MINISTRY OF EDUCATION
CERTIFICATE IN
INFORMATION COMMUNICATION TECHNOLOGY

KENYA INSTITUTE OF CURRICULUM DEVELOPMENT
STUDY NOTES

Computer Maintenance & Support

MODULE 2: SUBJECT NO 2

easytvet.com

Contents

TOPIC 1: INTRODUCTION TO COMPUTER MAINTENANCE

Definition & Terms

What is a Computer?
A **computer** is an electronic device that takes in data and instructions (input), works with the data (processing), and produces information (output).

Basic Terms

Data refers to the raw facts that are fed to a computer.
Information is data that has been processed and can be used for decision making.
Data and Information can take either of the following formats:
•**Text** – These are number, characters or special symbols. They are used when preparing reports, letters, etc.
•**Graphics** – These are images. Used when preparing charts, graphs, pictures
•**Multimedia** – These are audio and video recordings that may or may not combine of text and graphics.

Processing is the act of converting data into information.

A typical personal desk top computer

Importance and limitations of computers

The importance of computers cannot be exhausted as computers have become an integral part of our lives. Some of the areas that we shall identify are outline below. Find more at your free time and highlight them.

Advantages of using computers

1. A computer helps you automate various tasks that you cannot do or are very cumbersome to do manually. An example, a computer can be configured to record all transactions regarding co-operative members. It can then produce reports and statements regarding members instantly. Computers have made it possible for us to withdraw our money from our bank account from a remote location using automated teller machines (ATM).

2. It helps you organize your organizations data and information in a better way. This eases the process of retrieval. Therefore you become very efficient when you can respond to any queries in a very short while.

3. It has much more computing and calculating power than an ordinary human. It will help you become very effective in your work, make it easier and greatly improves the accuracy and quantity of your output. It makes it possible to solve problems faster than an ordinary human being.

4. It has a large storage capacity for data and files. This will therefore eliminate the bulkiness of manual files that are normally present in areas where there are many transactions.

5. Computers have consistency and reliability of performance without the need of rest that human being need.

6. Computers have made communication faster and cheaper. It has made it possible for one to communicate using voice or text with another person in far away location at a very affordable rate. Computers have also eased the time taken to exchange documents between two places. This is done using internet infrastructure that we shall learn more in lesson 8.

7. Computers have made research easy without the need to move physically to libraries. Access to materials that are from all over the world has been made possible. All this is through the internet.

8. Computers using the internet have now made it possible to meet partners and even date online via the dating sites. This has also made interaction with people from other parts of the world that you would have otherwise been unable to meet.

Limitations of computers

From the above advantages of using computers that we have identified, computer can outperform human beings in speed, memory and accuracy but still the computer has limitations. Some of the limitations of computers that we shall study are the following:

1. Though computer is programmed to work efficiently, fast and accurately but it is programmed by human beings to do so. Computer only follows these instructions. If the instructions are not accurate the working of computer will not accurate.

2. It is very difficult to make a computer act correctly in all situations since a computer cannot be truly intuitive. Without supervision, computers will operate poorly when dealing with unexpected circumstances, such as information or instructions that are incorrect or incomplete.

3. The computer cannot think by itself. The concept of artificial intelligence that we learnt in the fifth generation of computers (section 1.4) shows that the computer can think. But still this concept is dependent on set of instructions provided by the human beings.

4. A Computer cannot take care of itself like a human. A computer is dependent still to human beings for this purpose. A computer cannot therefore completely replace of human because it is always dependent of human

5. A computer can retrieve data very fast but this technique is linear. A human being's mind does not follow this rule. A human mind can think randomly which a computer machine cannot.

6. Computers have also made the users who are addicted to them very unhealthy as they do not walk around and exercise.

Computer Application Areas

Computers are now used in virtually all spheres of life. Here are a few of the application areas:

•**Science & technology (s&t) -** Computers are used in S&T to promote advances that could be useful to mankind, i.e. discovering better and more efficient ways of doing things.

•**Education -** Computers are useful for promoting learning experiences.

•**Banking & finance -** Computers are very useful for handling financial transactions, most especially the storage and processing of huge amounts of information kept by financial institutions.

•**Recreation -** On your average PC, you can play a variety of games,socializing.

•**Security -** information can be encrypted during transit and the use of fire walls and passwords additionally ensures that information stored is safe.

•**Others** - such as Medicine, Law, Sports, Entertainment, Media,Building, Construction, etc.

Caring for your computer
Here are some general tips on the care of your PC:
•Computers need air circulation to keep them cool.
•Computers should be kept in a dust free environment.
•Use a surge protector or a UPS, (Uninterruptible Power Supply).
•Do not plug devices into the computer while it is on, unless you are inserting a USB device.
•Monitors, CPU and Printers should be turned off only by the power button on the printer case.
•If at all possible, do not eat or drink around your PC.
•Always use some form of Anti-Virus software.
•Backing up your data periodically will protect your data and make it easier to recover from a disastrous event.
•Use Scandisk and Defrag on storage disks to protection of your data.
•Empty your Recycle Bin on a regular basis.

Basic computer system Component parts
A Computer is **made up of** two parts i.e.

Hardware –The physical (Tangible) part of a computer. The hardware is made up of the following parts:
–Input devices like the keyboard and mouse
–Central Processing Unit
–Storage devices like hard drives
–Output devices like printers and monitors

Software – The non physical part of a computer. It comprises of instructions fed to the computer to manipulate the hardware. The instructions tell the computer what to do.
–system software
–application software
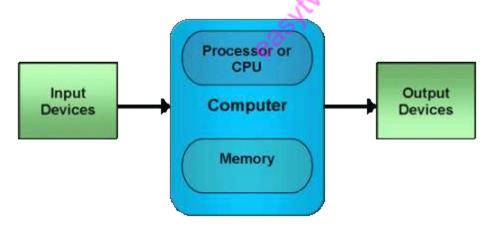
A **computer system** includes computer hardware, software and people.

COMPUTER HARDWARE

The term hardware refers to the tangible parts of a computer system, that is, the physical equipment of the computer.

The internal architectural design of computers differs from one system model to another. However, the basic organization remains the same for all computer systems. The following five units (also called *"The functional units"*) correspond to the five basic operations performed by all computer systems.

There are 4 primary parts to a computer system:

1.   **Input devices**
       Input devices allow a person to communicate information to the computer. Examples of input
       devices would be a keyboard and mouse.
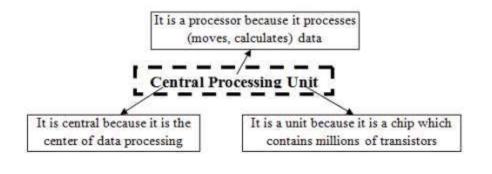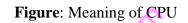
2.   **Output devices**

Output devices communicate information to the user. Examples of output devices would be a monitor or printer.

3.   **CPU [Central Processing Unit]**
Central Processing Unit (CPU) performs all the arithmetic and logical calculations in a computer. The CPU is said to be the brain of the computer system. It reads and executes the program instructions, perform calculations and makes decisions. The CPU is responsible for storing and retrieving information on disks and other media.

Figure: Meaning of CPU
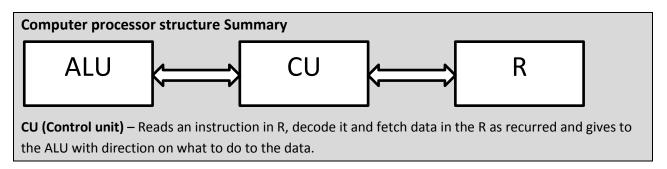
There are three major parts to the CPU: the CU, the ALU, and the registers.

Control Unit: The control unit issue control signals to perform specific operation and it directs the entire computer system to carry out stored program instructions

Arithmetic and Logic Unit: The ALU is the 'core' of any processor. It executes all arithmetic operations (addition, subtraction, multiplication and division), logical operations (compare numbers, letters, special characters etc.) and comparison operators (equal to, less than, greater than etc.).

Register Set: Register set is used to store immediate data during the execution of instruction. This area of processor consists of various registers.

Computer processor structure Summary

CU (Control unit) – Reads an instruction in R, decode it and fetch data in the R as recurred and gives to the ALU with direction on what to do to the data.
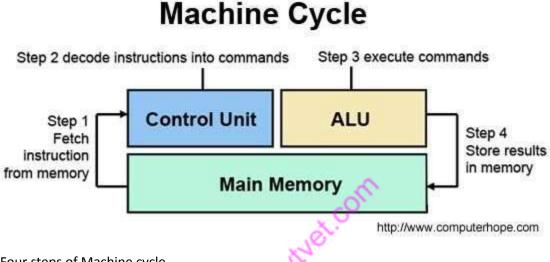
ALU (Arithmetic and Logic Unit) – takes data and direction from CU and works on the data to produce the desired results

R (Register) – small memory in the Processor that holds what the computer is working on immeditry

Machine cycle

The steps performed by the computer processor for each machine language instruction received. The **machine cycle** is a 4 process cycle that includes reading and interpreting the machine language, executing the code and then storing that code.

Four steps of Machine cycle

1. **Fetch** - Retrieve an instruction from the memory.
2. **Decode** - Tranlate the retrieved instruction into a series of computer commands.
3. **Execute** - Execute the computer commands.
4. **Store** - Sand and write the results back in memory.
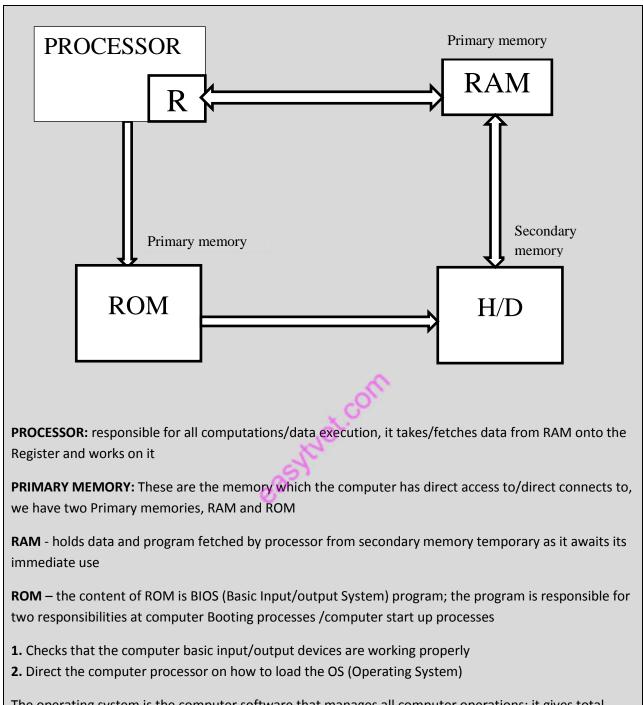
Instruction cycle

The sequence of operations that the cpu has to carry out while execution is called instruction cycle.

- 1:- Read an Instruction
- 2:- Decode the instruction
- 3:- Find the address of operand
- 4:- retrieve an operand
- 5:- perform desired operation
- 6:- find the address of destination
- 7:- store the result into the destination

Computer processor operation with memory

PROCESSOR

R

Primary memory

RAM

Primary memory

ROM

Secondary memory

H/D

PROCESSOR: responsible for all computations/data execution, it takes/fetches data from RAM onto the Register and works on it

PRIMARY MEMORY: These are the memory which the computer has direct access to/direct connects to, we have two Primary memories, RAM and ROM

RAM - holds data and program fetched by processor from secondary memory temporary as it awaits its immediate use

ROM – the content of ROM is BIOS (Basic Input/output System) program; the program is responsible for two responsibilities at computer Booting processes /computer start up processes

1. Checks that the computer basic input/output devices are working properly
2. Direct the computer processor on how to load the OS (Operating System)

The operating system is the computer software that manages all computer operations; it gives total direction to computer processor on how to do all operation. NOTE**:** The Processor works with the direction of operating system and when it's not loaded, the computer processor is primitive (can't do anything)

SECONDARY MEMORY: These are the memory which the computer has no direct access to/ connects to the memories under their responsible memory controllers; we have several secondary memories and

may be classified according to the technologies by which they works, H/D (Hard Disk/Local Disk) is the main secondary memory in a computer.

NOTE: the secondary memory/ secondary storage hold data/reserve data after use by the computer processor. It holds data permanently for future use

Computer Safety

Safety is a state of being protected from potential harm or something that has been designed to protect and prevent harm.

Tips to Keep Your Home Computer Safe and Secure

The safety and security of your personal computer is almost certainly something you've been dealing with for a long time. If you keep your anti-virus software updated and establish strong passwords for your online accounts, changing them on a regular basis, you've got all your bases covered. Or, do you? To make your online experience truly secure and keep those identity thieves at bay, read on for some lesser-known tips.

1. Check Your Firewall

Checking your firewall sounds complicated, but it really isn't. If you own a Windows-based system, just go to your control panel and type "firewall" in the search box. If your firewall is "on" or "connected," then you're good to go. If you own a Mac, click the Apple icon on your toolbar, go to "system preferences," then "security," then "firewall." Making sure you have a firewall in place can go a long way toward keeping criminals out. Make sure that you share some of your folders only on the home network. If you don't really need your files to be visible to other machines, disable file and media sharing completely.

