6

System Development

6.1 HARDWARE REQUIREMENTS

6.1.1 PC Level Processing Units

UNIX Workstations

The user running Client/Server applications form DOS or Windows typically run only a single business process at a time. And also UNIX has locked the familiar personal productivity tools such as word processors, e-mail, spreadsheet, presentation graphics and database management system, but recently few personal productivity applications were in place, user needs have increased with providing reliability with multitasking. Many Unix implementation with application execution offers the best of all words for the desktop user reliability and functionality. Nowadays Unix supports many of the most familiar personal computer applications like WordPerfect, DBASE IV, Lotus 1-2-3. Unix has become the workstation of choice for Client/Server environment on the basis of cost performance rather than functionality.

X-Window System

The X-Window System is an open, cross-platform, Client/Server system for managing a windowed graphical user interface in a distributed network. In X-Window, the Client/Server relationship is reversed from the usual. Remote computers contain applications that make client requests for display management services in each PC or workstation. X-Window is primarily used in networks of interconnected mainframes, minicomputers, and workstations. It is also used on the X-terminal, which is essentially a workstation with display management capabilities but without its own applications. (The X-terminal can be seen as a predecessor of the network PC or thin client computer).

X-Window System (commonly X11 or X) is a windowing system for bitmap displays. It provides the standard toolkit and protocol to build graphical user interfaces on Unix, Unix-like operating systems, and OpenVMS; and almost all modern operating systems support it. X provides the basic framework for a GUI environment to do drawing and moving windows on the screen and interacting with a mouse and keyboard. X does not mandate the user interface, individual client programs handle this. As such, the visual styling of X-based environments varies greatly; different programs may present radically different interfaces. X provides network transparency in which the machine where application programs (the *client* applications) run can differ from the user's local machine (the display *server*).

X-Terminal

An X-terminal is typically a diskless terminal especially designed to provide a low-cost user interface for applications that run in a network X-server as part of a distributed X-Window System. Typically, X-terminals are connected to a server running a UNIX-based operating system in a mainframe, minicomputer, or workstation. A terminal specially designed to run an X-server which allows users to display the output of programs running on another computer using the X-protocol over a network.

The X-terminal concept is essentially like tel-neting into a machine and then running some application there. All the working is done on the machine that you are connecting to but the display is shown on your machine. That just gives you access to console mode text applications, whereas an X-terminal setup will give you access to the entire range of GUI applications. All applications will be run on the server but the display will be exported to your computer. The machine that you setup as the X-terminal just serves as a display. This setup works very well with diskless workstations and older computers. An X-terminal is a great way to expand the computing presence in a home or office.

An X-terminal consists of a piece of dedicated hardware running an X-server as a thin client. This architecture became popular for building inexpensive terminal parks for many users to simultaneously use the same large server. X-terminals can explore the network (the local broadcast domain) using the X-Display Manager Control Protocol to generate a list of available hosts that they can run clients from. The initial host needs to run an X-display manager. Dedicated (hardware) X-terminals have become less common; a PC with an X-server typically provides the same functionality at a lower cost.

X-Server

An X-server is a server of connections to X-terminal in a distributed network that uses the X-Window System. From the terminal user's point-of-view, the X-server may seem like a server of applications in multiple windows. Actually, the applications in the remote computer with the X-server are making client request for the services of a windows manager that runs in each terminal. X-servers (as part of the X-Window System) typically are installed in a UNIX-based operating system in a mainframe, minicomputer, or workstation.

The X-server is the software that handles all the interactions between the GUI and hardware used. Windows equivalent would be the graphics card driver. But X is a lot more than that. Here it becomes a server with whom clients get connected. Clients would be the various GUI applications like GNOME, KDE etc. communicating through network protocols. This architecture allows a lot of flexibility. The clients can be run on any machine but the display can be routed to another machine. The X-server provides the following services.

- *Window services:* Clients ask the server to create or destroy windows, to change their attributes, to request information about them, etc.
- *Input handling:* Keyboard and mouse input are detected by the server and sent to clients.
- *Graphic operations:* Clients ask the server to draw pixels, lines, strings, etc. The client can ask information about fonts (size, etc.) and can ask transfer of graphic content.
- *Resource management:* The X-resource manager provides a content addressable database for clients. Clients can be implemented so they are customizable on a system and user basis.

The X-Client/Server model and network transparency

In X-Client/Server model, an *X-server* communicates with various *client* programs. The server accepts requests for graphical output (windows) and sends back user input (from keyboard, mouse, or touchscreen). The server may function as any one of the following:

- an application displaying to a window of another display system.
- a system program controlling the video output of a PC.
- a dedicated piece of hardware.

This Client/Server terminology the user's terminal as the "server", the remote applications as the "clients" often confuses new X users, because the terms appear reversed. But X takes the perspective of the program, rather than the end-user or the hardware. The local X display provides display services to programs, so it is acting as a server; the remote program uses these services, thus it acts as a client.

In above example, the X-server takes input from a keyboard and mouse and displays to a screen. A web browser and a terminal emulator run on the user's workstation, and a system updater runs on a remote server but is controlled from the user's machine. Note that the remote application runs just as it would locally.

The communication protocol between server and client operates network-transparently. The client and server may run on the same machine or on different ones, possibly with different architectures and operating systems, but they run the same in either case. A client and server can even communicate securely over the Internet by tunneling the connection over an encrypted connection. To start a remote client program displaying to a local server, the user will typically open a terminal window and telnet or ssh to the remote machine, tell it to display to the user's machine (*e.g.,* export DISPLAY = *[user's machine]*:0 on a remote machine running bash), then start the client. The client will then connect to the local server and the remote application will display to the local screen and accept input from the local input devices. Alternately, the local machine may run a small helper program to connect to a remote machine and start the desired client application there. Practical examples of remote clients include:

- administering a remote machine graphically.
- running a computationally-intensive simulation on a remote Unix machine and displaying the results on a local Windows desktop machine.
- running graphical software on several machines at once, controlled by a single display, keyboard and mouse.

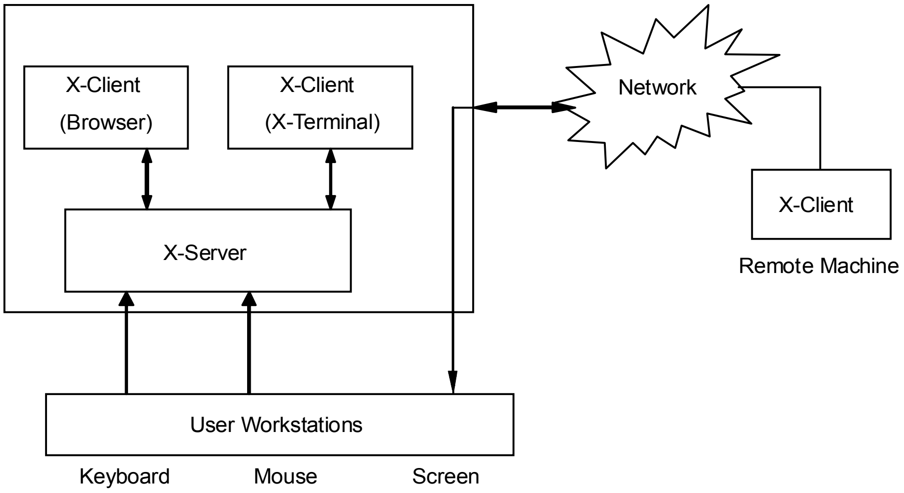

Fig. 6.1: X-Client-Server Model

Light Pen

Light Pen is an input device that utilizes a light-sensitive detector to select objects on a display screen. It is similar to a mouse, except that with a light pen you can move the pointer and select objects on the display screen by directly pointing to the objects with the pen. A light pen is pointing device that can be used to select an option by simply pointing at it, drawing figures directly on the screen. It has a photo-detector at its tip. This detector can detect changes in brightness of the screen. When the pen is pointed at a particular spot on the screen, it records change in brightness instantly and inform the computer about this. The computer can find out the exact spot with this information. Thus, the computer can identify where you are pointing on the screen.

Light pen is useful for menu-based applications. Instead of moving the mouse around or using a keyboard, the user can select an option by pointing at it. A light pen is also useful for drawing graphics in CAD.

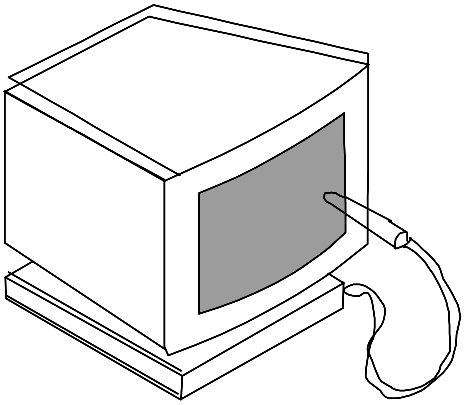

Fig. 6.2: Light Pen

Digital Pen

A digital pen writes on paper like any normal pen. The difference is that it captures everything you write. The digital pens include a tiny camera, some memory, a CPU and a communications unit. The paper is also special in that it needs to have an almost invisible dot pattern printed on it. You could use your laser to print this or get a specialist stationery printer to do it. Many paper products from 3M yellow sticky notes to black n' red notebooks are already available with the pattern pre-printed on them. The pen senses the pattern and this is how it knows where on the page you are writing. Most importantly using the digital pen is as easy as a normal pen with the quite significant benefit that a digital record is simultaneously created as you write.

