, the subnet number, and the machine number.

The standard procedure for creating and identifying subnets is provided in Internet RFC 950.

### **The IP Address**

The 32-bit IP address is often referred to as a dot address (sometimes called dotted quad notation) - that is, four groups (or quads) of decimal digits separated by periods.

Here's an example: 130.5.5.25

Each of the decimal digits represents a string of four binary digits. Thus, the above IP address really is this string of 0s and 1s:

```
10000101.00000101.00000101.00011001
```

In the example above we have inserted periods between each eight-digit sequence just as we did for the decimal version of the IP address. Obviously, the decimal version of the IP address is easier to read, and it is this form that is most commonly used.

Some portion of the IP address represents the network number or address and some portion represents the local machine address (also known as the host number or address).

IP addresses can be one of several classes, where each specific class determines how many bits represent the network number and how many represent the host number. The most common class used by large organizations (Class B) allows 16 bits for the network number and 16 for the host number. Using the above example, here's how the IP address is divided:

<--Network address--><--Host address-->  
130.5 . 5.25

If you wanted to add subnetting to this address, then some portion of the host address (in this example, eight bits) could be used for a subnet address. Thus:

<--Network address--><--Subnet address--><--Host address-->  
130.5 . 5 . 25

To simplify this example, we've divided the subnet into a neat eight bits, but in practice an organization may choose some other scheme that uses only part of the third quad, or even part of the fourth quad.

### **The Subnet Mask**

Once a packet, with its unique network number, has arrived at an organization's gateway or connection point, it can then be routed within the organization's internal gateways using the subnet number as well. The router knows which bits to look at (and which bits not to look at) by looking at the subnet mask. A mask is simply a screen of numbers that tells the router which numbers are relevant 'underneath' the mask. In a binary mask, a '1' over a number says 'look at the number underneath'; whereas, a '0' says 'don't look'. Using a mask saves the router having to handle the entire 32-bit address; it can simply look at the bits selected by the mask.

Using the previous example (which is a very typical case), the combined network number and subnet number occupy 24 bits or three of the quads. The appropriate subnet mask carried along with the packet in this case would be:  
255.255.255.0

This effectively translates to a string of all 1's for the first three quads (telling the router to look at these) and a string of 0's for the last quad that represents the host number (which the router doesn't need to look at). In this way, subnet masking allows routers to move the packets on more quickly.

If you have the job of creating subnets and/or specifying subnet masks for an organization (an activity called subnetting), your job can be simple or difficult dependent upon on the size and complexity of your organization.

### **Switch**

In telecommunications, a switch is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the router functioning which a device or program determines the route and, more specifically, what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.

On larger networks, the trip from one switch point to another in the network is called a hop. The time a switch takes to figure out where to forward a data unit is called its latency. The price paid for the flexibility switches provide in a network is increased latency.

Switches are found both at the backbone and gateway levels of a network (where one network connects with another), and, at the subnetwork level (where data is invariably forwarded to a destination close to its origin).

A switch is not always required in a network. Many local area networks (LANs) are organized as rings or buses in which all destinations inspect each message and read only those intended for that destination.

Circuit-Switching version Packet-Switching...

Two or more parties can use a network path exclusively for a certain duration. It can then be switched for use to other parties. This type of "switching" is known as circuit-switching and is really a dedicated and continuously connected path for its duration. Today, an ordinary voice phone call generally uses circuit-switching.

Most data today is sent, using digital signals, over networks that use packet-switching. Using packet-switching, all network users can share the same paths at the same time, and the route a data unit travels can be varied as prevailing conditions change. In packet-switching, a message is divided into packets, which are perhaps best described as units of data containing a variable number of bytes. The network addresses of both the sender and of the destination are added to the packet.

Each network point looks at the packet to see where to send it next. Packets associated with the same message may travel different routes and may not arrive in the same order that they were sent. At the destination, the packets in a message are collected and reassembled into the original message.

The Internet Protocol (IP) Switch...

An IP switch is a packet-switching switch that uses the Internet Protocol (IP). An IP switch includes the ability to determine routing. An IP switch performs the functions identified in layer-3 of the Open Systems Interconnection (OSI) model, the standard multi-layered architecture for network communication.

### **TCP**

TCP (Transmission Control Protocol) is a method (protocol) used along with the Internet Protocol (IP) to send data in the

form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing over the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message, or messages, has been successfully exchanged between the communicating applications. TCP ensures that a message is divided into manageable packets that IP then reassembles back into a complete message at the receiving end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

### **TCP/IP**

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language (or protocol) of the Internet. It is also used as a communications protocol in private networks called intranets, and in extranets. When your computer is set up for direct access to the Internet, it is provided with a copy of the TCP/IP program. Similarly, every computer you may like to send messages to must also be installed with a copy of the program.

TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembly of a message or file into smaller packets that are transmitted over the Internet. The packets are received by the TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets within the same message are routed differently than others, they are reassembled to reunite the message at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is subsequently provided with a service; such as, sending a Web page to another computer (a server) over the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) to another.

TCP/IP and the higher-level applications that use it are collectively said to be "connectionless" because each client request is considered a new request that is unrelated to any previous one. (unlike ordinary phone conversations that require a dedicated connection for the entire call duration). Being connectionless, frees network paths so that everyone can use them continuously. (Note that because the connection remains in place until all packets in a message have been successfully received, the TCP layer itself is not connectionless as far as any single message is concerned.)

Many Internet users are also familiar even with the higher layer application protocols that use TCP/IP to access the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (that allows you logon to remote computers), and the Simple Mail Transfer Protocol (SMTP). These and other protocols are often packaged together with TCP/IP as a "suite."