2. Back Up Your Data

Backing up your data protects you in the event of a computer crash or electrical outage or surge, like a lightning storm might produce. It also helps if you fall prey to the newer type of ransomware, which encrypts your sensitive data. You can do your back-up manually by transferring important documents to an external hard drive, or using a service like Carbonite. If you don't have a significant amount of data to store, use a service like Dropbox, where you get 2GB of storage for free. Kaspersky PURE has backup functionality as well, including Dropbox integration.

3. Stay Away From Rogue Websites

Spotting a rogue website can be difficult, but there are a few things you can do to hone your skills. Look for a green lock in the address bar and the code prefix "https://" at the beginning of the URL while visiting banking sites, entering your credit card data or accessing your web mail. Be careful when shopping at a website that ships items from overseas, and don't click on links sent to you in email messages, go directly to the website itself instead.

4. Avoid Deals That Are Too Good to Be True

If you see a deal for 90% off The Beatles Collection CD, it very well could be a knock off. Even worse, some sites are known to lure customers in with an amazing deal, and once they have your

credit card information they're never to be heard from again – your identity may be compromised and there's not even a product to show for it. The simple rule of thumb here is: If it looks to good to be true then it probably is.

5. Never Divulge Sensitive Information

No matter what website you're on be careful of the sensitive information you reveal. Although it's pretty much common knowledge not to give out your social security number or credit card information unless you trust a website completely, you should be just as careful with your social media profiles as well. Revealing information as innocent as your pet's name or mother's maiden name could lead to identity theft, because you probably use the same data as the security question on some other website.

6. Avoid Opening Unknown Emails

Never open an email from an unknown or suspicious source, and definitely never open any attachments contained in them. You have to be careful of emails coming from people on your contact list as well, especially if the sender's account has been hacked. If an email from someone you regularly communicate with has a suspicious link and unusual content, delete it and immediately alert this person that his or her account may have been compromised. This will help you prevent hacking and phishing scams where you may be a target.

A great way to give yourself an overall umbrella of protection is to use Kaspersky products. Its Internet security and anti-virus software protects you from malware, spyware, and viruses, and it comes with parental controls as well. Doing some of the legwork on your own certainly helps keep you safe, but use Kaspersky if you want to make sure all your bases are covered.

Maintenance Tools, Equipment Materials

Computer maintenance is the practice of keeping computers in a good state of repair. Computer valeting is the in-depth <u>cleaning</u> of the physical components of a personal computer.

Computer maintenance describes various steps to keep your computer functioning at an optimal
performance level from a software and hardware point of view.

A toolkit should contain all the tools necessary to complete hardware repairs. As you gain experience, you learn which tools to have available for different types of jobs. Hardware tools are grouped into four categories:

- ESD tools

- Hand tools

- Cleaning tools

- Diagnostic tools

Maintenance Tools

To troubleshoot and repair laptop systems properly, you need a few basic tools. If you intend to troubleshoot and repair systems professionally, you may want to purchase many more specialized tools as well. These advanced tools enable you to more accurately diagnose problems and make jobs easier and faster. Here are the basic tools that should be in every troubleshooter's toolbox:

- Simple hand tools for basic disassembly and reassembly procedures, including a selection of flat-blade and Phillips screwdrivers (both medium and small sizes), tweezers, an IC extraction tool, and a parts grabber or hemostat. Most of these items are included in $10–$20 starter toolkits found at most computer stores. Although most of the same toolkits sold for conventional desktop systems will have these tools, for portable systems you may also need sets of smaller-sized flat-blade and Phillips screwdrivers and a set of small Torx drivers or Torx bits as well. For laptops, you may encounter Torx screws as small as T5, so consider purchasing a set including bits down to that size.

- Diagnostics software and hardware for testing components in a system.

- A multimeter that provides accurate measurements of voltage and resistance, as well as a continuity checker for testing cables and switches.

- Chemicals (such as contact cleaners), component freeze sprays, and compressed air for cleaning the system.

- Foam swabs, or lint-free cotton swabs if foam isn't available.

- Small nylon wire ties for "dressing" or organizing wires or small cables (such as internal Wi-Fi/Bluetooth antennas).

You may want to consider the following items, although they're not required for most work:

- Memory-testing machines (used to evaluate the operation of memory modules). Note these can be very expensive, on the order of $1,000 or more, but can be useful for professional shops or larger companies with a lot of systems to support.

- Serial and parallel loopback (or wrap) plugs to test serial and parallel ports.

- A network cable tester or scanner (many types with varying functionality are available, from simple loopback jacks to full-blown Time Domain Reflectometers).

TOPIC 2: MAINTENANCE

Maintenance Concept

Computer maintenance is the practice of keeping computers in a good state of repair.

Types of Computer Maintenance

- Corrective maintenance: Reactive modification of a computer and peripherals performed after delivery and during use to correct discovered problems.
- Adaptive maintenance: Modification of a computer and peripherals performed after delivery and during use to keep a computer usable in a changed or changing environment.
- Perfective maintenance: Modification of a computer and peripherals performed after delivery and during use to improve performance or maintainability.
- Preventive maintenance: Modification of a computer and peripherals performed after delivery and during use to detect and correct latent faults in the computer before they become effective faults.

Computer cleaning

Computer cleaning involves physically cleaning the interior and exterior of a computer, including the removal of dust and debris from cooling fans, power supplies, and other hardware components. This should be done after certain period of time (weekly/monthly).

A computer containing accumulated dust and debris may not run properly.

General cleaning Tips

Below is a listing of suggestions to follow when cleaning any computer components or peripherals as well as tips to help keep a computer clean.

1. Never spray or squirt any liquid onto any computer component. If a spray is needed, spray the liquid onto a cloth.
2. You can use a vacuum to suck up dirt, dust, or hair around the computer. However, **do not** use a vacuum inside your computer as it generates static electricity that can damage your computer. If you need to use a vacuum inside your computer, use a portable battery powered vacuum or try compressed air.
3. When cleaning a component or the computer, turn it off before cleaning.
4. Be cautious when using any cleaning solvents; some people have allergic reactions to chemicals in cleaning solvents and some solvents can even damage the case. Try always to use water or a highly diluted solvent.
5. When cleaning, be careful to not accidentally adjust any knobs or controls. Also, when cleaning the back of the computer, if anything is connected make sure not to disconnect the plugs.
6. When cleaning fans, especially smaller fans, hold the fan or place something in-between the fan blades to prevent it from spinning. Spraying compressed air into a fan or cleaning a fan with a vacuum may cause damage or generate back voltage.
7. Never eat or drink around the computer.

8. Limit smoking around the computer.

Cleaning tools & Detergent

Although computer cleaning products are available you can also use household items to clean your computers and peripherals. Below is a listing of items you may need or want to use while cleaning your computer.

- **Cloth** - A cotton cloth is the best tool used when rubbing down computer components. Paper towels can be used with most hardware, but we always recommend using a cloth whenever possible. However, only use a cloth when cleaning components such as the case, a drive, mouse, and keyboard. You should not use a cloth to clean any circuitry such as the RAM or motherboard.
- **Water or rubbing alcohol** - When moistening a cloth, it is best to use water or rubbing alcohol. Other solvents may be bad for the plastics used with your computer.
- **Portable Vacuum** - Sucking the dust, dirt, hair, cigarette particles, and other particles out of a computer can be one of the best methods of cleaning a computer. However, do not use a vacuum that plugs into the wall since it creates lots of static electricity that can damage your computer.
- **Cotton swabs** - Cotton swaps moistened with rubbing alcohol or water are excellent tools for wiping hard to reach areas in your keyboard, mouse, and other locations.
- **Foam swabs** - Whenever possible, it is better to use lint-free swabs such as foam swabs.

Component Cleaning

1. Case cleaning

Why? Keeps the appearance of the computer looking new. While cleaning, if you see ventilation slots, these can be cleaned or cleared to help keep a steady airflow into the computer and keep all components cool.

Procedure: The plastic case that houses the PC components can be cleaned with a slightly damp lint-free cloth. For stubborn stains, add a little household detergent to the cloth. You should not use a solvent cleaner on plastics.

Make sure all vents and air holes are hair and lint free by rubbing a cloth over the holes and vents. It is also helpful to take a vacuum around each of the hole, vents, and crevices on the computer. It is safe to use a standard vacuum when cleaning the outside vents of a computer.

2. CD-ROM, DVD, and other disc drive cleaning

Why? A dirty CD-ROM drive or other disc drives can cause read errors when reading discs. These read errors could cause software installation issues or issues while running the program.

Procedure: To clean the CD-ROM drive we recommend purchasing a CD-ROM cleaner from your local retailer such as a local Radio Shack or other computer retailer. Using a CD-ROM cleaner should sufficiently clean the CD-ROM laser from dust, dirt, and hair.

In addition to cleaning the drive with a special disc designed to clean drives, you can also use a cloth dampened with water to clean the <u>tray</u> that ejects from the drive. However, make sure that after the tray is cleaned that it completely dry before putting the tray back into the drive.

CD and DVD disc cleaning

Why? Dirty <u>CDs</u> can cause read errors or cause CDs to not work at all.

Procedure: Use a cleaning kit or damp clean cotton cloth to clean CDs, DVDs, and other discs When cleaning a disc wipe against the tracks, starting from the middle of the CD or DVD and wiping towards the outer side as shown in the picture below. Never wipe with the tracks; doing so may put more scratches on the disc.

Cleaning a CD / DVD disc

http://www.computerhope.com

Tip: If the substance on a CD cannot be removed using water, pure alcohol can also be used.

3. Hard drive cleaning

Why? Hard drives cannot be physically cleaned, however, they can be cleaned with software utilities to help it run fast and efficiently. Utilizing these utilities prevent the hard drive from slowing down.

Procedure: <u>Basic troubleshooting</u> for operating system steps are followed/done to help improve the performance of your computer.

Data

Backups

Important data stored on computers may be copied and archived securely so that, in the event of failure, the data and systems may be reconstructed. When major maintenance such as patching is performed, a backup is recommended as the first step in case the update fails and reversion is required.
Disk cleanup may be performed as regular maintenance to remove these. Files may become fragmented and so slow the performance of the computer. Disk defragmentation may be performed to combine these fragments and so improve performance.

Legal issues

In the United States of America, the Digital Millennium Copyright Act specifically exempts computer-maintenance activities, so copies of copyright files may be made in the course of maintenance provided that they are destroyed afterwards.

Software

Operating system
Operating-system files such as the Windows registry may require maintenance. A utility such as a registry cleaner may be used for this.

Software updates
Software packages and operating systems may require regular updates to correct software bugs and to address security weaknesses.

Security

Service intervals
Depending on the environment, computers should be serviced at least once per quarter, though monthly service is optimal. Regular servicing helps computers provide their peak performance.

4. Headphones cleaning

Why? <u>Headphones</u> used by many different people may need to be frequently cleaned to help prevent the spreading of germs and head lice.

Procedure: If the headphones being used are plastic or vinyl, moisten a cloth with warm water and rub the head and earpieces of the headphones. If the headphones are being used for a library or school do not use any disinfectant or cleaning solvent since some people can have allergic reactions to the chemicals they contain.

Headphones that have cushions also have the availability of having the cushions replaced. Replacing these cushions can also help keep the headphones clean.

Finally, in regards to headphones spreading head lice. If many different students use the same headphones, consider having the students using their own headphones, placing bags over the headphones, or using headphones that can be wiped with warm water after each use.

5. Keyboard cleaning

These steps are for cleaning a desktop keyboard.

Dust, dirt, and bacteria

The computer keyboard is usually the most germ infected items in your home or office, it may even contain more bacteria than your toilet seat. Cleaning it helps remove any dangerous bacteria and keeps the keyboard working properly.

Hair, dust, dirt, and food under keyboard key

Procedure: Before cleaning the keyboard first turn off the computer or if you are using a USB keyboard unplug it. Not unplugging the keyboard can cause other computer problems as you may press keys that cause the computer to perform a task you do not want it to do.

Many people clean the keyboard by turning it upside down and shaking. A more efficient method is to use compressed air. Compressed air is pressurized air contained in a can with a very long nozzle. aim the air between the keys and blow away all of the dust and debris that has gathered there. A vacuum cleaner can also be used, but make sure the keyboard does not have loose "pop off" keys can be sucked up by the vacuum.

If you want to clean the keyboard more extensively remove the keys from the keyboard.

After the dust, dirt, and hair has been removed. Spray a disinfectant onto a cloth or use disinfectant cloths and rub each of the keys on the keyboard. As mentioned in our general cleaning tips, never spray any liquid onto the keyboard.

Substance spilt into the keyboard

If the keyboard has anything spilt into it (e.g. pop, cola, Pepsi, Coke, beer, wine, coffee, and milk), not taking the proper steps can destroy the keyboard.