They are available with desktop software applications integrating the pen with Microsoft Word and Outlook as well as a searchable notebook application. The pen is able to sent what you have written to a computer for storage and processing, or as an e-mail or fax. Applications range from: removing the need to re-key forms, to automatically storing and indexing pages written in a notebook. You can even send faxes and emails by simply writing them with a pen. Example of digital pens is Logitech io2 or a Nokia SU-1B pen.

Notebook Computers

If the portable computers are classified, they are of three types: laptops, notebooks and palmtops. Notebook computers are about the size of a notebook (approx. 21* 29.7 cm) and weight about 3 to 4 kg. Notebooks also offer the same power as a desktop PC. Notebooks have been designed to overcome the disadvantage of laptops that is they are bulky. Notebook/Portable computers are productivity-enhancement tools that allow busy execution to carry their office work with them. They are smaller in size. Several innovative techniques are being used to reduce size. Like VDU is compact, light, and usesless power, LCD (liquid crystal display that are light and consume very little power are used. Further numbers of keys on keyboard are reduced and also they are made to perform multiple functions. The size of hard disk is reduced is of 2.5" in diameter but capable of storing large quantities of data with weight only 300 gms. Examples of notebooks are Conture 3/20 from Compaq, and AcerAnyWhere from Zenith Computers.

6.1.2 Storage Devices

Storage refers to the media and methods used to keep information available for later use. Some things will be needed right away while other won't be needed for extended periods of time. So different methods are appropriate for different uses. Auxiliary Storage that is Secondary Storage holds what is not currently being processed. This is the stuff that is "filed away", but is ready to be pulled out when needed. It is non-volatile, meaning that turning the power off does not erase it. Auxiliary Storage is used for:

- Input—data and programs.
- Output—saving the results of processing.

So, Auxiliary Storage is where you put last year's tax info, addresses for old customers, programs you may or may not ever use, data you entered yesterday - everything that is not being used right now.

- Magnetic tape.
- Magnetic disks.
- Optical disks.
- Other storage devices—flash drives.

Magnetic Tape

Magnetic tape is a secondary storage device, generally used for backup purposes. They are permanent and not volatile by nature. The speed of access can be quite slow, however, when the tape is long and what you want is not near the start. So this method is used primarily for major backups of large amounts of data. Method used to store data on magnetic tape is similar to that of VCR tape. The magnetic tape is made up of mylar (plastic material) coated only on one side of the tape with magnetic material (Iron oxide). There are various types of magnetic tapes are available. But each different tape storage system has its own requirements as to the size, the container type, and the magnetic characteristics of the tape. Older systems designed for networks use reel-to-reel tapes. Newer systems use cassettes. Some of these are even smaller than an audio cassette but hold more data that the huge reels. Even if they look alike, the magnetic characteristics of tapes can vary. It is important to use the tape that is right for the system. Just as floppy disks and hard disks have several different formats, so do magnetic tapes. The format method will determine the some important characteristics like

Density: Higher density means more data on shorter tape that is measured as bpi (bits per inch that ranges from 800 bpi up to 6250 bpi.

Block: The tape is divided into logical blocks, as a floppy is divided into tracks and sectors. One file could take up many logical blocks, but must take up one whole block at least. So smaller blocks would result in more room for data.

Gap: Two kinds of blank spots, called gaps, are set on the tape. Interblock gap, which separates logical blocks. Interrecord gap, which is wider and separates records. Notice the two size lines cutting across the tape in the Fig. 6.3 below. Smaller gaps would allow more data to be stored on the same size tape.

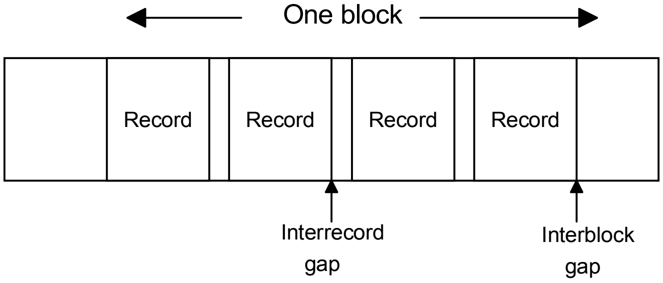

Fig. 6.3: Magnetic Tape

Magnetic Disks

There are various types of auxiliary storage; all of them involve some type of magnetic disk. These come in various sizes and materials, as we shall see. This method uses magnetism to store the data on a magnetic surface. The advantages associated with such type of storage media is they are of high storage capacity, reliable and provides direct access to the data. A drive spins the disk very quickly underneath a *read/write head*, which does what its name says. It reads data from a disk and writes data to a disk.

There are various types of auxiliary storage; all of them involve some type of magnetic disk. These come in various sizes and materials. This method uses magnetism to store the data on a magnetic surface. The advantages associated with such type of storage media is they are of high storage capacity, reliable and provides direct access to the data. A drive spins the disk very quickly underneath a *read/write head*, which does what its name says. It reads data from a disk and writes data to a disk. The available magnetic disks are Diskette/ Floppy disk and Hard disk.

All the magnetic disks are similarly formatted, or divided into areas that are tracks sectors and cylinders. The formatting process sets up a method of assigning addresses to the different areas. It also sets up an area for keeping the list of addresses. Without formatting there would be no way to know what data went with what. It would be like a library where the pages were not in books, but were scattered around on the shelves and tables and floors.

All the magnetic disks contain a track that is a circular ring on one side of the disk. Each track has a number. A disk sector is a wedge-shape piece of the disk. Each sector is numbered. Generally on a 5¼″ disk there are 40 tracks with 9 sectors each and on a 3½″ disk there are 80 tracks with 9 sectors each. Further a track sector is the area of intersection of a track and a sector. A cluster is a set of track sectors, ranging from 2 to 32 or more, depending on the formatting scheme in use.

The most common formatting scheme for PCs sets the number of track sectors in a cluster based on the capacity of the disk. A 1.2 giga hard drive will have clusters twice as large as a 500 MB hard drive. One cluster is the minimum space used by any read or write. So there is often a lot of slack space, unused space, in the cluster beyond the data stored there. The only way to reduce the amount of slack space is to reduce the size of a cluster by changing the method of formatting. You could have more tracks on the disk, or else more sectors on a track, or you could reduce the number of track sectors in a cluster.

A cylinder is a set of matched tracks on a double-sided floppy, a track from the top surface and the same number of track from the bottom surface of the disk make up a cylinder. The concept is not particularly useful for floppies. On a hard disk, a cylinder is made of all the tracks of the same number from all the metal disks that make up the “hard disk.” If all these are putted together on the top of each others. It will looks like a tin can with no top or bottom forming a cylinder.

What happens when a disk is formatted?

Whether all data is erased? Surfaces are checked for physical and magnetic defects. A root directory is created to list where things are on the disk.

The capacity of a magnetic disk depends on several factors.

Optical Disk

The disk is made up of a resin (such as polycarbonate) coated with a highly reflective material (Aluminium and also silicon, silver, or gold in double-layered DVDs). The data is stored on a layer inside the polycarbonate. A metal layer reflects the laser light back to a sensor. Information is written to read from an optical disk using laser beam. Only one surface of an optical disk is used to store data. The coating will change when a high intensity laser beam is focused on it. The high intensity laser beam forms a tiny pit along a trace to represent 1 for reading the data laser beam of less intensity is employed (normally it is 25mW for writing and 5mW for reading). Optical disks are inexpensive and have long life up to 100 years. The data layer is physically molded into the polycarbonate. Pits (depressions) and lands (surfaces) form the digital data. A metal coating (usually aluminium) reflects the laser light back to the sensor. Oxygen can seep into the disk, especially in high temperatures and high humidity. This corrodes the aluminium, making it too dull to reflect the laser correctly. There are three types of optical disk are available:

- Compact Disk Read Only Memory (CD-ROM)
- Write Once Read Many (WORM)
- Erasable Optical Disk
- Digital Video Device (DVD)

All these optical disk are of similar characteristics like formed layers, organization of data in a spiral groove on starting form the center of the disk and finally nature of stored data is digital. 1’s and 0’s are formed by how the disk absorbs or reflects light from a tiny laser. An option for backup storage of changing data is **rewritable disks,** CD-RW, DVD-

RW, DVD + RW, and DVD + RAM. The data layer for these disks uses a phase-changing metal alloy film. This film can be melted by the laser's heat to level out the marks made by the laser and then lasered again to record new data. In theory you can erase and write on these disks as many as 1000 times, for CD-RW, and even 100,000 times for the DVD-RW types.

In case of WORM, the user can write data on WORM and read the written data as many times desired. Its tracks are concentric circles. Each track is divided into a number of sectors. Its disk controller is somewhat more expensive than that required for reading. The advantages of WORM are its high capacity, longer life and better reliability.