Personal computer users usually get to the Internet through the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). These protocols encapsulate the IP packets so that they can be sent over a dial-up phone connection to an access provider's modem.

Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP), the Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP), and the Border Gateway Protocol (BGP).

### **Telnet**

Telnet is a simple method with which to access someone else's computer—assuming they have given you permission. (Such a computer is frequently called a host computer.) At a more technical level, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. The Web or HTTP protocol and the FTP protocol allow you to request specific files from remote computers, but do not allow you logon as a user of that computer. With Telnet, you logon as a regular user with whatever privileges you may have been granted for specific applications and data residing on that computer.

A Telnet command request looks like this (the computer name is made-up):

```
telnet the.libraryat.harvard.edu
```

The result of this request would be an invitation to logon with a userid and a prompt for a password. If accepted, you may logon just like any other regular user.

Telnet is most likely to be used by program developers, or anyone that has a need to use specific applications that reside on a remote host computer.

**Tilt**

The rotation of a camera along its perpendicular line of sight, i.e. moving a camera target vertically. If animated, a nodding effect is achieved.

**Time-lapse recorder**

The type of video recorder commonly used in the security industry has the ability to record up to one-week of video on a single tape. The most commonly used timing is the 24-hour mode. Having to change tapes only once a day and retaining large amounts of information are perceived as key advantages in using this particular mode of recording.

**TVL**

TV Lines, a method to define resolutions within analog video.

**UDP**

UDP (User Datagram Protocol) is a communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network using the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and subsequently very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

In the Open Systems Interconnection (OSI) communication model, UDP, like TCP, is in layer 4, the Transport Layer.

**VPN**

Virtual Private Network. This creates a secure tunnel between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. The VPN network can be residing within a normal company LAN (Local Area Network), and/or over public networks such as Internet. VPN also allow for different sites to be connected together over Internet in safe and secure way. Another common use is for travelers to use VPN when connecting their laptop from a hotel room to the corporate network.

**Video camera**

The modern CCTV video camera is available in both monochrome (black and white) and color. Cameras can be set in fixed-positions or placed on 'pan-and-tilt' devices that allow the camera to be moved up, down, left and right. Using a zoom lens provides a closer view of the person, or object, you wish to see.

**Video Switchers**

These units sequentially display full screen images, one camera after another typically at 3 to 5 seconds intervals. While the image source from one camera is displayed on screen the other camera sources are not being recorded.

**Wavelet**

A wavelet is a mathematical function useful in signal processing and image compression. The use of wavelets for these purposes is a recent development, although the theory is not new. The principles are similar to those of Fourier analysis, which was first developed in the early part of the 19th century.

In signal processing, wavelets make it possible to recover weak signals from noise. This has proven useful especially in the processing of X-ray and magnetic resonance images in medical applications. Images processed in this way can be "cleaned up" without blurring or muddling the details.

In Internet communications, wavelets have been used to compress images to a greater extent than is generally possible with other methods. In some cases, a wavelet-compressed image can be as much as 25% smaller than a JPEG-compressed image of a similar quality. In practice, this can mean that a photograph compressed with JPEG to 200 KB taking a minute to download, can be compressed with wavelet to 50 KB and take only 15 seconds to download.

Wavelet compression works by analyzing an image and converting it into a set of mathematical expressions that can then be decoded by the receiver. A wavelet-compressed image file is often given a name suffix of ".WIF." Either your browser must support these files or will require a plug-in program to read the files.

Wavelet compression is not yet widely used on the Web. GIF remains the most common image compression formats, used mainly for drawings, and JPEG, used mainly for photographs.

**Web server**

A Web server is a program, which allows Web browsers to retrieve files from computers connected to the Internet. The Web server listens for requests from Web browsers and upon receiving a request for a file sends it back to the browser.

The primary function of a Web server is to serve pages to other remote computers; consequently, it needs to be installed on a computer that is permanently connected to the Internet. It also controls access to the server whilst monitoring and logging server access statistics.

**WEP**

Wireless Equivalent Privacy. Compression used in WiFi networks. Exists in two different security levels, 40(64) bit and 128 bit encryption. The higher the bit number, the more secure the encryption.

**WINS**

WINS (Windows Internet Naming Service), part of the Microsoft Windows NT Server, manages the association of workstation names and locations with Internet Protocol addresses (IP addresses) without the user or an administrator having to be involved in each configuration change. WINS automatically maps computer names with their corresponding IP addresses into a table, ensuring that each name is unique and dissimilar to any existing computer name. When a computer is moved to another geographical location, the subnet part of the IP address is likely to change. Using WINS, the new subnet information will be updated automatically in the WINS table. WINS complements the NT Server's Dynamic Host Configuration Protocol (DHCP), which negotiates dynamic IP addresses for different computers each time they connect to the network. If you are using a computer user on a network connected to a Windows NT Server, you may find WINS mentioned in some of your network-related programs or system messages.

Based on Microsoft's paper, DHCP and WINS have been proposed open standards to the Internet Engineering Task Force (IETF) in Request for Comments 1533, 1534, 1541, and 1542. New features are included in the follow-on to Windows NT, Windows 2000.

**WPA**

WiFi Protected Access. It is a fairly new standard for wireless networks and is more secure than WEP.

**Zoom**

Enlarges the view of an object enabling you to see more detail.

In photographic terms, 'Telescopic' and 'Wide' are general expressions used to describe the varying extremes of the zoom function; where:

telescopic - brings distant objects into closer view, and

wide - sends objects foreground object to the background to enlarge the field of view.