Procedure: Below are a few recommendations that can help prevent a keyboard from becoming bad after something has spilt into the keys.

If anything is spilt onto the keyboard turn the computer off immediately or at the very least disconnect the keyboard from the computer. Once done flip the keyboard over to prevent the substance from penetrating circuits. While the keyboard is upside down, shake the keyboard over a surface that can be cleaned later. While still upside down, use a cloth to start cleaning the keys. After cleaned leave the keyboard upside down for at least one night allowing it to dry. Once dry, continue cleaning the keyboard with any remaining substance.

If after cleaning the keyboard you have keys that stick remove the keys and clean below the keys and the bottom portion of the key.

Finally, if the keyboard still works but remains dirty or sticky before discarding the keyboard as a last resort try washing the keyboard in the dishwasher.

If after doing all the above steps the keyboard still does not work we recommend buying a new keyboard.

6. LCD cleaning

Why? Dirt, dust, and fingerprints can cause the computer screen to be difficult to read.

Procedure: Unlike a computer monitor, the LCD or flat-panel display is not glass and requires special cleaning procedures.

When cleaning the LCD screen it is important to remember to not spray any liquids onto the LCD directly, press gently while cleaning, and do not use a paper towel since it scratches the LCD.

To clean the LCD screen use a non-rugged microfiber cloth, soft cotton cloth, or Swiffer duster. If a dry cloth does not completely clean the screen, you can apply rubbing alcohol to the cloth and wipe the screen with a damp cloth. Rubbing alcohol is used to clean the LCD before it leaves the factory.

7. Monitor cleaning

Tip: This section is for computer monitors if you have an LCD or flat-panel see the LCD cleaning section.

Why? Dirt, dust, and fingerprints can cause the computer screen to be difficult to read.

Procedure: A glass monitor screen can be cleaned with ordinary household glass cleaner. Be sure to remove power from the monitor and spray the cleaner onto a lint free-cloth so the fluid does not leak into the electrical components inside the monitor. Vacuum off any dust that has settled on top of the monitor, and make sure no books or papers are covering the air vents. Obstructed monitor vents can cause the monitor to overheat or even catch on fire.

Caution: We suggest only using a cloth dampened with water when cleaning non-glass monitors or any anti-glare screens. Using ordinary household glass cleaner on special screens, especially cleaners with ammonia can remove anti-glare protection or other special surfaces.

Other good cleaning solutions

- Microfiber Towels
- Swiffer Dusters

Related pages

8. Motherboard cleaning

Why? Dust and especially particles of cigarette smoke can build up and corrode circuitry causing various problems such as computer lockups

Caution: When inside the computer take the necessary ESD precautions and try to avoid unplugging any cables or other connections.

Procedure: Our recommendation when cleaning the motherboard from dust, dirt, or hair is to use compressed air. When using compressed air, hold it in the up-right position to prevent any of the chemicals from coming out of the container, which may damage or corrode the Motherboard or other components. Also, ensure when using compressed air that you always blow the dust or dirt away from the motherboard, or out of the case.

Another good alternative to compressed air is to use a portable battery powered vacuum that can effectively remove the dust, dirt, and hair from the motherboard completely and prevent it from getting trapped within the case. However, do not use a standard electricity powered vacuum as it can cause lots of static electricity that can damage the computer. When using a vacuum keep it a couple inches away from the motherboard and all other components to prevent damage and anything from being sucked into the vacuum (e.g. jumpers or small cables).

Tip: When cleaning the inside of the case also look at any fans or heat sinks. Dust, dirt, and hair collects around these components the most.

9. Mouse cleaning

Why? A dirty optical-mechanical mouse (mouse with a ball) can cause the mouse to be difficult to move as well as cause strange mouse movement.

Procedure: To clean the rollers of an optical-mechanical mouse, you must first remove the bottom cover of the mouse. To do this, examine the bottom of the mouse to see what direction to rotate the cover. As you can see in the below illustration, the mouse cover must be moved counter clockwise. Place two fingers on the mouse cover and push the direction of the arrows.

Once the cover has rotated about an inch, rotate the mouse into its normal position, covering the bottom of the mouse with one hand and the bottom should fall off including the mouse ball. If the cover does not fall off try shaking the mouse gently.

Mechanical mouse

Once the bottom cover and the ball is removed, you should be able to see three rollers located within the mouse. Use a cotton swab, finger, or fingernail to remove any substance. Usually, there is a

small line of hair and dirt in the middle of the roller, remove as much as this substance as possible.

Once you have removed as much dirt and hair as possible, set the ball back within the mouse and place the cover back on.

If the mouse still has the same problems repeat the above process. If after several attempts the mouse is still having the same problems your mouse has other hardware issues and should be replaced.

Note: Cleaning your mouse pad with a damp cloth can also help improve a computer's mouse movement.

Why? To help keep the mouse clean and germ free it can be helpful to clean the mouse.

Procedure: Use a cloth moistened with rubbing alcohol or warm water and rub the surface of the mouse and each of its buttons.

10.Printer cleaning

Why? Cleaning the outside of a printer can help keep the printer's appearance looking good and if used by many different people keep the printer clean of germs.

Procedure: First, make sure to turn off the printer before cleaning it. Dampen a cloth with water or rubbing alcohol and wipe the case and each of the buttons or knobs on the printer. As mentioned earlier, never spray any liquid directly onto the printer.

Why? Some printers require the inside to be cleaned to help keep the printer running smoothly.

11.Scanner cleaning

Why? Flatbed scanners commonly become dirty with dust, fingerprints, and hair. When the scanner is dirty, the images may have distortions.

Procedure: Clean a flatbed scanner's surface by spraying a window cleaner onto a paper towel or cotton cloth and wipe the glass until clean. As mentioned earlier, never spray a liquid directly onto the component.

The same towel or cotton cloth can also be used to clean the outside of the scanner.

Miscellaneous cleaning steps

Below are a listing of miscellaneous computer hardware that is rarely used today, but kept on this page people working on older computers and need to clean these devices.

1. Floppy drive cleaning

Why? Dirty read/write heads on the floppy drive can cause errors during the reading or writing process.

Procedures: The floppy drive can be cleaned two different ways. The first method of cleaning a floppy drive is to purchase a kit at your local retail store designed to clean the read/write heads on your floppy drive.

The second method of cleaning the floppy drive is only recommended for experienced computer users. Open the floppy drive casing and physically swab the read/write heads with a lint-free foam swab soaked in pure alcohol, free-on, or trichloroethane. When performing these steps, be extremely careful when cleaning the heads to ensure that you do not lock them out of alignment causing the floppy drive to not work. To help prevent the heads from becoming out of alignment, use a dabbing motion lightly putting the swab on the head and removing it, do not perform a side-to-side motion with the swab.

2. Palm pilot cleaning
Why? Dirty touch screens can cause difficult navigation.

Procedure: To clean the Palm Pilot Screen, use a soft cloth moistened with rubbing alcohol and rub the screen and the casing of the palm pilot. It is not recommended to use glass cleaner as it could damage plastics over time.

3. SuperDisk and LS120 cleaning
Why? Cleaning the SuperDisk and LS120 prevents the drive heads from becoming dirty.

Procedure: Purchase the SuperDisk cleaning kit available through Imation. Using any other method voids the warranty on your drive.

Active vs passive maintenance

Active maintenance of the PC involves keeping the system clean and free of errors, preventing problems before they start. Many different types of software can be used to do this, but the main ones are as follows:

- ✓ Antivirus
- ✓ Anti-malware
- ✓ Defragmenter
- ✓ Firewall
- ✓ System cleaner

By combining these different methods of preventing system problems or infections, you are taking preventative measures to ensure that your computer continues to run well.

Passive maintenance involves taking care of the system by providing the best possible environment—both physical and electrical—for the system. Physical concerns are conditions such as ambient temperature, thermal stress from power cycling, dust and smoke contamination,

and disturbances such as shock and vibration. Electrical concerns are items such as ESD, power-line noise, and radio-frequency interference. Each of these environmental concerns is discussed in the following sections. This can be define as the way of avoid sudden failure of the equipment and to extend the life span of the equipment.

Difference between active and passive Prevetive Maintenance In Computer System?

Active maintenance is for all hard ware components and Passive maintenance for the supporting devices of hard ware components

TOPIC 3: COMPUTER INPUT & OUTPUT DEVICES

Introduction to I/O Devices

An **input**/**output** (I/O) **device** is a hardware **device** that has the ability to accept inputted, outputted or other processed data. It also can acquire respective media data as **input** sent to a computer or send computer data to storage media as storage **output**. An I/O **device** is also known as an IO **device**.

I/O Hardware Operations

Computers operate on many kinds of devices. General types include *storage devices* (disks, tapes), *transmission devices* (network cards, modems), and *human-interface devices* (screen, keyboard, mouse). Other devices are more specialized. A device communicates with a computer system by sending signals over a cable or even through the air.

The device communicates with the machine via a connection point termed a *port* (for example, a serial port). If one or more devices use a common set of wires, the connection is called a *bus*. In other terms, a bus is a set of wires and a rigidly defined protocol that specifies a set of messages that can be sent on the wires.

Daisy chain

When device A has a cable that plugs into device B, and device B has a cable that plugs into device C, and device C plugs into a port on the computer, this arrangement is called a **daisy chain**. It usually operates as a bus.

Controller

A controller is a collection of electronics that can operate a port, a bus, or a device. A serial-port controller is an example of a simple device controller. This is a single chip in the computer that controls the signals on the wires of a serial port.

The SCSI bus controller is often implemented as a separate circuit board (a host adapter) that plugs into the computer. It contains a processor, microcode, and some private memory to enable it to process the SCSI protocol messages. Some devices have their own built-in controllers.
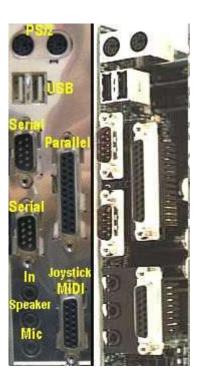
I/O port & Types

Alternatively referred to as **I/O address**, **I/O ports**, and **I/O port address**, the **input/output port** is what allows the software drivers to communicate with hardware devices on your computer.
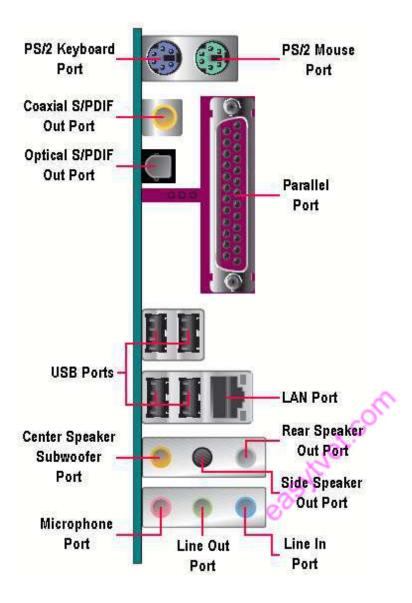
I/O Ports

The picture above shows an internal view of some of the I/O ports on the right and a covered view on the left.

I/O stands for Input and Output. The most common device for input is the keyboard. When you type, you are putting information into the computer, which is known as input. The most common device for output is the monitor. After the information has made its way through the computer, it is sent out to the monitor for us to see. This is known as output. On the back of computers are several I/O, (or Input/Output), ports. Above, on the very top are two PS/2 ports, normally used for mouse and keyboard connections. Below that are the USB, (or Universal Serial Bus), ports. Below those are two serial ports beside a long parallel port that is often used to connect to a printer. On the bottom right is a game port for joysticks or other game controllers. On the bottom left is a microphone hook up, a speaker hook up, and an additional hook up for another sound input device like a musical keyboard. Below is a picture of the I/O ports on a more recent computer.

I/O devices can be divided into two categories −

- **Block devices** − A block device is one with which the driver communicates by sending entire blocks of data. For example, Hard disks, USB cameras, Disk-On-Key etc.
- **Character devices** − A character device is one with which the driver communicates by sending and receiving single characters (bytes, octets). For example, serial ports, parallel ports, sounds cards etc

I/O Devices can be categorized into following category.

S.N.	Category & Description
1	**Human readable** Human Readable devices are suitable for communicating with the computer user.

	Examples are printers, video display terminals, keyboard etc.	
2	**Machine readable** Machine Readable devices are suitable for communicating with electronic equipment. Examples are disk and tape drives, sensors, controllers and actuators.	
2	**Communication** Communication devices are suitable for communicating with remote devices. Examples are digital line drivers and modems.	