The Erasable optical disk is read/write optical memory. The disk contents can be erased and new data can be rewritten to it. It is also used as secondary memory of computer. The tracks are concentric circle. The coating of an erasable optical disk is done by a magnetic material, which does not lost its magnetic properties at the room temperature. The reading and writing operations are performed using magneto-optical system. In which a laser beam is employed together with a magnetic field to read/write operations.

Working mechanism of Optical disks in case of CD vs. DVD

As it has been discussed above that an optical disc is made mainly of polycarbonate (a plastic) see the Fig. 6.4 given below. The data is stored on a layer inside the polycarbonate. A metal layer reflects the laser light back to a sensor. And to read the data on a disk, laser light shines through the polycarbonate and hits the data layer. How the laser light is reflected or absorbed is read as a 1 or a 0 by the computer.

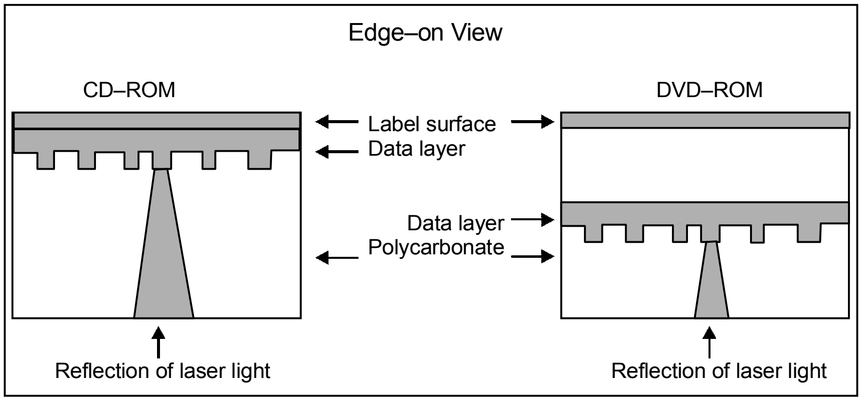

Fig. 6.4: Optical Disks (CD vs. DVD)

In a CD, the data layer is near the top of the disk, the label side. In a DVD the data layer is in the middle of the disk. A DVD can actually have data in two layers. It can access the data from 1 side or from both sides. This is how a double-sided, double-layered DVD can hold 4 times the data that a single-sided, single-layered DVD can. The CDs and DVDs that are commercially produced are of the Write Once Read Many (WORM) variety. They can't be changed once they are created.

Other Storage Devices—Flash Drives

Pen Drives

Also known as USB Flash Drive, USB Thumb Drive, Flash Drives. A thumb drive is portable memory storage. It is rewritable and holds its memory without a power supply, unlike RAM. Thumb drives will fit into any USB port on a computer. They will also "hot swap," which means a user can plug the drive into a computer and will not have to restart it to access the thumb drive. The drives are small, about the size of a human thumb hence, their name and are very stable memory storage devices. The thumb drive is available in storage sizes of up to 8 gigabytes (starting from 128MB, 256MB, 512MB, 1GB, 2GB, 4GB, 8GB). They are stable, versatile, durable and portable data storage devices. As such they are ideal for almost any computer user who wants safe, long-term storage for a low price. USB flash drives may have different design, different capacity and different price and some USB flash drives feature add-on functions such as MP3 players. But they do share some other characteristics:

USB flash drives are lightweight. Most USB flash drives are as light as a car key.

USB flash drives are small. Can be kept in your or attached with key chain.

USB flash drives carry large capacity of data, up to 8GB USB flash drives.

USB flash drives are helpful to store personal information without saving them in computer hard drive in case of sharing of a computer with other peoples at work place.

Tape Drives

A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes of information without having to spend large sums of money on disks. Their transfer speeds also vary considerably. Fast tape drives can transfer as much as 20MB (megabytes) per second. Tape Drives software is generally easy to use and can usually be ran without supervision. While Tape Drives are cost efficient and easy to use one major disadvantage. Tape Drives have the speed which they backup and recover information. Tape drives are a sequential access device, which means to read any data on the Tape Drive; the Tape Drive must read all preceding data. Tape drives are available in various design and shape like 8mm tape drive similar to what are used in camcorder with the transfer rate up to 6M/Sec. Other is DLT (Digital Linear Tape) drive that is a robust and durable medium. The DLT segments the tape into parallel horizontal tracks and records data by streaming the tape across a single stationary head. Some other examples are DAT (Digital Audio Tape), QIC Standard. The disadvantage of tape drives is that they are *sequential-access* devices, which means that to read any particular block of data, it requires to read all the preceding blocks. This makes them much too slow for general-purpose storage operations. However, they are the least expensive media for making backups.

Zip Drives

Zip disks are high capacity(up to 100MB), removable, magnetic disks. ZIP disks are similar to floppy disks, except that they are much faster, and have a much greater capacity.

While floppy disks typically hold 1.44 megabytes, ZIP disks are available in two sizes, namely 100 megabytes and 250 megabytes. ZIP drives should not be confused with the super-floppy, a 120 megabyte floppy drive which also handles traditional 1.44 megabyte floppies. ZIP drives are available as internal or external units, using one of three interfaces:

- Small Computer Standard Interface (SCSI): Interface is the fastest, most sophisticated, most expandable, and most expensive interface. The SCSI interface is used by all types of computers from PC's to RISC workstations to minicomputers, to connect all types of peripherals such as disk drives, tape drives, scanners, and so on. SCSI ZIP drives may be internal or external, assuming your host adapter has an external connector.
- Integrated Drive Electronics (IDE): Interface is a low-cost disk drive interface used by many desktop PC's. Most IDE devices are strictly internal.
- The parallel port interface is popular for portable external devices such as external ZIP drives and scanners, because virtually every computer has a standard parallel port (usually used for printers). This makes things easy for people to transfer data between multiple computers by toting around their ZIP drive.

Zip disks can be used to store, backup, and move basic office application files, digital music, presentations, digital photos, digital video, etc. On the other hand, in spite of Iomega's claims that this drives "meet high capacity storage needs" for PC users, these products belong to the mobile storage rather than to the back-up category.

6.1.3 Network Protection Devices

System and network security is the term used to describe the methods and tools employed to prevent unauthorized and malicious access or modification of data on a system or during data transmission over network. Network security is not just for big corporations and government organizations only. The new breed of viruses, worms, and deceptive software that can infect computer or allow malicious hackers to unauthorized use of computers from any type of network interconnects. A bigger question arises what to protect on the network? The protection involves the following:

- Intrusion prevention.
- Intrusion detection.
- Web filtering.
- E-mail security.
- Security management.
- Integrated security appliance.
- Vulnerability assessment.

Network protection devices are used to preemptively protect computer network from viruses, worms and other Internet attacks. Intrusion detection and prevention, firewalls, vulnerability assessment, integrated security appliances, web filtering, mail security and a centralized management system, all work to maximize your network uptime and minimize the need for active administrator involvement.

Firewall used for all these provides only one entry point to your network. And if the modems are allowed to answer incoming calls, can provide an easy means for an attacker to sneak around the firewall. Just as castles weren't built with moats only in the front, then network needs to be protected at all of its entry points.

Secure Modems; Dial-Back Systems: If modem access is to be provided, this should be guarded carefully. The *terminal server*, or network device that provides dial-up access to your network needs to be actively administered, and its logs need to be examined for strange behaviour. Its password need to be strong. Accounts that are not actively used should be disabled. In short, it is the easiest way to get into your network from remote: guard it carefully. There are some remote access systems that have the feature of a two-part procedure to establish a connection. The first part is the remote user dialing into the system, and providing the correct user-Id and password. The system will then drop the connection, and call the authenticated user back at a known telephone number. Once the remote user's system answers that call, the connection is established, and the user is on the network. This works well for folks working at home, but can be problematic for users wishing to dial in from hotel rooms and such when on business trips. Other possibilities include one-time password schemes, where the user enters his user-Id, and is presented with a "challenge," a string of between six and eight numbers.

Crypto-Capable Routers: A feature that is being built into some routers is the ability to session encryption between specified routers. Because traffic travelling across the Internet can be seen by people in the middle, who have the resources (and time) to snoop around, these are advantageous for providing connectivity between two sites, such that there can be secure routes.

Virtual Private Networks

Given the ubiquity of the Internet, and the considerable expense in private leased lines, many organizations have been building *VPNs* (Virtual Private Networks). Traditionally, for an organization to provide connectivity between a main office and a satellite one, an expensive data line had to be leased in order to provide direct connectivity between the two offices. Now, a solution that is often more economical is to provide both offices connectivity to the Internet. Then, using the Internet as the medium, the two offices can communicate. The danger in doing this, of course, is that there is no privacy on this channel, and it's difficult to provide the other office access to "internal" resources without providing those resources to everyone on the Internet. VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although going over the Internet, is private (because the link is encrypted), and the link is convenient, because each can see each other's internal resources without showing them off to the entire world.