Following are the differences between I/O Devices

S.N.	Criteria & Description
1	**Data rate** There may be differences of several orders of magnitude between the data transfer rates.
2	**Application** Different devices have different use in the system.
3	**Complexity of Control** A disk is much more complex whereas printer requires simple control interface.
4	**Unit of transfer** Data may be transferred as a stream of bytes or characters or in larger blocks.
5	**Data representation** Different data encoding schemes are used for different devices.
6	**Error Conditions** The nature of errors differs widely from one device to another.
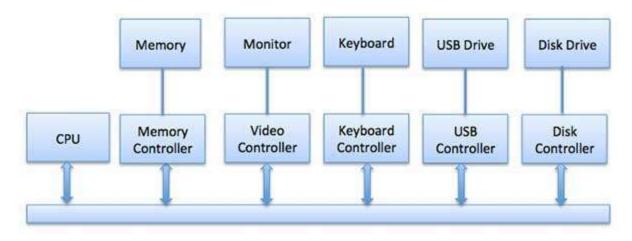
Device Controllers

Device drivers are software modules that can be plugged into an OS to handle a particular device. Operating System takes help from device drivers to handle all I/O devices.

The Device Controller works like an interface between a device and a device driver. I/O units (Keyboard, mouse, printer, etc.) typically consist of a mechanical component and an electronic component where electronic component is called the device controller.

There is always a device controller and a device driver for each device to communicate with the Operating Systems. A device controller may be able to handle multiple devices. As an interface its main task is to convert serial bit stream to block of bytes, perform error correction as necessary.

Any device connected to the computer is connected by a plug and socket, and the socket is connected to a device controller. Following is a model for connecting the CPU, memory, controllers, and I/O devices where CPU and device controllers all use a common bus for communication.

Synchronous vs asynchronous I/O

- **Synchronous I/O** − In this scheme CPU execution waits while I/O proceeds
- **Asynchronous I/O** − I/O proceeds concurrently with CPU execution

Communication to I/O Devices

The CPU must have a way to pass information to and from an I/O device. There are three approaches available to communicate with the CPU and Device.
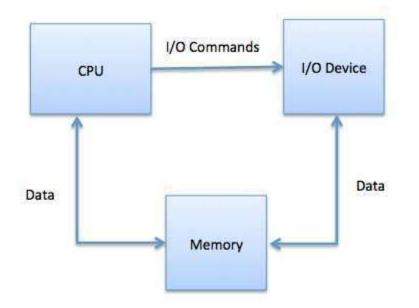
- Special Instruction I/O
- Memory-mapped I/O
- Direct memory access (DMA)

Special Instruction I/O

This uses CPU instructions that are specifically made for controlling I/O devices. These instructions typically allow data to be sent to an I/O device or read from an I/O device.

Memory-mapped I/O

When using memory-mapped I/O, the same address space is shared by memory and I/O devices. The device is connected directly to certain main memory locations so that I/O device can transfer block of data to/from memory without going through CPU.

While using memory mapped IO, OS allocates buffer in memory and informs I/O device to use that buffer to send data to the CPU. I/O device operates asynchronously with CPU, interrupts CPU when finished.
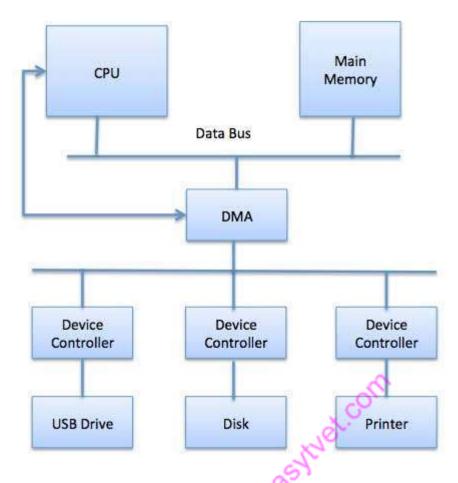
The advantage to this method is that every instruction which can access memory can be used to manipulate an I/O device. Memory mapped IO is used for most high-speed I/O devices like disks, communication interfaces.

Direct Memory Access (DMA)

Slow devices like keyboards will generate an interrupt to the main CPU after each byte is transferred. If a fast device such as a disk generated an interrupt for each byte, the operating system would spend most of its time handling these interrupts. So a typical computer uses direct memory access (DMA) hardware to reduce this overhead.

Direct Memory Access (DMA) means CPU grants I/O module authority to read from or write to memory without involvement. DMA module itself controls exchange of data between main memory and the I/O device. CPU is only involved at the beginning and end of the transfer and interrupted only after entire block has been transferred.

Direct Memory Access needs a special hardware called DMA controller (DMAC) that manages the data transfers and arbitrates access to the system bus. The controllers are programmed with source and destination pointers (where to read/write the data), counters to track the number of transferred bytes, and settings, which includes I/O and memory types, interrupts and states for the CPU cycles.

The operating system uses the DMA hardware as follows −

Step	Description
1	Device driver is instructed to transfer disk data to a buffer address X.
2	Device driver then instruct disk controller to transfer data to buffer.
3	Disk controller starts DMA transfer.
4	Disk controller sends each byte to DMA controller.
5	DMA controller transfers bytes to buffer, increases the memory address, decreases the counter C until C becomes zero.
6	When C becomes zero, DMA interrupts CPU to signal transfer completion.

Polling vs Interrupts I/O

A computer must have a way of detecting the arrival of any type of input. There are two ways that this can happen, known as **polling** and **interrupts**. Both of these techniques allow the processor to deal with events that can happen at any time and that are not related to the process it is currently running.

Polling I/O

Polling is the simplest way for an I/O device to communicate with the processor. The process of periodically checking status of the device to see if it is time for the next I/O operation, is called polling. The I/O device simply puts the information in a Status register, and the processor must come and get the information.

Most of the time, devices will not require attention and when one does it will have to wait until it is next interrogated by the polling program. This is an inefficient method and much of the processors time is wasted on unnecessary polls.

Compare this method to a teacher continually asking every student in a class, one after another, if they need help. Obviously the more efficient method would be for a student to inform the teacher whenever they require assistance.

Interrupts I/O

An alternative scheme for dealing with I/O is the interrupt-driven method. An interrupt is a signal to the microprocessor from a device that requires attention.

A device controller puts an interrupt signal on the bus when it needs CPU's attention when CPU receives an interrupt, It saves its current state and invokes the appropriate interrupt handler using the interrupt vector (addresses of OS routines to handle various events). When the interrupting device has been dealt with, the CPU continues with its original task as if it had never been interrupted.
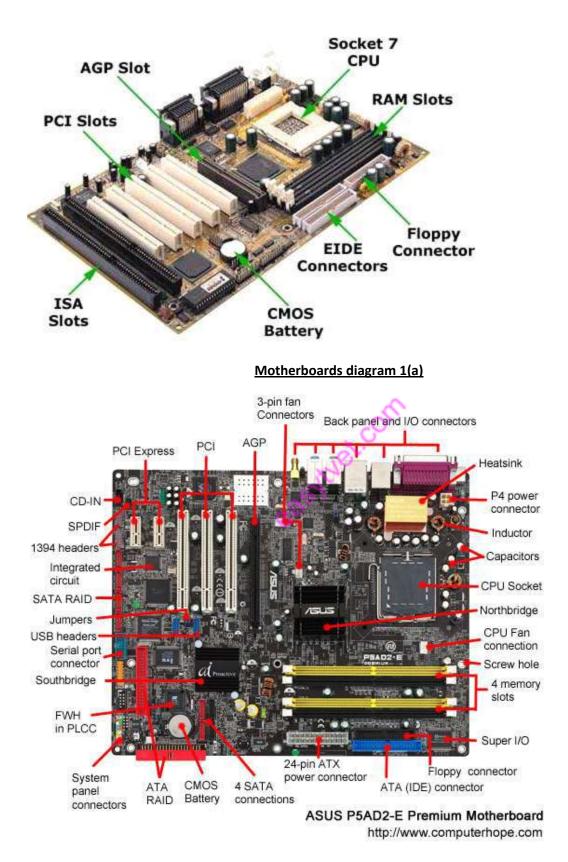
TOPIC 4: MOTHERBOARD & BUSES

Introduction to Computer Motherboard & Components

This is the main circuit board of the PC. It contains all the basic, core components of the computer.

It contains all the basic, core components of the computer. It usually contains:
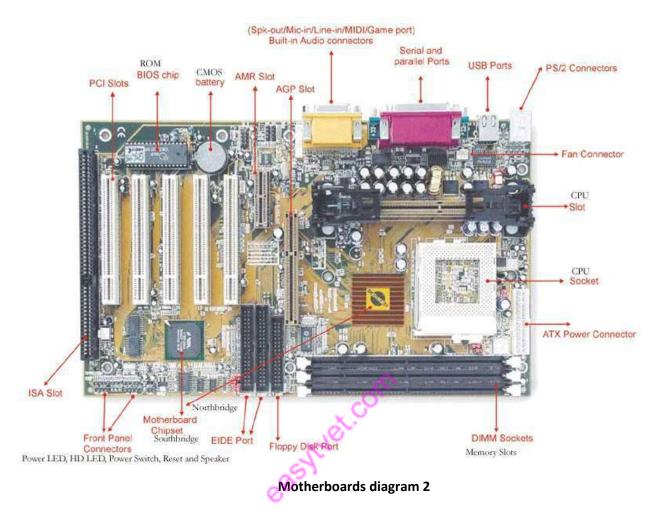
- *The CPU*, which plugs into a socket designed for a particular CPU's pin arrangement. Because a motherboard has sockets that can only accept certain types of CPU, it is important to make sure when upgrading your CPU that your motherboard can accept it.

- *Memory chips* - these hold data and programs that the CPU is currently using.

- *Input/output ports* ("I/O") such as connectors that hard disk drives, floppy disk drives and CD-ROM drives plug in to, serial port sockets, parallel port sockets and USB port sockets.

- *BIOS chips* (Basic Input Output System) - the BIOS chips are PROM (Programmable Read Only Memory) chips that contain the most basic information that a computer needs to start up and operate. The BIOS contains bootup information, details of what sort of CPU is installed, what hard disks are available, how the motherboard should behave etc. More details below.

- *Real time Clock (RTC)* so the computer knows the time and date. The RTC needs a battery to keep the clock running when the computer's power is turned off.

- *Chips* to control basic devices such as hard disks, floppy disks, serial/parallel ports etc. These basic chips are sometimes called the "chip set".

- Some motherboards, especially laptop motherboards, have built-in graphics chips, sound chips and modem chips so expansion cards are not needed. Unfortunately, this also means laptops can be very hard to upgrade because these chips are usually impossible to remove and replace. An example of "integrated peripherals" is **AC '97 Audio**. It combines a low-cost audio codec (**co**mpressor/**dec**ompressor) integrated circuit (IC) with a small portion of the core chipset's processing power to form a complete PC audio subsystem. Soft audio processing consumes minimal CPU overhead and does away with the need for a separate PCI audio controller (e.g. Soundblaster card). The result is reduced motherboard space and overall system cost. Building in AC '97 costs a manufacturer about $2, compared to almost $100 for a PCI sound card.

While motherboards have been getting smaller and smaller, computer cases seem to be getting bigger because the new computers generate more and more heat and need lots of empty space to ventilate themselves.

Motherboards diagram 1(a)

ASUS P5AD2-E Premium Motherboard
http://www.computerhope.com

Motherboards diagram 1(b)

Page **35** of **128**

Motherboards diagram 2

Types of motherboards (Form Factors)

(Old school)
AT (Full vs. Baby)
XT (rip)
LPX (rip)

(Newer)
ATX vs. BTX motherboard

<u>Definitions</u>

AT - Advanced Technology, A *motherboard* that follows the same design and 12x13" form factor that was in the original IBM PC/AT. It was superseded by the Baby AT. the Baby AT reduced width from 12" to 8.5"

ATX motherboard (Advanced Technology EXtended **motherboard**) The PC **motherboard** that superseded the Baby AT design. The ATX layout rotated the CPU and memory 90 degrees, allowing full-length expansions to be plugged into all sockets.

LPX (Low Profile eXtension), originally developed by Western Digital, was a loosely **defined motherboard** format (form factor) widely used in the 1990s.

BTX (for Balanced Technology eXtended) is a form factor for **motherboards**, originally intended to be the replacement for the aging ATX **motherboard** form factor in late 2004 and early 2005.

Note : Although all motherboards have some features in common, their layout and size vary a great deal. The most common motherboard designs in current use include ATX, Micro ATX, BTX, and NLX. Some of these designs feature riser cards and daughterboards.

ATX and Micro ATX

The ATX family of motherboards has dominated desktop computer designs since the late 1990s. ATX stands for "Advanced Technology Extended," and it replaced the AT and Baby-AT form factors developed in the mid 1980s for the IBM PC AT and its rivals. ATX motherboards have the following characteristics:

  ☐ A rear port cluster for I/O ports

  ☐ Expansion slots that run parallel to the short side of the motherboard

  ☐ Left side case opening (as viewed from the front of a tower PC)

There are four members of the ATX family, listed in Table 3-2. In practice, though, the Mini-ATX design is not widely used.