Wireless Network Protection

In case of wireless network, it requires to take an additional security steps when wireless access point is set up first. Wireless networks are protected by something called Wired Equivalent Privacy (WEP) encryption. There are two steps to enabling WEP:

Step-1 is the configuring the wireless access point: The wireless access point is the device that is probably connected to cable or DSL modem. Instructions for configuration will vary slightly for wireless access points from different manufacturers.

Step-2 is the configuring the wireless network adapter: The wireless network adapter is either plugged into computer, or that is built-in to computer. In case of an older wireless network adapter, it requires check with the manufacturer to find out which WEP key lengths it supports.

6.1.4 Surge Protectors

A surge is defined as a voltage increase that lasts for as little as three nanoseconds (one nanosecond is one billionth of a second), and significant damage can be done in that miniscule amount of time, if the voltage surge is strong enough. A spike, which lasts for only one or two nanoseconds, can also do its share of damage, especially when several spikes occur repeatedly over an extended period. Voltage surges and spikes occur for a number of reasons. Perhaps the most common is the sudden jump in voltage that occurs when high-power appliances such as refrigerators and air conditioners first start up. The appliances need quite a bit of electrical energy to activate compressors, and that sudden and sharp increase in flow through the lines will be felt by the electronics. A surge protector is necessary to protect electronics against "dirty" electricity. Electrical power has a standard voltage for most residential uses of 120 volts to 240 volts, and it remains relatively steady. But when that power makes a sharp and brief jump for any of a variety of reasons, the resulting sudden alteration in voltage can seriously damage delicate circuits.

Electricity is your computer's lifeblood. Power anomalies and surges also pose a big threat to computer equipment. But the power line that supplies your computer with electricity also carries the seeds of your computer's destruction. Surges that are brief pulses of high voltage they sneak down the power line and, in an instant, can destroy the circuits inside computer. The way to protect your computer from lightning and power surges is to use a good surge protector. A power strip, which is a simple strip of outlets, is not necessarily a surge protector. A surge protector may look like a power strip, but it has built-in protection against power surges. Surge protectors are simple to install, maintenance free and have become much more affordable. Surge protection units are available that offer four to six protected outlets in one protection "center," which makes it easy and convenient to protect not only the computer but the printer, fax, external modem, scanner and other home office components. Many of these units also offer surge protection for one or more phone lines. A good surge protector should offer four features.

- The surge protector should cover lightning strikes. Some do not.

- The surge protector should offer insurance to cover the loss of properly attached equipment.
- For a regular modem, get a surge protector with an R-11 telephone jack where it can be hooked up with telephone line.
- With a cable modem, use a surge protector which will also accommodate the television/Internet cable.

The performance of surge protectors is rated three ways that are clamping voltage, response time and energy absorption. The first, clamping voltage, tells what level of voltage surge has to occur before the surge protector activates and diverts the excess voltage to ground. With this rating, the lower the voltage number is the better the surge protector will perform. It takes less of a surge to activate. For good protection, especially for computers, a protector with a clamping voltage of less than 400 volts will be preferred. Response time is the amount of time it takes for the surge protector to respond to the surge. Obviously, a fast response time is important, so look for a unit that will respond in one nanosecond or less. Surge protectors are not made to last forever, so the third rating, energy absorption, indicates how much energy the unit will absorb before it fails. For this rating, look for a unit rated at 300 joules or better, up to around 600 joules for even better performance.

A surge protection strip or center is also well-suited for home entertainment components like TV, VCR, stereo, etc. While not as delicate as computers, providing good surge protection will certainly help extend the useful life of any of these components. Entertainment center surge protectors may also contain protection for a phone line and a cable TV line, and typically cost a little less than the ones designed for computer protection. Example of some most commonly used surge protectors are ISP3 Inline Surge Protector with audible alarm, ISP 4 (Inline Surge Protector), ISP 5-perfect protection, ISP6 (Inline Surge Protector) 'cloverleaf'.

UPS (Uninterruptible Power Supply)

A UPS (Uninterruptible Power Supply) is basically a battery back-up system to maintain power in the event of a power outage for computer. UPS provides power for a short time (usually 10 or 15 minutes) to the computer or other critical hardware when its primary power source is unavailable. A UPS keeps a computer running for several minutes after a power outage, enabling you to save data that is in RAM and shutdown the computer gracefully. Power spikes, sags, and outages can not only cause lose of unsaved work and precious data, they can also damage valuable hardware and network infrastructure.

It acts as a surge suppressor, filtering line noise and providing protection against spikes. But, in the event of a power outage it keeps your computer up and running, sounding an alarm and allowing you to close any running programs and shutdown your computer safely. There are various common power problems that UPS units are used to correct. They are as follows:

Power failure: Total loss of utility power, causes electrical equipment to stop working.

Voltage sag: Transient (short term) under-voltage that causes flickering of lights.

Voltage spike: Transient (short term) over-voltage i.e., spike or peak that causes wear or acute damage to electronic equipment.

Under-voltage (brownout): Low line voltage for an extended period of time that causes overheating in motors.

Over-voltage: Increased voltage for an extended period of time that causes light bulbs to fail.

Line noise: Distortions superimposed on the power waveform that causes electromagnetic interference.

Frequency variation: Deviation from the nominal frequency (50 or 60 Hz) that causes motors to increase or decrease speed and line-driven clocks and timing devices to gain or lose time.

Switching transient: Instantaneous undervoltage (notch) in the range of nanoseconds. May cause erratic behaviour in some equipment, memory loss, data error, data loss and component stress.

Harmonic distortion: Multiples of power frequency superimposed on the power waveform that causes excess heating in wiring and fuses.

There are two basic types of UPS systems available in the market one is on-line UPS systems. And other one is off-line UPS systems (also known as standby power systems. An on-line UPS always powers the load from its own internal energy supply, which is in turn continuously charged by the input power. An SPS monitors the power line and switches to battery power as soon as it detects a problem. The switch to battery, however, can require several milliseconds, during which time the computer is not receiving any power. Standby Power Systems are sometimes called Line-interactive UPSs. An on-line UPS avoids these momentary power lapses by constantly providing power from its own inverter, even when the power line is functioning properly. In general, on-line UPSs are much more expensive than SPSs. In a standby (off-line) system the load is powered directly by the input power and the backup power circuitry is only invoked when the utility power fails.

Most UPS below 1 kVA are of the standby variety which are cheaper, though inferior to on-line systems which have no delay between a power failure and backup power being supplied. A true ‘uninterruptible’ system is a double-conversion system. In a double-conversion system alternating current (AC) comes from the power grid, goes to the battery (direct current or DC), then is converted back to AC power. Most systems sold for the general market, however, are of the “standby” type where the output power only draws from the battery, if the AC power fails or weakens. For large power units, Dynamic Uninterruptible Power Supply are sometimes used. A synchronous motor/alternator is connected on the mains via a choke. Energy is stored in a flywheel. When the mains fails, an Eddy-current regulation maintains the power on the load. DUPS are sometimes combined or integrated with a diesel-genset. In recent years, Fuel cell UPS have been developed that uses hydrogen and a fuel cell as a power source potentially providing long run times in a small space. A fuel cell replaces the batteries as energy storage used in all UPS design.

6.1.5 RAID Technology

RAID is also known as redundant array of independent disks or often incorrectly known as redundant array of inexpensive disks. RAID is a system of using multiple hard drives for sharing or replicating data among the drives. Depending on the version chosen, the benefit of RAID is one or more of increased data integrity, fault-tolerance, throughput or capacity compared to single drives. In its original implementations its key advantage is the ability to combine multiple low-cost devices using older technology into an array that offeres greater capacity, reliability, or speed, or a combination of these things, than affordably available in a single device using the newest technology.

At the very simplest level, RAID combines multiple hard drives into one single logical unit. Thus, instead of seeing several different hard drives, the operating system sees only one. RAID is typically used on server computers, and is usually implemented with identically-sized disk drives. With decreases in hard drive prices and wider availability of RAID options built into motherboard chipsets. RAID is also being found and offered as an option in more advanced end user computers. This is especially true in computers dedicated to storage-intensive tasks, such as video and audio editing.

The RAID specification suggests a number of prototype “RAID levels”, or combinations of disks. Each had theoretical advantages and disadvantages. Over the years, different implementations of the RAID concept have appeared. Most differ substantially from the original idealized RAID levels, but the numbered names have remained. The very definition of RAID has been argued over the years. The use of the term *redundant* leads many to split hairs over whether RAID 0 is a “real” RAID type. Similarly, the change from *inexpensive* to *independent* confuses many as to the intended purpose of RAID. There are even some single-disk implementations of the RAID concept. For the purpose of this article, we will say that any system which employs the basic RAID concepts to recombine physical disk space for purposes of reliability, capacity, or performance is a RAID system. There are number of different RAID levels:

Level 0—RAID (Striped Disk Array without fault tolerance)

Level 1—RAID (Mirroring and Duplexing)

Level 2—RAID (Error-Correcting Coding)

Level 3—RAID (Bit-Interleaved Parity)

Level 4—RAID (Dedicated Parity Drive)

Level 5—RAID (Block Interleaved Distributed Parity)

Level 6—RAID (Independent Data Disks with Double Parity)

Nested RAID levels: Many storage controllers allow RAID levels to be nested. That is, one RAID can use another as its basic element, instead of using physical disks.