Table 3-2. ATX Motherboard Family Comparison

Motherboard Type	Maximum Width	Maximum Depth	Maximum Number of Expansion Slots	Typical Uses
ATX	12 in	9.6 in	Seven	Full tower
Mini-ATX	11.2 in	8.2 in	Seven	Full tower
microATX	9.6 in	9.6 in	Four	Mini tower
FlexATX	9.0 in	7.5 in	Four	Mini tower, small form factor

Micro ATX - A smaller version of Full ATX

Flex ATX - Another version of the ATX motherboard

BTX

One problem with the ATX design has been the issue of system cooling. Because ATX was designed more than a decade ago, well before the development of today's faster components, it's been difficult to properly cool the hottest-running components in a typical system: the processor, memory modules, and the processor's voltage regulator circuits.

To enable better cooling for these devices, and to promote better system stability, the BTX family of motherboard designs was introduced in 2004. Compared to ATX motherboards, BTX motherboards have the following:

- Heat-producing components such as the process, memory, chipset, and voltage regulator are relocated to provide straight-through airflow from front to back for better cooling.
- The processor socket is mounted at a 45-degree angle to the front of the motherboard to improve cooling.
- A thermal module with a horizontal fan fits over the processor for cooling.
- The port cluster is moved to the rear left corner of the motherboard.
- BTX cases include multiple rear and side air vents for better cooling.
- Because of the standardization of processor and memory locations, it's easy to use the same basic design for various sizes of BTX motherboards; the designer can just add slots.
- BTX tower cases use a right-opening design as viewed from the front.

Although BTX designs are easier to cool than ATX designs, the development of cooler-running processors has enabled system designers to continue to favor ATX. There are relatively few BTX-based motherboards and systems currently on the market.

Riser Cards and Daughterboards

Riser cards and daughterboards provide two different methods for providing access to motherboard–based resources. In current slimline or rackmounted systems based on ATX or BTX technologies, riser cards are used to make expansion slots usable that would otherwise not be available because of clearances inside the case. Riser card designs can include one or more expansion slots, and are available in PCI, PCI-X (used primarily in workstation and server designs), and PCI-Express designs

The term *daughterboard* is sometimes used to refer to riser cards, but daughterboard can also refer to a circuit board that plugs into another board to provide extra functionality. For example, some small form factor motherboards support daughterboards that add additional serial or Ethernet ports, and some standard-size motherboards use daughterboards for their voltage regulators.

NLX Motherboard

NLX motherboards are designed for quick replacement in corporate environments. They use a riser card that provides power and expansion slots that connect to the right edge of the motherboard (as viewed from the front). NLX motherboards have a two-row cluster of ports along the rear edge of the motherboard.

Most systems that use NLX motherboards are considered obsolete.

NLX (Supports motherboards with overall dimensions of 9.0" x 13.6" [maximum] to 8.0" x 10.0" [minimum]) Implemented in 1998 by Intel this form factor is gaining popularity the last couple of years because there found on most clone computers
Support for the Pentium II
Support for AGP
Support for USB.

Support for DIMM.
Easier Access to internal components
Support for motherboards that can be removed without using tools
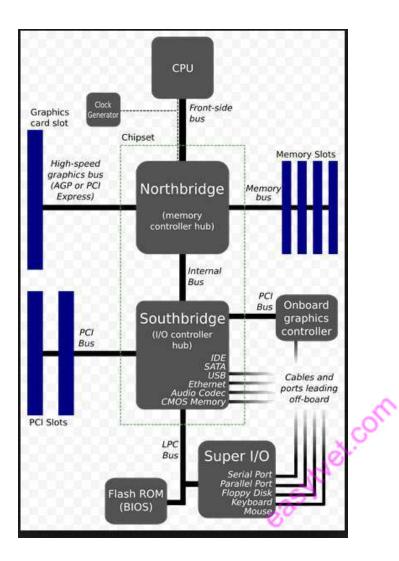
Power supply
The power supply provides the electricity needed by the motherboard and different components in the computer. It usually provides a series of power leads carrying 12 volts or 5 volts. A special lead feeds the motherboard and other leads power the disk drives. The power supply is a sealed cube about 12cm on each side and has a fan in it to cool itself and the computer case down.

Computer bus

A **bus**, in computing, is a set of physical connections (cables, printed circuits, etc.) which can be shared by multiple hard   ware components in order to communicate with one another.

The purpose of buses is to reduce the number of "pathways" needed for communication between the components, by carrying out all communications over a single data channel. This is why the metaphor of a "data highway" is sometimes used.

Characteristics

A bus is characterised by the amount of information that can be transmitted at once. This amount, expressed in bits, corresponds to the number of physical lines over which data is sent simultaneously. A 32-wire ribbon cable can transmit 32 bits in parallel. The term "**width**" is used to refer to the number of bits that a bus can transmit at once.

Additionally, the bus speed is also defined by its **frequency** (expressed in Hertz), the number of data packets sent or received per second. Each time that data is sent or received is called a **cycle**.

This way, it is possible to find the maximum **transfer speed** of the bus, the amount of data which it can transport per unit of time, by multiplying its width by its frequency. A bus with a width of 16 bits and a frequency of 133 MHz, therefore, has a transfer speed equal to:

$16 * 133.10^6 = 2128*10^6$ bit/s,
or $2128*10^6/8 = 266*10^6$ bytes/s
or $266*10^6 /1000 = 266*10^3$ KB/s
or $259.7*10^3 /1000 = 266$ MB/s

<u>Architecture</u>
In reality, each bus is generally constituted of 50 to 100 distinct physical lines, divided into three subassemblies:

- The **address bus** (sometimes called the *memory bus*) transports memory addresses which the <u>processor</u> wants to access in order to read or write data. It is a unidirectional bus.

- The **data bus** transfers instructions coming from or going to the processor. It is a bidirectional bus.

- The **control bus** (or *command bus*) transports orders and synchonisation signals coming from the control unit and travelling to all other hardware components. It is a bidirectional bus, as it also transmits response signals from the hardware.
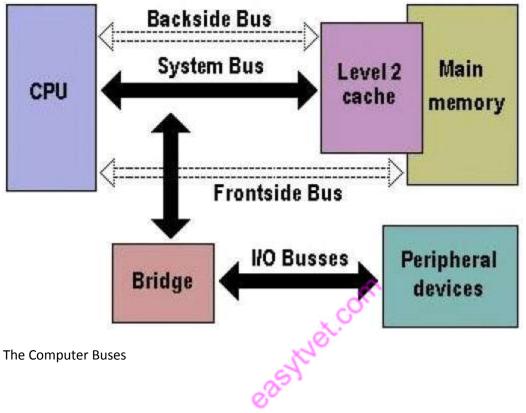
<u>Chipset</u>
A **chipset** is the component which routes data between the computer's buses, so that all the components which make up the computer can communicate with each other. The **chipset** originally was made up of a large number of electronic chips, hence the name. It generally has two components:

- The **NorthBridge** (also called the *memory controller*) is in charge of controlling transfers between the processor and the RAM, which is way it is located physically near the processor. It is sometimes called the **GMCH**, forr *Graphic and Memory Controller Hub*.

- The **SouthBridge** (also called the *input/output controller* or *expansion controller*) handles communications between peripheral devices. It is also called the **ICH** (*I/O Controller Hub*). The tem **bridge** is generally used to designate a component which connects two buses.

Types of Buses in Computer Architecture
Computers comprises of many internal components and in order for these components to communicate with each other, a *'bus'* is used for that purpose.

A **bus** is a **common pathway** through which information flows from one component to another. This pathway is used for communication purpose and can be established between two or more computer components. We are going to review different **computer bus architectures** that are used in computers.

The Computer Buses

Functions of Buses in Computers

The functions of buses can be summarized as below:

1. **Data sharing** - All types of buses found on a computer must be able to transfer data between the computer peripherals connected to it.

The data is transferred in in either serial or parallel, which allows the exchange of 1, 2, 4 or even 8 bytes of data at a time. (A byte is a group of 8 bits). Buses are classified depending on how many bits they can move at the same time, which means that we have 8-bit, 16-bit, 32-bit or even 64-bit buses.

2. Addressing - A bus has address lines, which match those of the processor. This allows data to be sent to or from specific memory locations.

3. Power - A bus supplies power to various peripherals that are connected to it.

4. Timing - The bus provides a **system clock** signal to synchronize the peripherals attached to it with the rest of the system.

The expansion bus facilitates the easy connection of additional components and devices on a computer for example the addition of a TV card or sound card.

Bus Terminologies

Computers can be viewed to be having just two types of buses:

1. System bus:- The bus that connects the CPU to main memory on the motherboard. The system bus is also called the front-side bus, memory bus, local bus, or host bus.

2. A number of I/O Buses, (Acronym for input/output), connecting various peripheral devices to the CPU -these are connected to the system bus via a 'bridge' implemented in the processors chipset. Other names for the I/O bus include "expansion bus", "external bus" or "host bus".

Expansion Bus Types

These are some of the common expansion bus types that have ever been used in computers:

- **ISA** - Industry Standard Architecture
- **EISA** - Extended Industry Standard Architecture
- **MCA** - Micro Channel Architecture
- **VESA** - Video Electronics Standards Association
- **PCI** - Peripheral Component Interconnect
- **PCMCIA** - Personal Computer Memory Card Industry Association (Also called PC bus)
- **AGP** - Accelerated Graphics Port
- **SCSI** - Small Computer Systems Interface.

Table of Comparisson

8-Bit ISA card (XT-Bus)	16-Bit ISA (AT –Bus card)
8-bit data interface	16-bit data interface
4.77 MHZ bus	8-MHZ bus
62-pin connector	62-pin connector
	36-pin AT extension connection

Comparison of 8-bit, & 16-bit ISA Bus as used in early computers.

ISA Bus

This is the most common type of early expansion bus, which was designed for use in the original IBM PC.The IBM PC-XT used an 8-bit bus design. This means that the data transfers take place in 8 bit chunks (i.e. one byte at a time) across the bus. The ISA bus ran at a clock speed of 4.77 MHz.

For the 80286-based IBM PC-AT, an improved bus design, which could transfer 16-bits of data at a time, was announced. The 16-bit version of the ISA bus is sometimes known as the AT bus. (AT-Advanced Technology)

The improved AT bus also provided a total of 24 address lines, which allowed 16MB of memory to be addressed. The AT bus was backward compatible with its 8-bit predecessor and allowed 8-bit cards to be used in 16-bit expansion slots.

When it first appeared the 8-bit ISA bus ran at a speed of 4.77MHZ – the same speed as the processor. It was improved over the years and eventually the AT bus ran at a clock speed of 8MHz.

MCA (Micro Channel Architecture)
This bus was developed by IBM as a replacement for ISA when they designed the PS/2 PC which was launched in 1987.

The bus offered a number of technical improvements over the ISA bus. For instance, the MCA runs at a faster speed of 10MHz and can support either 16-bit or 32-bit data. It also supports bus mastering - a technology that placed a mini-processor on each expansion card. These mini-processors controlled much of the data transfer allowing the CPU to perform other tasks.

One advantage of MCA was that the plug-in cards were software configurable i.e. they required minimal intervention by the user when configuring.

The MCA expansion bus did not support ISA cards and IBM decided to charge other manufacturers royalties for use of the technology. This made it unpopular and it is now an obsolete technology.

EISA Bus

EISA (Extended Industry Standard Architecture)

It was developed by a group of manufactures as an alternative to MCA. It was designed to use a 32-bit data path and provided 32 address lines giving access to 4GB of memory.

Like the MCA, EISA offered a disk-based setup for the cards, but it still ran at 8MHz in order for it to be compatible with ISA.

The EISA expansion slots are twice as deep as an ISA slot. If an ISA card is placed in an EISA slot it will use only the top row of connectors, whereas a full EISA card uses both rows. It offered bus mastering.

EISA cards were relatively expensive and were normally found on high-end workstations and network servers.

VESA Bus

Also known as the Local bus or the VESA-Local bus. VESA (**Video Electronics Standards Association**) was invented to help standardize PCs video specifications, thus solving the problem of proprietary technology where different manufacturers were attempting to develop their own buses.

The VL Bus provides 32-bit data path and can run at 25 or 33MHZ. It ran at the same clock frequency as the host CPU. But this became a problem as processor speeds increased because, the faster the peripherals are required to run, the more expensive they are to manufacture.

It was difficult to implement the VL-Bus on newer chips such as the 486s and the new Pentiums and so eventually the VL-Bus was superseded by PCI.

VESA slots have extra set of connectors and therefore the cards are larger. The VESA design was backward compatible with the older ISA cards.

Features of the VESA local bus card:-

- ☐ 32-bit interface
- ☐ 62/36-pin connector
- ☐ 90+20 pin VESA local bus extension

Peripheral Component Interconnect

Peripheral Component Interconnect **(PCI)** is one of the latest developments in bus architecture and is the current standard for PC expansion cards. It was developed by Intel and launched as the expansion bus for the Pentium processor in 1993. It is a local bus like VESA i.e. it connects the CPU, memory and peripherals to wider, faster data pathway.

PCI supports both 32-bit and 64-bit data width; therefore it is compatible with 486s and Pentiums. The bus data width is equal to the processor, for example, a 32 bit processor would have a 32 bit PCI bus, and operates at 33MHz.