Hardware and Software of RAID

RAID can be implemented either in dedicated hardware or custom software running on standard hardware. Additionally, there are hybrid RAIDs that are partly software and partly hardware-based solutions. With a software implementation, the operating system manages the disks of the array through the normal drive controllers like IDE (Integrated Drive Electronics)/ATA (Advanced Technology Attachment), SCSI (Small Computer System Interface) and Fibre Channel or any other. With present CPU speeds, software RAID can be faster than hardware RAID, though at the cost of using CPU power which might be best used for other tasks. One major exception is where the hardware implementation of RAID incorporates a battery backed-up write cache and an application, like a database server. In this case, the hardware RAID implementation flushes the write cache to a secure storage to preserve data at a known point if there is a crash. The hardware approach is faster and limited instead by RAM speeds, the amount of cache and how fast it can flush the cache to disk. For this reason, battery-backed caching disk controllers are often recommended for high transaction rate database servers. In the same situation, the software solution is limited to no more flushes than the number of rotations or seeks per second of the drives. Another disadvantage of a pure software RAID is that, depending on the disk that fails and the boot arrangements in use, the computer may not be able to be rebooted until the array has been rebuilt.

A hardware implementation of RAID requires (at a minimum) a special-purpose RAID controller. On a desktop system, this may be a PCI (Peripheral Component Interconnect) expansion card, or might be a capability built in to the motherboard. In larger RAIDs, the controller and disks are usually housed in an external multi-bay enclosure. The disks may be IDE, ATA, SATA, SCSI, Fibre Channel, or any combination thereof. The controller links to the host computer(s) with one or more high-speed SCSI, Fibre Channel or ISCSI (Internet SCSI) connections, either directly, or through a fabric, or is accessed as network attached storage. This controller handles the management of the disks, and performs parity {In computing and telecommunication, a parity bit is a binary digit that takes on the value zero or one to satisfy a constraint on the overall parity of a binary number. The *parity scheme* in use must be specified as even or odd (also called *even parity* and *odd parity*, respectively). Parity is even if there are an even number of ‘1’ bits, and odd otherwise} calculations (needed for many RAID levels). This option tends to provide better performance, and makes operating system support easier. Hardware implementations also typically support hot swapping, allowing failed drives to be replaced while the system is running. In rare cases hardware controllers have become faulty, which can result in data loss. Because of this drawback, software RAID is a slightly more reliable and safer option.

Hybrid RAIDs have become very popular with the introduction of very cheap *hardware RAID controllers*. The hardware is just a normal disk controller that has no RAID features, but there is a boot-time set-up application that allows users to set up RAIDs that are controlled via the BIOS(Basic input output systems) . When any modern operating systems are used, they will need specialized RAID drivers that will make the array look like a single block device. Since these controllers actually do all the calculations in software, not hardware, they are often called “fakeraids”. Unlike software RAID, these “fakeraids” typically cannot span multiple controllers.

Both hardware and software versions may support the use of a *hot spare* (A hot spare is a disk or group of disk used to automatically or manually, depending on the Hot spare policy, replace a failing disk in a RAID), a preinstalled drive which is used to immediately (and almost always automatically) replace a failed drive. This cuts down the time period in which a second failure can take out the array. Some software RAID systems allow building arrays from partitions instead of whole disks. Unlike Matrix RAID they are not limited to just RAID 0 and RAID 1 and not all partitions have to be RAID.

Reliability Factors of RAID

There are some important factors affecting the relaibility of RAID configuration like failure rate of disk, mean time of data loss and mean time of recovery.

Failure rate: A failure rate is the average frequency with which something fails. Failure rate can be defined as " The total number of failures within an item population, divided by the total time expended by that population, during a particular measurement interval under stated conditions. (MacDiarmid, et al.)" The meantime to failure of a given RAID may be lower or higher than those of its constituent hard drives, depending on what type of RAID is employed.

Mean Time to Data Loss (MTTDL): In this context, the meantime to elapse before a loss of user data in a given array, usually measured in hours.

Mean Time to Recovery (MTTR): Meantime to recovery is the average time that a device will take to recover from a non-terminal failure. Examples of such devices range from self-resetting fuses (where the MTTR would be very short, probably seconds), up to whole systems which have to be replaced. In arrays that include redundancy for reliability, this is the time following a failure to restore an array to its normal failure-tolerant mode of operation. This includes time to replace a failed disk mechanism as well as time to rebuild the array (i.e., to replicate data for redundancy).

6.1.6 Server Specific Jargon

In the client/server environment servers are also computers like other workstations with some configurational differences where processing speed is measured megahertz (MHz), hard disk capacity measured in gigabytes (GB), data transfer rates measured in milliseconds (MS); apart from these, there are some server specific jargon that are useful to know like EDC Memory, Memory Cache, Rack Mounting, Power Protection, RAID and Symmetrical Multiprocessing.

EDC Memory

Error Detection and Correction (EDC) such type of memory is configured at the hardware level with special circuitry that verifies RAM output and resends output whenever the memory errors occur. This type of memory is used to boost overall reliability of servers and tending to become standard equipment.

Memory Cache

Memory cache sets aside a portion of the server RAM to store the most frequently used network instructions so that these instructions can be accessed as soon as possible. While the server is in operation cache storage is being constantly updated. While network processing, less frequently accessed instructions are pushed out of cache, replaced by instructions that are accessed more frequently. The larger the size of the memory cache, the more instructions the server can keep on hand for fast access.

Rack Mounting

A rack mount server usually refers to multiple servers stacked on top of one another in a single cabinet to save space. In case of very large client/server a system that requires more than a single file server rack mount can be used, where the system is complex and highly centralized.

Power Protection

Power supply is a unit that distributes electricity within the server. A RDS redundant power supply is a backup power supply that takes over in the event that the main power supply fails. This feature is different from an UPS (uninterruptible power supply) an external device that provides continuous electrical power to the server, usually for a short time, in the event of an electrical power failure. Details of UPS has already discussed in Section 6.1.4, i.e. surge protectors, RDS keeps the network running indefinitely, as long as electricity is being fed to it on other hand UPS keeps the network running just long enough after a power failure to store and protect data before shuting down. A line conditioner that is another form of power protectors can be used to monitor the electrical current and compensates for extreme fluctuations (i.e. *spikes,* burst of too much voltage or *brownouts,* sudden drop in voltage).

Symmetrical Multiprocessing

Symmetrical Multiprocessing (SMP) technology is used to integrate the power of more than one central processor into a single file server, along with necessary additional hardware and software to divide processing chores between them. There is a drastic effect on the server speed by using multiple processors, although it is not as simple as doubling speed with two processors or tripling speed with three. SMP involves additional processing overhead to manage the distribution of processing among those multiple processors. In case of big client/server systems where a large scale networks is involved the features of SMP are used.

6.2 SOFTWARE REQUIREMENTS

6.2.1 Client OS

The client always provides presentation services, all the user Input and Output are presented at client workstation. Software to support specific functions like field edits, context-sensitive help, navigation, training, personal data storage, and manipulation frequently get executes on the client workstation. All these functions use the GUI and windowing functionality. Additional business logic for calculations, selection, and analysis can reside on the client workstation. A client workstation uses a local operating system to host both basic services and the network operating system interfaces. This operating system may be the same or different from that of the server. Numbers of OS are installed depending upon the application and user requirement running on Client/Server environment. There are various OS are in use as a client platform like DOS, Windows 3.1, OS/2, UNIX, Windows NT (New Technology), AIX and Mc systems 7. The client workstation frequently provides personal productivity functions, such as word processing, which use only the hardware and software resident right on the workstation. When the client workstation is connected to a LAN, it has access to the services provided by the network operating system (NOS) in addition to those provided by the client workstation. The workstation may load software and save word-processed documents from a server and therefore use the file server functions provided through the NOS. It also can print to a remote printer through the NOS. The client workstation may be used as a terminal to access applications resident on a host minicomputer or mainframe processor. This enables the single workstation to replace the terminal, as well as provide client workstation functionality.

6.2.2 Server OS

Servers provide the platform for application, database, and communication services also the server provides and controls shared access to server resources. Applications on a server must be isolated from each other so that an error in one cannot damage another. Preemptive multitasking ensures that no single task can take overall the resources of the server and prevent other tasks from providing service. There must be a means of defining the relative priority of the tasks on the server. These requirements are specific to the Client/Server implementation and not to the file server implementation. Because file servers execute only the single task of file service, they can operate in a more limited operating environment without the need for application isolation and preemptive multitasking.