PCI was used in developing Plug and Play (PnP) and all PCI cards support PnP i.e. the user can plug a new card into the computer, power it on and it will "self identify" and "self specify" and start working without manual configuration using jumpers.

Unlike VESA, PCI supports **bus mastering** that is, the bus has some processing capability and therefore the CPU spends less time processing data. Most PCI cards are designed for 5v, but there are also 3v and dual-voltage cards, Keying slots are used to differentiate 3v and 5v cards and slots to ensure that a 3v card is not slotted into a 5v socket and vice versa..

Accelerated Graphics Port
The need for high quality and very fast performance of video on computers led to the development of the **Accelerated Graphics Port (AGP)**. The AGP Port is connected to the CPU and operates at the speed of the processor bus. This means that video information can be sent more quickly to the card for processing.

The AGP uses the main PC memory to hold 3D images. In effect, this gives the AGP video card an unlimited amount of video memory. To speed up the data transfer, Intel designed the port as a direct path to the PC's main memory.

Data transfer rate ranges from 264 Mbps to 528mbps, 800 Mbps upto 1.5 Gbps. AGP connector is identified by its brown colour.

Personal Computer Memory Card Industry Association (PC Card)
The Personal Computer Memory Card Industry Association was founded to provide a standard bus for laptop computers. So it is basically used in the small computers.

Small Computer System Interface
Short for Small Computer System Interface, a parallel interface standard used by Apple Macintosh computers,PC's and Unix systems for attaching peripheral devices to a computer.

Universal Serial Bus (USB)

This is an external bus standard that supports data transfer rates of 12 Mbps. A single USB port can be used to connect up to **127 peripheral devices**, such as mice, modems, and keyboards. The USB also supports hot plugging/insertion (ability to connect a device without turning the PC of) and plug and play (You connect a device and start using it without configuration).

We have two versions of USB:-

USB 1x

First released in 1996, the original USB 1.0 standard offered data rates of 1.5 Mbps. The USB 1.1 standard followed with two data rates: 12 Mbps for devices such as disk drives that need high-speed throughput and 1.5 Mbps for devices such as joysticks that need much less bandwidth.

USB 2x

In 2002 a newer specification USB 2.0, also called Hi-Speed USB 2.0, was introduced. It increased the data transfer rate for PC to USB device to 480 Mbps, which is 40 times faster than the USB 1.1 specification. With the increased bandwidth, high throughput peripherals such as digital cameras, CD burners and video equipment could now be connected with USB.

IEEE 1394

The IEEE 1394 is a very fast external serial bus interface standard that supports data transfer rates of up to 400Mbps (in 1394a) and 800Mbps (in 1394b).This makes it ideal for devices that need to transfer high levels of data in real-time, such as video devices. It was developed by apple with the name firewire.
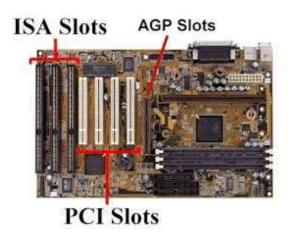
A single 1394 port can be used to connect up 63 external devices.

- ☐ It supports Plug and play
- ☐ Supports hot plugging, and
- ☐ Provides power to peripheral devices.

Expansion slots:

These are sockets that expansion cards like network cards, sound cards, graphics cards can be plugged into. There have been various types of slots over the years to cater for increasingly complex expansion cards. The earliest cards were ISA, then came EISA, then PCI and AGP

(which have special high-priority access to the CPU - AGP is used by fast graphic cards). All expansions slots connect to a bus so data can travel between subsystems and the CPU.

Cache
Cache is a storage place (buffer or bucket) that exists between two subsystems in order for data to be accessed more quickly to increase performance. Performance is increased because the cache subsystem usually has faster access technology and does not have to cross an additional bus. Cache is typically used for reads, but it is increasingly being used for writes as well. For example, getting information to the processor from the disk involves up to five cache locations:
1. L1 cache in the processor (memory cache)
2. L2 cache (memory cache)
3. Software disk cache (in main memory)
4. Hardware disk cache (common on SCSI controllers; EIDE usually uses only a FIFO buffer)
5. Disk buffer
For reads, one subsystem will usually request more data than what is immediately needed, and that excess data is stored in the cache(s). During the next read, the cache(s) are searched for the requested data, and if it is found, a read to the subsystem beyond the cache is not necessary.

How to install a computer motherboard
Installing a motherboard can be a complex process. This page provides general steps and guidelines for how to install a motherboard. Please refer to the manual and configuration guide that is included with the motherboard for specific details on installation and configuration steps.

Note: If replacing an existing motherboard in a computer with a new motherboard, you need to first remove the existing motherboard. The steps on this page can be referred to for removing the motherboard, followed in reverse order.

Before getting started

1. Write down relevant information from the top or bottom of the board, such as the Model Number, Serial Number, and specifications.

2. Ensure you are familiar with ESD and its potential dangers while working with any circuit board.

3. When installing a motherboard, turn the computer off and disconnect the power cord from the power supply.

Form factor

Before installing a computer motherboard, make sure the case supports the form factor of your motherboard. Today, the majority of available computer motherboards are either ATX or MicroATX.

Verify and set jumpers

Before installing the computer motherboard, make sure all the jumpers or dip switches are correct. The jumpers and dip switches can be changed when the motherboard is installed, but it is easier to verify them while the motherboard is outside of the case.

Today, motherboards have the jumpers set as auto, allowing either the BIOS or the software to setup the proper settings for the CPU and memory and other settings. If the motherboard supports this feature, make sure the jumpers are set to auto. If you want to adjust the settings manually for your peripherals, make sure you are using acceptable settings. Although you may be able to overclock a system, it is recommended you use auto or the real values of the system first to make sure the system works before tampering with its settings.

Install pegs or standoffs

After checking the jumpers, if pegs or standoffs are not in the chassis, insert these attachments now. These are required to prevent the motherboard from shorting out and must be inserted before installing the motherboard.

When installing the pegs or standoffs make sure to insert them into the proper holes. Many cases support different motherboard form factors, and if not placed in the proper holes, it may cause damage to the motherboard. The holes on the case have a small indication of what the holes are

for; for example, a hole may have the words ATX listed next to it to indicate the hole is for an ATX motherboard.

As the standoff is being installed, make sure they are installed firmly into the case to help prevent issues such as the pegs coming loose when unscrewing the screw from the peg.

Motherboard Installation

After the standoffs are attached and the I/O plate is in place, install the motherboard into the case and make sure you align the back of the motherboard with the back of the case. As the motherboard is being installed align the holes in the motherboards with the pegs or standoffs.

Once aligned, begin placing screws into the motherboard that should go into the peg or standoff inserted earlier.

Caution: when screwing in the screw you do not want the screw to be too tight. If tightened too much it can cause the motherboard to crack. However, the screw should be in enough to hold the motherboard in place.

Install essential components
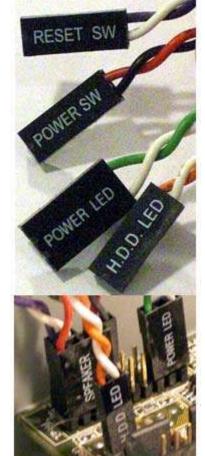If not already installed, install the below necessary components into the computer.

Front Panel Setup
Once the motherboard has been successfully physically installed into the computer, the Fpanel (short for front panel connectors) must be connected. This panel controls such things as the power button, reset button, hard drive light, and power light.
Unfortunately, the setup of this panel can be confusing at first, even with the instructions provided from the motherboard manufacturer. Below are steps and additional information and help with successfully connecting the cables to this connector.

1. This connector consists of a series of two pin connectors.

2. The cables that connect to the connector are 2, 3 or 4-pin connectors.

3. The cables consist of red, green, blue, white or another color cable with a black cable. This may vary, the important thing to remember is that the black cable or the dark color of the cable is ground or '-'.

System Panel cables and connector

4. Most cases have a separate cable for each setting, but some computers now have all of these cables as one large connector. If the computer has one large connector, it only connects in one direction. If you are installing a new computer motherboard into an OEM case that uses a large connector, it may not work with your motherboard since it could be proprietary.

5. Finally, the computer cannot boot if one or more of the cables is not properly connected. If you are unable to turn on the computer or receive <u>no post</u>, check these cables first.

Connect Cables

Once the front panel cables are connected, connect the other cables in the below order.

1. Connect the main motherboard <u>ATX style</u> power cable coming from the power supply to the motherboard.

   Note: Connect the cables in the right direction and never force the cable. If improperly connected, it can damage the motherboard. Today, ATX and other motherboard form factors have a keyed power supply connector that allows the cable to be connected in only one direction.

2. Next, connect the <u>IDE/EIDE</u>, <u>SATA</u>, or <u>SCSI</u> cables to the motherboard from the hard drive, CD Drive, floppy drive.

3. Connect the <u>Molex</u> power cables from the power supply to each of the drives in the computer.

CMOS setup

Once the motherboard has been successfully installed and connected into the computer, connect the keyboard, monitor, and power to the computer. Do not connect all of the cables yet in case you encounter problems and need to disconnect all the cables again.

Once the computer boots <u>enter CMOS setup</u> and set all of the values not automatically detected. We recommend you check or set the below values.

1. **CPU Settings** - make sure the proper CPU speed and voltage is shown or that it is set to auto.

2. **Memory** - make sure the memory settings are right, and all memory is detected.

3. **Drives** - verify the floppy, hard drive, and CD-ROM drive are all shown.

4. If <u>onboard</u> video, modem, network, or sound is on your motherboard and you want to them disabled for an <u>expansion card</u> you are installing, disable these devices now.

5. Check other settings such as the time, date, and COM ports.

Once everything has been properly detected and setup, save the settings, then exit CMOS setup and reboot the computer.

TOPIC 5: PROCESSOR

Introduction to Computer Processing Unit (CPU)

Alternatively referred to as the **brain of the computer**, **processor**, **central processor**, or **microprocessor**, the **CPU** (pronounced as C-P-U) short for **Central Processing Unit**. The computer CPU is responsible for handling all <u>instructions</u> it receives from <u>hardware</u> and <u>software</u> running on the computer.

Processor Evolution

4-bit Microprocessors

The first microprocessor was introduced in 1971 by Intel Corp. It was named Intel 4004 as it was a 4 bit processor. It was a processor on a single chip. It could perform simple arithmetic and logic operations such as addition, subtraction, boolean AND and boolean OR. It had a control unit capable of performing control functions like fetching an instruction from memory, decoding it, and generating control pulses to execute it. It was able to operate on 4 bits of data at a time. This first microprocessor was quite a success in industry. Soon other microprocessors were also introduced. Intel introduced the enhanced version of 4004, the 4040. Some other 4 bit processors are International's PPS4 and Thoshiba's T3472.

8-bit Microprocessors

The first 8 bit microprocessor which could perform arithmetic and logic operations on 8 bit words was introduced in 1973 again by Intel. This was Intel 8008 and was later followed by an improved version, Intel 8088. Some other 8 bit processors are Zilog-80 and Motorola M6800.

16-bit Microprocessors

The 8-bit processors were followed by 16 bit processors. They are Intel 8086 and 80286.

32-bit Microprocessors

The 32 bit microprocessors were introduced by several companies but the most popular one is Intel 80386.

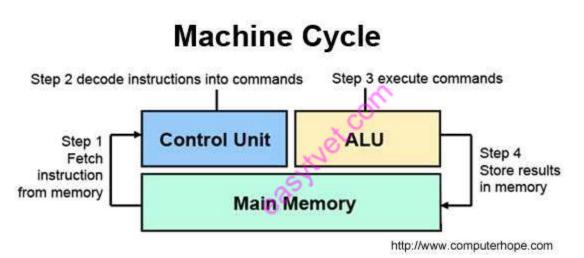### Pentium Series

Instead of 80586, Intel came out with a new processor namely Pentium processor. Its performance is closer to RISC performance. Pentium was followed by Pentium Pro CPU. Pentium Pro allows allow multiple CPUs in a single system in order to achive multiprocessing. The MMX extension was added to Pentium Pro and the result was Pentiuum II. The low cost version of Pentium II is Celeron.

The Pentium III provided high performance floating point operations for certain types of computations by using the SIMD extensions to the instruction set. These new instructions makes the Pentium III faster than high-end RISC CPUs.

Interestingly Pentium IV could not execute code faster than the Pentium III when running at the same clock frequency. So Pentium IV had to speed up by executing at a much higher clock frequency.

Components of the CPU

In the CPU, the primary components are the ALU (Arithmetic Logic Unit) that performs mathematical, logical, and decision operations and the CU (Control Unit) that directs all of the processors operations.

A **microprocessor** is a computer processor that incorporates the functions of a computer's central processing unit (CPU) on a single integrated circuit (IC), or at most a few integrated circuits

Microprocessor Characteristics

A processor, or "**microprocessor,**" is a small chip that resides in computers and other electronic devices. Its basic job is to receive input and provide the appropriate output. While this may seem like a simple task, modern processors can handle trillions of calculations per second.