The server is a multiuser computer. There is no special hardware requirement that turns a computer into a server. The hardware platform should be selected based on application demands and economics. There is no pre-eminent hardware technology for the server. The primary characteristic of the server is its support for multiple simultaneous client requests for service. Therefore, the server must provide multitasking support and shared memory services. Servers for Client/Server applications work best when they are configured with an operating system that supports shared memory, application isolation, and preemptive multitasking. High-end Intel, RISC (including Sun SPARC, IBM/Motorola PowerPC, HP PA RISC, SGI MIPS, and DEC Alpha), IBM System/370, and DEC VAX processors are all candidates for the server platform. The server is responsible for managing the server-requester interface so that an individual client request response is synchronized and directed back only to the client requester. This implies both security when authorizing access to a service and integrity of the response to the request. Some of the operating system dominating the server word nowadays are NetWare, Windows NT, OS/2, MVS, VMS, and UNIX.

NetWare

In 2003, Novell announced the successor product to NetWare (Open Enterprise Server OES). Later on completes the separation of the services traditionally associated with NetWare like directory services, file, and printer from the platform underlying the delivery of those services. OES is essentially a set of applications (eDirectory, NetWare Core Protocol services, iPrint, etc.) that can run a top either a Linux or a NetWare kernel platform. Also known as self-contained operating system so does not requires separate operating system to run.

OS/2

The last released version was 4.0 in 1996. Early versions found their way into embedded systems and still, as of mid-2003, run inside many of the world's automated teller machines. Like Unix, OS/2 was built to be preemptively multitasking and would not run on a machine without an MMU (early versions simulated an MMU using the 286's memory segmentation). Unlike Unix, OS/2 was never built to be a multiuser system. Process-spawning was relatively cheap, but IPC was difficult and brittle. Networking was initially focused on LAN protocols, but a TCP/IP stack was added in later versions. There were no programs analogous to Unix service daemons, so OS/2 never handled multi-function networking very well. OS/2 had both a CLI and GUI. Most of the positive legendary around OS/2 was about the Workplace Shell (WPS), the OS/2 desktop. The combination of Novell with an OS/2 database and application servers can provide the necessary environment for a production-quality Client/Server implementation.

Windows NT

Windows NT (New Technology) is Microsoft's operating system released in september 1993, for high-end personal and server use. Microsoft staked its unique position with a server operating system. Microsoft's previous development of OS/2 with IBM did not create the single standard UNIX alternative that was hoped for. NT provides the preemptive multitasking services required for a functional server. It provides excellent support for Windows clients and incorporates the necessary storage protection services required for a reliable server operating system.

NT has file attributes in some of its file system types. They are used in a restricted way, to implement access-control lists on some file systems, and do not affect development style very much. It also has a record-type distinction, between text and binary files, that produces occasional annoyances (both NT and OS/2 inherited this misfeature from DOS).

NT systems on the Internet are notoriously vulnerable to worms, viruses, defacements, and cracks of all kinds. There are many reasons for this, some more fundamental than others. The most fundamental is that NT's internal boundaries are extremely porous. Because Windows does not handle library versioning properly, it suffers from a chronic configuration problem called "DLL hell", in which installing new programs can randomly upgrade (or even downgrade!) the libraries on which existing programs depend. This applies to the vendor-supplied system libraries as well as to application-specific ones: it is not uncommon for an application to ship with specific versions of system libraries, and break silently when it does not have them. On the bright side, NT provides sufficient facilities to host Cygwin, which is a compatibility layer implementing Unix at both the utilities and the API level, with remarkably few compromises. Cygwin permits C programs to make use of both the Unix and the native APIs, and is the first thing many Unix hackers install on such Windows systems as they are compelled by circumstances to make use of. The intended audience for the NT operating systems is primarily nontechnical end users, implying a very low tolerance for interface complexity. It is used in both client and server roles. Early in its history Microsoft relied on third-party development to supply applications. They originally published full documentation for the Windows APIs, and kept the price of development tools low. But over time, and as competitors collapsed, Microsoft's strategy shifted to favor in-house development, they began hiding APIs from the outside world, and development tools grew more expensive.

MVS

MVS (Multiple Virtual Storage) is IBM's flagship operating system for its mainframe computers as a platform for large applications. MVS is the only one OS that could be considered older than Unix. It is also the least influenced by Unix concepts and technology, and represents the strongest design contrast with Unix. The unifying idea of MVS is that all work is batch; the system is designed to make the most efficient possible use of the machine for batch processing of huge amounts of data, with minimal concessions to interaction with human users. MVS uses the machine MMU; processes have separate address spaces. Interprocess communication is supported only through shared memory. There are facilities for threading (which MVS calls "subtasking"), but they are lightly used, mainly because the facility is only easily accessible from programs written in assembler. Instead, the typical batch application is a short series of heavyweight program invocations glued together by JCL (Job Control Language) which provides scripting, though in a notoriously difficult and inflexible way. Programs in a job communicate through temporary files; filters and the like are nearly impossible to do in a usable manner. The intended role of MVS has always been in the back office. Like VMS and Unix itself, MVS predates the server/client distinction. Interface complexity for back-office users is not only tolerated but expected, in the name of making the computer spend fewer expensive resources on interfaces and more on the work it's there to get done.

VMS

OpenVMS is a multi-user, multiprocessing virtual memory-based operating system (OS) designed for use in time sharing, batch processing, real time (process priorities can be set higher than OS kernel jobs) and transaction processing. It offers high system availability through clustering, or the ability to distribute the system over multiple physical machines. This allows the system to be "disaster-tolerant" against natural disasters that may disable individual data-processing facilities. VMS also includes a process priority system that allows for real-time process to run unhindered, while user processes get temporary priority "boosts" if necessary Open VMS commercialized many features that are now considered standard requirements for any high-end server operating system. OpenVMS commercialized many features that are now considered standard requirements for any high-end server operating system. These include Integrated computer networking, a distributed file system , Integrated database features and layered databases including relational database, Support for multiple computer programming languages, Hardware partitioning of multiprocessors, High level of security. Enterprise class environments typically select and use OpenVMS for various purposes including as a mail server, network services, manufacturing or transportation control and monitoring, critical applications and databases, and particularly environments where system uptime and data access is critical.

UNIX

Unix operating system developed in 1969 by a group of AT&T employees at Bell Labs including Ken Thompson, Dennis Ritchie and Douglas McIlroy. During the late 1970s and early 1980s, Unix's influence in academic circles led to large-scale adoption of Unix by commercial startups, the most notable of which is Sun Microsystems. Today, in addition to certified Unix systems, Unix-like operating systems such as Linux and BSD derivatives are commonly encountered. Sometimes, "traditional Unix" may be used to describe a Unix or an operating system that has the characteristics of either Version 7 Unix or UNIX System V.

Unix operating systems are widely used in both servers and workstations. The Unix environment and the Client/Server program model were essential elements in the development of the Internet and the reshaping of computing as centered in networks rather than in individual computers. Unix was designed to be portable, multi-tasking and multi-user in a time-sharing configuration. Unix systems are characterized by various concepts like the use of plain text for storing data, a hierarchical file system, treating devices and certain types of inter-process communication (IPC) as files and the use of a large number of small programs that can be strung together through a command line interpreter using pipes, as opposed to using a single monolithic program that includes all of the same functionality. Unix operating system consists of many of these utilities along with the master control program, the kernel. The kernel provides services to start and stop programs, handle the file system and other common "low level" tasks that most programs share, and, perhaps most importantly, schedules access to hardware to avoid conflicts if two programs try to access the same resource or device simultaneously. To mediate such access, the kernel was given special rights on the system, leading to the division between *user-space* and *kernel-space.*

6.2.3 Network OS

A Network Operating System (NOS) is a systen software that controls a network and its message (e.g., packet) traffic and queues, controls access by multiple users to network resources such as files, and provides for certain administrative functions, including security. Also includes special functions for connecting computers and devices into a local-area network (LAN) or Inter-networking. A Network Operating System (NOS) is an operating system that has been specifically written to keep networks running at optimal performance with a native structure for use in a network environment. Some of the important features of Network Operating System includes:

- Provide file, print, web services, back-up and replication services.
- Provide basic operating system features such as support for processors, protocols, automatic hardware detection and support multi-processing of applications.
- Security features such as authentication, authorization, logon restrictions and access control.
- Provide name and directory services.
- User management and support for logon and logoff, remote access, system management, administration and auditing tools with graphic interfaces.
- Support Internetworking such as routing and WAN ports.

Some of the components that an NOS usually has built in that a normal operating system might not have are built in NIC (network interface card) support, file sharing, server log on, drive mapping, and native protocol support. Most operating systems can support all of these components with add-on either by the original manufacture of the operating system or from a third party vendor. Some of the operating system dominating the networking OS are Novell NetWare, LAN Manager, IBM LAN Server, Banyan VINES etc.

Novell NetWare

NetWare is a network operating system developed by Novell, Inc. The latest version of NetWare is v6.5 Support Pack 7, which is identical to OES 2, NetWare Kernel. It initially used cooperative multitasking to run various services on a PC, and the network protocols were based on the archetypal Xerox XNS stack. NetWare has been superseded by Open Enterprise Server (OES). With Novell NetWare, disk space was shared in the form of NetWare volumes, comparable to DOS volumes. Clients running MS-DOS would run a special Terminate and Stay Resident (TSR) program that allowed them to *map* a local drive letter to a NetWare volume. Clients had to log in to a server in order to be allowed to map volumes, and access could be restricted according to the login name. Similarly, they could connect to the shared printers on the dedicated server, and print as if the printer was connected locally.