The central processor of a computer is also known as the CPU, or "central processing unit." This processor handles all the basic system instructions, such as processing mouse and keyboard input and running applications.

Three basic characteristics differentiate microprocessors:

- **Instruction set**: The set of instructions that the microprocessor can execute.

- **Bandwidth :** The number of bits-processed in a single instruction. The amount of <u>data</u> that can be transmitted in a fixed amount of time

- **Clock speed :** Given in megahertz (<u>MHz</u>), the clock speed determines how many instructions per second the <u>processor</u> can <u>execute</u>.

In both cases, the higher the value, the more powerful the CPU. For example, a <u>32-bit</u> microprocessor that runs at 50MHz is more powerful than a 16-bit microprocessor that runs at 25MHz.

Specifications
Important specifications to consider when selecting microprocessor chips (MPU) include:

- **Data bus** - Most microprocessor chips are available with an 8-bit, 16-bit, 24-bit, 32-bit, 64-bit, 128-bit, or 256-bit data bus.

- **Microprocessor family** - Products from many proprietary microprocessor families are commonly available.

- **Supply voltage** - Supply voltages range from - 5 V to 5 V and include intermediate voltages such as - 4.5 V, - 3.3 V, - 3 V, 1.2 V, 1.5 V, 1.8 V, 2.5 V, 3 V, 3.3 V, and 3.6 V.

- **Clock speed** - Clock speed, the frequency that determines how fast devices connected to the system bus operate, is generally expressed in megahertz (MHz).

- **Random access memory (RAM)** - RAM is usually expressed in kilobytes (kB) or megabytes (MB).

- **Power dissipation** - Power dissipation, the device's total power consumption, is generally expressed in watts (W) or milliwatts (mW).

- **Operating temperature** - Operating temperature is a full-required range.

CPU Packaging (Microprocessor Types)
The actual microprocessor and its associated electronic circuits are packaged in a protective outer packaging. When you look at a processor, it's the packaging you see and not the microprocessor itself. Typically, the processor's packaging is ceramic or plastic.
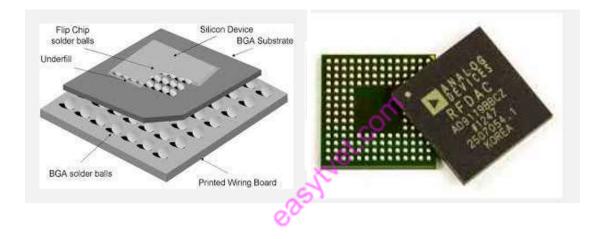
The outer covering of the processor protects its core (also called the die) that contains the microchip and the wiring that connects the chip to the processor's mounting pins. A variety of packaging types have been used on processors. Here are the basic types.

1) <u>Pin Grid Array (PGA):</u> Common among early processors, the mounting pins are located on the bottom of the chip in concentric squares. The earliest chips were packaged in the Ceramic PGA (CGPA). Later chips , including some current ones, use the Plastic PGA (PPGA). The early Pentium chips used a variation that staggered the pin pattern (in order to cram more

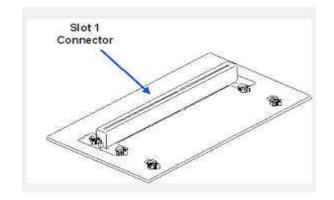pins onto the package) called the Staggered PGA (SPGA). The Pentium III features a variation of the PGA package with its Slot 370-like Flip Chip-Pin Graphics Assembly (FC-PGA)

2) <u>Plastic Ball Grid Array (PBGA):</u> The Primary difference between this packaging technology and the PGA is that the PBGA doesn't have mounting pins projecting from the bottom of the chip, which eliminates the threat of bent pins on the bottom of the processor. Otherwise, these package styles look similar.

3) <u>Single Edge Connector (SEC):</u> You may find a few variations on the packageing technology, including the Single Edge Contact Cartridge (SECC) and others. They all boil down to a packaging style that is mounted perpendicular to the motherboard into a single slot, much like expansion cards and memory modules. The Pentium II was the first processor to sport this new packaging style. This style made cooling the processor easier.

Microprocessor Addressing Modes

The different ways in which a source operand is denoted in an instruction is known as **addressing modes**. There are 8 different addressing modes in 8086 programming −

Immediate addressing mode

The addressing mode in which the data operand is a part of the instruction itself is known as immediate addressing mode.

Example

```
MOV CX, 4929 H, ADD AX, 2387 H,  MOV AL, FFH
```

Register addressing mode

It means that the register is the source of an operand for an instruction.

Example

```
MOV CX, AX   ; copies the contents of the 16-bit AX register into

             ; the 16-bit CX register),

ADD BX, AX
```

Direct addressing mode

The addressing mode in which the effective address of the memory location is written directly in the instruction.

Example

```
MOV AX, [1592H], MOV AL, [0300H]
```

Register indirect addressing mode

This addressing mode allows data to be addressed at any memory location through an offset address held in any of the following registers: BP, BX, DI & SI.

Example

```
MOV AX, [BX]  ; Suppose the register BX contains 4895H, then the contents

              ; 4895H are moved to AX

ADD CX, {BX}
```

Based addressing mode

In this addressing mode, the offset address of the operand is given by the sum of contents of the BX/BP registers and 8-bit/16-bit displacement.

<u>Example</u>

```
MOV DX, [BX+04], ADD CL, [BX+08]
```

Indexed addressing mode

In this addressing mode, the operands offset address is found by adding the contents of SI or DI register and 8-bit/16-bit displacements.

<u>Example</u>

```
MOV BX, [SI+16], ADD AL, [DI+16]
```

Based-index addressing mode

In this addressing mode, the offset address of the operand is computed by summing the base register to the contents of an Index register.

<u>Example</u>

```
ADD CX, [AX+SI], MOV AX, [AX+DI]
```

Based indexed with displacement mode

In this addressing mode, the operands offset is computed by adding the base register contents. An Index registers contents and 8 or 16-bit displacement.

<u>Example</u>

```
MOV AX, [BX+DI+08], ADD CX, [BX+SI+16]
```

Processor selection and upgrades

Upgrading your CPU can be a frustrating experience, even though the physical acts of removing an old processor and installing the new one are pretty easy. The more difficult questions to answer are these: When is the right time for me to upgrade a CPU? What processor will give me the best bang for the buck?

Complicating the matter for Intel CPU users is the plethora of socket formats that may be involved. At last count, Intel had four active socket formats for desktop PCs:

Choosing a replacement processor

Socket type, motherboard compatibility, and other factors limit the range of suitable upgrade processors. Even with those limitations, though, you'll likely have at least several and possibly dozens of processors to choose among.

Microprocessor manufacturers
There are a bunch of microprocessor manufacturers but Intel and AMD are the major producers and distributers in the microprocessor market.
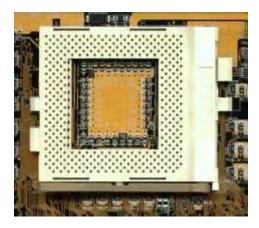
Intel - Intel is the leading microprocessor manufacturer. Its microprocessors include the Pentium, Celeron and Core lines. **Intel Corporation** is an American multinational technology company headquartered in Santa Clara, California. Intel is one of the world's largest and highest valued semiconductor chip makers, based on revenue. It is the inventor of the x86 series of microprocessors, the processors found in most personal computers.

AMD - AMD is Intel's main microprocessor rival. Its microprocessors include the Athlon, Turion and Phenom lines. Advanced Micro Devices, Inc. (AMD) is an American worldwide semiconductor company based in Sunnyvale, California, United States, that develops computer processors and related technologies for business and consumer markets.

Processor Socket and Slot Types

The motherboard has one or more sockets or slots into which the processor is inserted. The type of processor that can be used is defined by the type of socket or slot present on the motherboard.

A **CPU socket** or CPU slot is a mechanical component(s) that provides mechanical and electrical connections between a microprocessor and a printed circuit board (PCB). This allows the CPU to be placed/ sat and replaced without soldering.
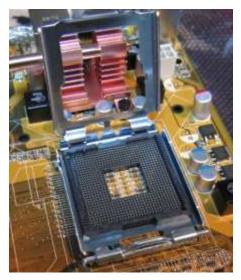
CPU socket example

A **CPU slot** is a computer processor connection designed to make upgrading the processor much easier, where the user would only have to slide a processor into a slot.

Intel Slot 1
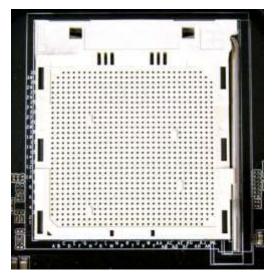
What Types Of Sockets Exist?

Many sockets have existed throughout history but only three are relevant today. These are LGA, PGA and BGA.

LGA and PGA can be understood as opposites. LGA stands for land grid array and consists of a socket with pins on which the processor is placed. PGA, on the other hand, places the pins on the processor, which are then inserted in a socket with appropriately placed holes. Intel uses the former while AMD uses the latter.

Then there's BGA, which stands for ball grid array. This technique is used to permanently attach a processor to its motherboard during production, making future upgrades impossible. BGA is typically less expensive and requires less physical space than a socket-able processor.

BGA technically is not technically a socket because it's permanent. It's worth mentioning however, because it serves the same function and may become the socket's replacement. Intel will start to ship more processors with BGA packaging by 2014 and <u>ARM processor</u> manufacturers, like Qualcomm and Nvidia, already rely heavily on BGA.

How to Install a New Computer Processor on a Motherboard

Things You Need:

- ✓ Processor
- ✓ Motherboard
- ✓ Screwdriver

Building your own computer can be a fun and challenging do-it-yourself project. Installing a new **computer processor** on your **motherboard** is the most delicate and important upgrade installation you can do. The **computer processor** is the centerpiece of the entire machine. You'll want to be cautious when installing processors in a socket on your **motherboard**, but it's a quick and simple task. Follow these simple steps to install your own computer **processor** safely.

Installing a Computer Processor:

1. Check motherboard compatibility: Each motherboard has a computer processor socket, but not all processors fit all motherboards. If you've already purchased either the motherboard or the processor or both, be sure that your computer processor is compatible with the processor socket on the motherboard.

2. Prepare the motherboard: If you're simply upgrading an old computer processor on an old motherboard, you may want to disassemble the computer and remove the motherboard from the computer case. Work on your computer in a non-carpeted area to reduce static electricity which can damage your computer processor, your motherboard and other components. Touch an unpainted metal surface to discharge static from your body.

3. Inspect the computer processor: The bottom of your processor will have many tiny pins. If any of the pins are broken or severely bent, you may need to return it for a new one.

4. Insert the processor: Most motherboards have a zero insertion force (ZIF) computer processor socket. This means you won't need to press down on the processor to install it. You'll instead use a lever on the motherboard socket itself.

   - Unlock the processor socket on the motherboard by lifting the small metal or plastic lever on the side of the processor socket. If you're replacing the old computer processor, remove it now and set it aside.

- Align the processor with the socket. The pins on the bottom of your computer processor are arranged in a specific pattern. When properly aligned, the pins will simply fall into place on the motherboard socket. Often, one corner of the processor will be marked to match up with a corresponding corner on the motherboard socket.

- Drop the processor into place and lock the socket. Once the pins are aligned with the holes in the processor socket, very gently lower and drop the processor into the socket on the mother board. Don't apply any pressure or force. Instead, gently close the socket lever and lock it in place. Your computer processor is now installed.

5. Finish installing components and test: Once you've finished installing the motherboard and other components into the computer case, test your computer system.

TOPIC 6: MEMORY

Introduction to Memory

Memory is the electronic holding place for instructions and data that your computer's microprocessor can reach quickly. When your computer is in normal operation, its memory usually contains the main parts of the operating system and some or all of the application programs and related data that are being used.

Memory is sometimes distinguished from *storage*, or the physical medium that holds the much larger amounts of data that won't fit into RAM and may not be immediately needed there.

Characteristics of Computer Memory

1. Electrical Characteristics - The voltage and current requirements depend on the manufacturing technology of the device. The voltage level is not of major concern because most of the semiconductor memory devices operate at TTL voltage levels.

2. Speed - There is a finite time delay between the application of address and the availability of stable and accurate data on the data lines. This memory delay depends on the manufacturing technology and other factors such as size.

3. Capacity representing the global volume of information (in bits) that the memory can store. Memory is small in size and hence its storage is relatively low

Types of Memories

1. **Random access memory**, generally called **RAM** is the system's main memory, i.e. it is a space that allows you to temporarily store data when a program is running.

    Unlike data storage on an auxiliary memory such as a hard drive, RAM is volatile, meaning that it only stores data as long as it supplied with electricity. Thus, each time the computer is turned off, all the data in the memory are irremediably erased.

2. **Read-only memory**, called **ROM**, is a type of memory that allows you to keep the information contained on it even when the memory is no longer receiving electricity. Basically, this type of memory only has read-only access. However, it is possible to save information in some types of *ROM* memory.