Novell had introduced limited TCP/IP support in NetWare v3.x (circa 1992) and v4.x (circa 1995), consisting mainly of FTP services and UNIX-style LPR/LPD printing (available in NetWare v3.x), and a Novell-developed webserver (in NetWare v4.x). Native TCP/IP support for the client file and print services normally associated with NetWare was introduced in NetWare v5.0. Most network protocols in use at the time NetWare was developed didn't trust the network to deliver messages. A typical client file read would work something like this:

- Client sends read request to server.
- Server acknowledges request.
- Client acknowledges acknowledgement.
- Server sends requested data to client.
- Client acknowledges data.
- Server acknowledges acknowledgement.

In contrast, NCP was based on the idea that networks worked perfectly most of the time, so the reply to a request served as the acknowledgement. Here is an example of a client read request using this model:

- Client sends read request to server.
- Server sends requested data to client.

All requests contained a sequence number, so if the client didn't receive a response within an appropriate amount of time it would re-send the request with the same sequence number. If the server had already processed the request it would re-send the cached response, if it had not yet had time to process the request it would send a 'positive acknowledgement' which meant, "I received your request but I haven't gotten to it yet so don't bug me." The bottom line to this 'trust the network' approach was a 2/3 reduction in network traffic and the associated latency. In 4.x and earlier versions, NetWare did not support preemption, virtual memory, graphical user interfaces etc. Processes and services running under the NetWare OS were expected to be cooperative, that is to process a request and return control to the OS in a timely fashion. On the down side, this trust of application processes to manage themselves could lead to a misbehaving application bringing down the server.

LAN Manager

LAN Manager is a network operating system developed by Microsoft developed in cooperation with 3Com (Computers, Communication and Compatibility) that runs as a server application under OS/2. It supports DOS, Windows and OS/2 clients. LAN Manager provides client support for DOS, Windows, Windows NT, OS/2, and Mac System 7. Server support extends to NetWare, AppleTalk, UNIX, Windows NT, and OS/2. Client workstations can access data from both NetWare and LAN Manager Servers at the same time. LAN Manager supports NetBIOS and Named Pipes LAN communications between clients and OS/2 servers. Redirection services are provided to map files and printers from remote workstations for client use. LAN Manager was superseded by Windows NT Server, and many parts of LAN Manager are used in Windows NT and 2000.

IBM LAN Server

A network operating system developed by IBM that runs as a server application under OS/2 and supports DOS, Windows and OS/2 clients. Originally based on LAN Manager when OS/2 was jointly developed by IBM and Microsoft, starting with LAN Server 3.0, it runs only under IBM's version of OS/2. Short term LAN Server refers to the IBM OS/2 LAN Server product. There were also LAN Server products for other operating systems, notably AIX (now called Fast Connect) and OS/400. LAN server is a file server in a network. LAN Server provides disk mirroring, CID capability and Network Transport Services/2 (NTS/2) for concurrent access to NetWare servers. Options are LAN Server for the Macintosh for Mac client access and System Performance/2 (SP/2), a series of network management utilities. LAN Server, are the standard products for use in Client/Server implementations using OS/2 as the server operating system. LAN Manager/X is the standard product for Client/Server implementations using UNIX System V as the server operating system.

Banyan VINES

Banyan VINES (Virtual Integrated Network Service) is developed during 1980. Banyan VINES is a computer network operating system and set of computer network protocols, it used to talk to client machines on the network. In other words Banyan VINES is a network operating system with a UNIX kernel that allows clients operating systems such as DOS, OS/2, Windows, and those for Macintosh systems to share information and resources with each other and with host computing systems. VINES provide full UNIX NFS (Network File System) support in its core services and the Transmission Control Protocol/Internet Protocol (TCP/IP) for transport, it also includes Banyan's StreetTalk Directory Services, one of the first viable directory services to appear in a network operating system.

VINES ran on a low-level protocol known as VIP (VINES Internetwork Protocol) essentially identical to the lower layers of XNS), addresses consisted of a 32-bit address and a 16-bit subnet, which mapped onto the 48-bit Ethernet address in order to route to machines. This meant that, like other XNS-based systems, VINES could only support a two-level internet. However, a set of routing algorithms set VINES apart from other XNS systems at this level. The key differentiator, ARP (Address Resolution Protocol), allowed VINES clients to automatically set up their own network addresses. When a client first booted up it broadcast a request on the subnet asking for servers, which would respond with suggested addresses. The client would use the first to respond, although the servers could hand off better routing instructions to the client if the network changed. The overall concept very much resembled AppleTalk's AARP system, with the exception that VINES required at least one server, whereas AARP functioned completely headlessly. Like AARP, VINES required an inherently chatty network, sending updates about the status of clients to other servers on the internetwork. At the topmost layer, VINES provided the standard file and print services, as well as the unique StreetTalk, likely the first truly practical globally consistent name service for an entire internetwork. Using a globally distributed, partially replicated database, StreetTalk could meld multiple widely separated networks into a single network that allowed seamless resource sharing. It accomplished this through its rigidly hierarchical naming scheme; entries in the directory always had the form *item@group@organization*. This applied to user accounts as well as to resources like printers and file servers. VINES client software ran on most PC-based operating systems, including MS-DOS and earlier versions of Microsoft Windows. It was fairly light weight on the client, and hence remained in use during the later half of the 1990s, when many machines not up to the task of running other networking stacks then in widespread use. This occurred on the server side as well, as VINES generally offered good performance even from mediocre hardware.

6.3 COMMUNICATION INTERFACE TECHNOLOGY

For the data communication to be taking place on a network, four basic elements are involved there:

Sender: the device that creates and transmits the data.

Message: the data to be sent. It could be a spreadsheet, database, or document, converted to digital form.

Medium: the physical material that connects the devices and carries the data from the sender to the receiver. The medium may consist of an electrical wire or airwaves.

Receiver: the destination device for the data.

To communicate with other devices, a sending device must know and follow the rules for sending data to receiving devices on the network. These rules for communication between devices are called *protocols*. Numerous standards have been developed to provide common foundations for data transmission. The International Standards Organization (ISO) has divided the required communication functions into seven levels to form the Open Systems Interconnections (OSI) model. Each layer in the OSI model specifies a group of functions and associated protocols used at that level in the source device to communicate with the corresponding level in the destination device.

Connectivity and interoperability between the client and the server are achieved through a combination of physical cables and devices and software that implements communication protocols. To communicate on a network the following components are required:

- A network interface card (NIC) or network adapter.
- Software driver.
- Communication protocol stack.

Computer networks may be implemented using a variety of protocol stack architectures, computer buses or combinations of media and protocol layers, incorporating one or more of among the LAN Cabling, WAN, Ethernet, IEEE NIC, Token Ring, Ethernet and FDDI.

6.3.1 Network Interface Card

The physical connection from the computer to the network is made by putting a network interface card (NIC) inside the computer and connecting it to the shared cable. A network interface card is a device that physically connects each computer to a network. This card controls the flow of information between the network and the computer. The circuit board needed to provide network access to a computer or other device, such as a printer. Network interface cards, or NICs, mediate between the computer and the physical media, such as cabling, over which transmissions travel. NIC is an adapter card that is installed in the controller that allows it to connect to a network (for example, Ethernet and Token Ring etc. The card contains both the hardware to accommodate the cables and the software to use the network's protocols. The NIC is also called a network adapter card.

6.3.2 LAN Cabling

LAN is data communication network, which connects many computers or client workstations and permits exchange of data and information among them within a localized area (2 to 5 Km). Where all connected devices share transmission media (cable) and also each connection device can work either stand alone or in the network. Each device connected in the network can communicate with any other device with a very high data transmission rate that is of 1Mbps to 100Mbps. Due to rapid change in technology, design and commercial applications for the LANs the number of approaches has emerged like High speed wireless LAN fast Ethernet. At the result, in many applications the volume of data handled over the LAN has been increased. For example in case of centralized server farms there is need for higher speed LAN. There is a need for client system to be able to draw huge amount of data from multiple centralized servers.

6.3.3 WAN

WAN (Wide area network) is a data communications network that covers a large geographical area such as cities, states or countries. WAN technologies generally function at the lower three layers of the OSI reference model, the physical layer, the data-link layer, and the network layer. WAN consists of a number of interconnected switching nodes via telephone line, satellite or microwaves links. A transmission form any one device is routed through internal nodes to the specific destination device. In WAN two computing device are not connected directly, a network of 'switching nodes' provides a transfer path and the process of transferring data block from one node to another is called data switching. Further this switching technique utilizes the routing technology for data transfer. Whereas the routing is responsible for searching a path between source and destination nodes. Earlier WAN have been implemented using circuit or packet switching technology, but now frame relay, ATM and wireless networks are dominating the technology.

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, bridge, gateway, repeater, brouter, modems, CSU/DSUs and ISDN terminal adapters. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

6.3.4 ATM

Asynchronous Transfer Mode (ATM) is a connection-oriented technology, in which a logical connection is established between the two end points before the actual data exchange begins. ATM has proved very successful in the WAN scenario and numerous telecommunication providers have implemented ATM in their wide-area network cores ATM is a cell relay, packet switching network and data link layer protocol which encodes data traffic into small (53 bytes; 48 bytes of data and 5 bytes of header information) fixed-sized cells. ATM provides data link layer services that run over Layer 1 links. This differs from other technologies based on packet-switched networks (such as the Internet Protocol or Ethernet), in which variable sized *packets* (known as *frames* when referencing layer 2) are used. The motivation for the use of small data *cells* was the reduction of jitter (delay variance, in this case) in the multiplexing of data streams; reduction of this (and also end-to-end round-trip delays) is particularly important when carrying voice traffic. An ATM network is designed to be able to transfer many different types of traffic simultaneously, including real time flows such as video, voice and bursty TCP flows. ATM services are categorised into mainly two categories one is Real-Time Services and other one is Non-real-Time Services which are used by an end system to identify the type of service required. RTS concerns the delay and the variability of delay, referred to as jitter, that the application can tolerate. Real time applications typically involve a flow of information to a user that is intended to reduce that flow at a source. Constant Bit Rate services are the simplest real time services. CBR are used by the applications that requires a fixed data rate that is continuously available during the connections lifetime and a relatively tight upper bound on transfer delay. CBR applications are used mostly in video conferencing, interaction audio and audio/video retrieval and distribution. Real time variable bit rate (rtVB) are another real-time services that allows the network more flexibility than CBR. The network is able to statistically multiplex a number of connections over the same dedicated capacity and still provide the required service to each connection.

6.3.5 Ethernet

Ethernet is a family of frame-based computer networking technologies for Local Area Networks (LANs) that is also based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium. The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access. The communication methods used shows some similarities to radio systems, although there are fundamental differences, such as the fact that it is much easier to detect collisions in a cable broadcast system than a radio broadcast. The coaxial cable was replaced with point-to-point links connected by hubs and/or switches to reduce installation costs, increase reliability, and enable point-to-point management and troubleshooting. StarLAN was the first step in the evolution of Ethernet from a coaxial cable bus to a hub-managed, twisted-pair network.

Eathernet is most widely used LAN technology to get connected PCs and workstations more than 84% world wide due to its protocol that has following characteristics:

- Is easy to understand, implement, manage, and maintain.
- Allows low-cost network implementations.
- Provides extensive topological flexibility for network installation.
- Guarantees successful interconnection and operation of standards.
- Compliant products, regardless of manufacturer.

Ethernet LANs consist of network nodes and interconnecting media. The network nodes fall into two major classes:

- Data Terminal Equipment (DTE)—Devices that are either the source or the destination of data frames. DTEs are typically devices such as PCs, workstations, file servers, or print servers that, as a group, are all often referred to as end stations.
- Data Communication Equipment (DCE)—Intermediate network devices that receive and forward frames across the network. DCEs may be either stand alone devices such as repeaters, network switches, and routers, or communications interface units such as interface cards and modems.

6.3.6 Token Ring

Token-Ring was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5. Physically, a token ring network is wired as a star, with 'hubs' and arms out to each station and the loop going out-and-back through each. Stations on a token ring LAN are logically organized in a ring topology with data being transmitted sequentially from one ring station to the next with a control token circulating around the ring controlling access. Token ring is a local area network protocol which resides at the Data Link Layer (DLL) of the OSI model. It uses a special three-byte frame called a token that travels around the ring. Token ring frames travel completely around the loop.

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time. If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks. Token ring networks had significantly superior performance and reliability compared to early shared-media implementations of Ethernet (IEEE 802.3), and were widely adopted as a higher-performance alternative to the shared-media Ethernet.

6.3.7 FDDI

FDDI (Fiber Distributed Data Interface), as a product of American National Standards Institute X3T9.5 (now X3T12), conforms to the Open Systems Interconnection (OSI) model of functional layering of LANs using other protocols.

FDDI provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium, it uses optical fiber (though it can use copper cable, in which case one can refer to CDDI). A FDDI network contains two token rings (dual-ring architecture) with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. Secondary ring also provides possible backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km. FDDI has a larger maximum-frame size than standard 100 Mbit/s ethernet, allowing better throughput. The primary purpose of the dual rings is to provide superior reliability and robustness.

6.3.8 TCP/IP

The Internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It has also been referred to as the TCP/IP protocol suite, which is named after two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP is referred as protocol suite because it contains many different protocols and therefore many different ways for computers to talk to each other. TCP/IP is not the only protocol suite, although TCP/IP has gained wide acceptance and is commonly used. TCP/IP also defines conventions by connecting different networks, and routing traffic through routers, bridges, and other types of connections. The TCP/IP suite is result of a Defence Advanced Research Projects Agency (DARPA) research project about network connectivity, and its availability has made it the most commonly installed network software.

6.3.9 SNMP

The Simple Network Management Protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. In typical SNMP usage, there are a number of systems to be managed, and one or more systems managing them. A software component called an *agent* runs on each managed system and reports information via SNMP to the managing systems. An SNMP-managed network consists of three basic key components:

- Managed devices
- Agents
- Network-Management Systems (NMSs)

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be any type of device including, but not limited to, routers and access servers, switches and bridges, hubs, IP telephones, computer hosts, or printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

6.3.10 NFS

Network File System (NFS) is a network file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system. Assuming a Unix-style scenario in which one machine (the client) requires access data, stored on another machine (the NFS server).

The server implements NFS daemon processes (running by default as NFSD) in order to make its data generically available to clients. The server administrator determines what to make available, exporting the names and parameters of directories (typically using the/etc./exports configuration file and the exports command).

The server security-administration ensures that it can recognize and approve validated clients. The server network configuration ensures that appropriate clients can negotiate with it through any firewall system. The client machine requests access to exported data, typically by issuing a mount command. If all goes well, users on the client machine can then view and interact with mounted file systems on the server within the parameters permitted.

6.3.11 SMTP

Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the Internet developed during 1970's. SMTP is a relatively simple, text-based protocol, in which one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. It is a Client/Server protocol, whereby a client transmits an e-mail message to a server. Either an end-user's e-mail client, a.k.a. MUA (Mail User Agent), or a relaying server's MTA (Mail Transfer Agents) can act as an *SMTP client*. An email client knows the *outgoing mail* SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the e-mail address to the right of the at (@) sign). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. Some current mail transfer agents will also use SRV records, a more general form of MX, though these are not widely adopted. (Relaying servers can also be configured to use a smart host. SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Another SMTP server can trigger a delivery in SMTP using ETRN.

An e-mail client requires the name or the IP address of an SMTP server as part of its configuration. The server will deliver messages on behalf of the user. This setting allows for various policies and network designs. End users connected to the Internet can use the services of an e-mail provider that is not necessarily the same as their connection provider. Network topology, or the location of a client within a network or outside of a network, is no longer a limiting factor for e-mail submission or delivery. Modern SMTP servers typically use a client's credentials (authentication) rather than a client's location (IP address), to determine whether it is eligible to relay e-mail.

One of the limitations of the original SMTP is that it has no facility for authentication of senders. Therefore, the SMTP-AUTH extension was defined. However, the impracticalities of widespread SMTP-AUTH implementation and management means that E-mail spamming is not and cannot be addressed by it.

EXERCISE 6

1. In a typical Client/Server under Network environment, explain the following in details:
   (*a*) What are the Server requirements?
   (*b*) What are the H/W requirements?
   (*c*) What are the Client requirements?
   (*d*) What are the Network requirements?
   (*e*) What do you mean by a thin client network?
   (*f*) List some advantages of Thin Client Network system.
2. Microsoft Windows NT Server provides various network services to support specific requirements of the users on the network. All network services impact the capacity of a network. Some of the services are:

(*a*) Net Logon

(*b*) Computer Browser

(*c*) DHCP

(*d*) Internet Explorer

(*e*) Workstation

(*f*) Server

Explain the above part in brief in a Client/Server environment.

3. In Client/Server architecture in a network environment, explain the following phenomena examples:–

(*a*) UPS

(*b*) Surge Protector

(*c*) Optical Disk

(*d*) CDDI

4. Explain the functions and features of Network Operating System.

5. Explain the working principal of following:

(*a*) CDROM

(*b*) WORM

(*c*) Mirror disk

(*d*) Tape optical disk

(*e*) UNIX Workstation

(*f*) Notebooks

6. In design a network operating system; discuss the relative advantages and disadvantages of using a single server and multiple servers for implementing a service.

7. Write short notes on the following:

(*a*) X-Terminals

(*b*) RAID Array Disk

(*c*) FDDI

(*d*) Power Protection Devices

(*e*) Network Interface Cards

(*f*) Network Operating System

(*g*) Fax Print Services

8. Explain how microkernels can be used to organize an operating system in a Client/Server fashion.

9. What are different client hardware and software for end users? Explain them.