3. **Flash memory** is a compromise between RAM-type memories and ROM memories. Flash memory possesses the non-volatility of ROM memories while providing both read and write access However, the access times of flash memories are longer than the access times of RAM.

Types of Memory Modules Packaging

A **memory module** is a printed circuit board on which memory integrated circuits are mounted. Memory is made from tiny semiconductor chips and must be packaged into something less fragile and tiny in order to be integrated with the rest of the system.
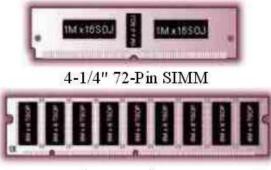
Types of memory module include:

SIMMS

SIMM stands for Single In-Line Memory Module. Like other types of memory modules, a SIMM consist of memory chips soldered onto a modular printed circuit board (PCB), which inserts into a socket on the motherboard. 72 pin SIMMs transfer 32 bits of data at a time, therefore in modern microcomputers with a 64-bit data bus two SIMMs have to be paired up in order to function.

DIMMS

Dual In-line Memory Modules, or DIMMs, closely resemble SIMMs. Like SIMMs, most DIMMs install vertically into expansion sockets. The principal difference between the two is that on a SIMM, pins on opposite sides of the board are "tied together" to form one electrical contact; on a DIMM, opposing pins rem a in electrically isolated to form two separate contacts.

168-pin DIMMs transfer 64 bits of data at a time and are typically used in computer configurations that support a 64-bit or wider memory bus. Some of the physical differences between 168-pin DIMMs and 72-pin SIMMs include: the length of module, the number of notches on the module, and the way the module installs in the socket. Another difference is that many 72-pin SIMMs install at a slight angle, whereas 168-pin DIMMs install straight into the memory socket and remain completely vertical in relation to the system motherboard. The illustration below compares a 168-pin DIMM to a 72-pin SIMM.

Comparison of a 72-pin SIMM and a 168-pin DIMM.

SO DIMMS

A type of memory commonly used in notebook computers is called SO DIMM or Small Outline DIMM. The principal difference between a SO

DIMM and a DIMM is that the SO DIMM, because it is intended for use in notebook computers, is significantly smaller than the standard DIMM. The 72-pin SO DIMM is 32 bits wide and the 144-pin SO DIMM is 64 bits wide.
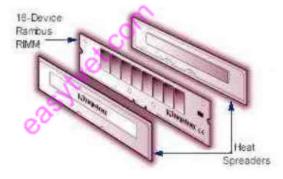
2.35" 72-pin SO DIMM   2.66" 144-Pin SO DIMM
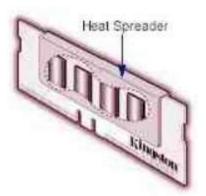
Comparison of a 72-pin SO DIMM and a 144-pin SO DIMM.

RIMMS AND SO-RIMMS

RIMM is the trademarked name for a Direct Rambus memory module. RIMMs look similar to DIMMs, but have a different pin count. RIMMs transfer data in 16-bit chunks. The faster access and transfer speed generates more heat. An aluminums heath, called a heat spreader, covers the module to protect the chips from overheating. A 184-pin Direct Rambus RIMM shown with heat spreaders pulled away.

An **SO-RIMM** looks similar to an SO DIMM, but it uses Rambus technology.

A 160-pin SO-RIMM module.

Memory-Mapping

What Is Memory-Mapping?

Memory-mapping is a mechanism that maps a portion of a file, or an entire file, on disk to a range of addresses within an application's address space. The application can then access files on disk in the same way it accesses dynamic memory. This makes file reads and writes faster in comparison with using functions such as `fread` and `fwrite`.

Benefits of Memory-Mapping

The principal benefits of memory-mapping are efficiency, faster file access, the ability to share memory between applications, and more efficient coding.

Faster File Access

Accessing files via memory map is faster than using I/O functions such as `fread` and `fwrite`. Data are read and written using the virtual memory capabilities that are built in to the operating system rather than having to allocate, copy into, and then deallocate data buffers owned by the process.

Efficiency

Mapping a file into memory allows access to data in the file as if that data had been read into an array in the application's address space. Initially, As a result, memory-mapped files provide a mechanism by which applications can access data segments in an extremely large file without having to read the entire file into memory first.

Memory Mapping types

There are a few different kinds of mappings that can be specified in the map attribute. All use the format described in the previous section.

Device Mapping: The most common kind of mapping. It is used for devices, RAM and ROM objects. The *target* field is not set.

Translator Mapping: Sometimes the address has to be modified between memory-spaces, or the destination memory-space depends on the address or some other aspect of the access such as the initiating processor. In these cases a *translator* can be used. A translator mapping is specified with the translator in the *object* field, and the default target as *target*. The translator has to implement the TRANSLATE interface. When an access reaches a translator mapping, the *translate* function in the TRANSLATE interface is called. The translator can then modify the address if necessary, and specify what destination memory-space to use. If it doesn't specify any new memory-space, the default one from the configuration is used. The following fields can be changed by the translator: physical_address, ignore, block_STC, inverse_endian and user_ptr.

Translate to RAM/ROM Mapping: Used to map RAM and ROM objects with a translator first. The *object* field is set to the translator, and *target* is set to the RAM/ROM object.

Space-to-space Mapping: Map one memory-space in another. Both *object* and *target* should be set to the destination memory-space object.

Bridge Mapping: A bridge mapping is typically used for mappings that are setup by some kind of bridge device. The purpose of a bridge mapping is to handle accesses where nothing is mapped, in a way that corresponds to the bus architecture. For a bridge mapping, the *object* field is set to the bridge device, implementing the BRIDGE interface. The *target* field is set to the destination memory-space.

Selection and upgrading memory

Do you suspect your computer could use more memory? Here's how to tell.

Here are a few simple — but telling — signs that your computer could benefit from a memory upgrade.

You experience poor or sub-par performance in everyday tasks. For instance, a program doesn't respond or seems to take forever to open.

You get system notifications that say "low memory" or "out of memory".

You are having display problems. Like when you pull up a page and it either partially loads or if refuses to load at all. Or you see a blank space where data should be.

In some cases, the PC refuses to operate at all. When you try to open anything, the system will not respond.

If you are experiencing any of these symptoms, a memory upgrade may be in order.

It's easy to tell how much memory is installed on your system and how much is being used.

Hardware Tips: Choose the Right Kind of Memory for Your System

Adding RAM to your PC usually delivers the most bang for your upgrade buck, but only if you buy the right kind of memory module for your PC. There are more types of PC RAM than there are lattes at Starbucks: Do you want SDRAM, PC100, non-parity, or un-buffered DIMM? Why not enjoy a refreshing DDR SDRAM, PC2700, CL2.5, or registered DIMM? Here are the ins and outs of PC memory.

Begin by checking your system's user manual to identify the types of RAM your PC's motherboard supports. If you don't have the manual, visit the manufacturer's Web site and search for downloadable manuals or other tools that might help you find the information you need.

Before you buy, ascertain the following:

Maximum module size: Find out the maximum size of memory module that your PC supports. Don't buy a module larger than what your motherboard's memory slots can each accommodate.

RAM and connector types: Determine which of the four types of RAM your system uses: DRAM (EDO or FPM), SDRAM, DDR SDRAM, or RDRAM. All four types are mounted on one of three module types: SIMM, DIMM, or RIMM.

Most machines support only one type of RAM and have one type of module or connector, so mixing types isn't an option. The few motherboards that do accept two types of RAM allow only a single type to be used at any one time.

Memory speed: SDRAM, DDR SDRAM, and RDRAM are rated to match or exceed the PC's front side bus speed, which is the speed at which data moves between the CPU and RAM. If your system comes with PC66 SDRAM, you can use PC100 SDRAM to replace it and get the faster speed, as long as your PC's front side bus supports the higher rate. But if you mix RAM of different speeds, all RAM will operate at the speed of the slowest chip.

Memory banks: On some PCs, the memory slot closest to the CPU--usually called bank 0--must be filled before the motherboard's other memory slots. On other systems, bank 0 must have the largest RAM module (if you are using modules of different sizes). There's no fixed rule, so check your PC's documentation.

Non-parity or ECC: If your system supports error-correcting code (ECC) and has more than 512MB of RAM, buying ECC memory may be worth the added cost. Large amounts of RAM are more likely to experience occasional, random errors (which may be caused by cosmic rays, among other sources). However, unless your current RAM is ECC, forget it; you can use non-parity and ECC modules together, but error correction will be disabled.

To determine your type of memory, count the number of chips on the memory module. If the number is divisible by three, you have ECC or parity memory.

Column address strobe: The lower the CAS rating--or the CL rating--is, the better. SDRAM comes in CL2 or CL3 types, and DDR SDRAM comes in CL2 or CL2.5. Unless your motherboard requires a specific CAS or CL rating, get the lower (faster) rated module. Cost differences should be negligible. Again, if you mix modules of different speeds, they'll all operate at the slowest module's speed.

Bios Hardware & Software

Short for **Basic Input/Output System**, the **BIOS** (pronounced bye-oss) is a ROM chip found on motherboards that allows you to access and set up your computer system at the most basic level.

The BIOS includes instructions on how to load basic computer hardware and includes a test referred to as a POST (Power On Self-Test) that helps verify the computer meets requirements to boot up properly. If the computer does not pass the POST, you will receive a combination of beeps indicating what is malfunctioning within the computer.

The four main functions of a PC BIOS

- **POST** - Test the computer hardware and make sure no errors exist before loading the operating system. Additional information on the POST can be found on our POST and Beep Codes page.
- **Bootstrap Loader** - Locate the operating system. If a capable operating system is located, the BIOS will pass control to it.
- **BIOS drivers** - Low-level drivers that give the computer basic operational control over your computer's hardware.
- **BIOS or CMOS Setup** - Configuration program that allows you to configure hardware settings including system settings such as computer passwords, time, and date.

What is the difference between BIOS and CMOS?

The terms **BIOS** and **CMOS** both refer to essential parts of your computer's motherboard. They work together and they're both important, but they are not the same thing.

Let's take a look at what the BIOS and CMOS are, and how they're different.

1. The **BIOS**, or "Basic Input/Output System", is special firmware stored in a chip on your computer's motherboard. It is the first program that runs every time you turn on your computer.

   The BIOS performs the POST, which initializes and tests your computer's hardware. Then it locates and runs your boot loader, or loads your operating system directly.

   The BIOS also provides a simple interface for configuring your computer's hardware. When you start your computer, you may see a message like "Press F2 for setup." This setup is your BIOS configuration interface. For more information about configuring your BIOS, see our guide to configuring your BIOS.

2. When you make changes to your BIOS configuration, the settings are not stored on the BIOS chip itself. Instead, they are stored on a special memory chip, which is referred to as "the CMOS." **CMOS** stands for "Complementary Metal-Oxide-Semiconductor." It's the name of a manufacturing process used to create processors, RAM, and digital logic circuits, and is also the name for chips created using that process.

   Like most RAM chips, the chip that stores your BIOS settings is manufactured using the CMOS process. It holds a small amount of data, usually 256 bytes. The information on the CMOS chip includes what types of disk drives are installed on your computer, the current date and time of your system clock, and your computer's boot sequence.

   On some motherboards, the CMOS is a separate chip. However, on most modern motherboards, it is integrated with the real-time clock (RTC) on the Southbridge.

   Your BIOS memory is non-volatile: it retains its information even when your computer has no power because your computer needs to remember its BIOS settings even when it's turned off. That's why the CMOS has its own dedicated power source, which is the CMOS battery.

How to enter the BIOS or CMOS setup

Because of the wide variety of computer and BIOS manufacturers over the evolution of computers, there are numerous ways to enter the BIOS or CMOS Setup. Below is a listing of most of these methods, as well as other recommendations for entering the BIOS setup.

Note: Apple, or Mac, computers do not have a BIOS and instead utilize an EFI, which does not need to modified based on the hardware in the computer, like a BIOS. The EFI provides better integration between hardware and software for Apple computers, virtually eliminating the need for a BIOS.

New computers

Computers manufactured in the last few years allow you to enter the BIOS setup using one of the five keys shown below during the boot process.

- F1
- F2 *
- F10 **
- Del
- Esc

Note: F1, F2, and F10 are all function keys on the top of the keyboard.

* If pressing F2 opens a diagnostics tool, your setup key is likely F10

** F10 is also used for the boot menu. If F10 opens a boot menu, your setup key is likely F2.

Setup keys are to be pressed as the computer is booting up. Most users will see a message similar to the example below upon startup. Some older computers may also display a flashing block to indicate when to press the F1 or F2 keys.

Press <F2> to enter BIOS setup

Tip: If your computer is new and you are unsure of what key to press when the computer is booting, try pressing and holding one or more keys on the keyboard to cause a stuck key error. Once you get this error, you should have the option to continue or enter setup.

Note: If you are still unable to enter the BIOS using the methods listed above, check the motherboard's manual for the appropriate key to enter BIOS. Documentation for the motherboard may also be found on the manufacturer's website.

Once you have successfully entered the CMOS setup, you should see a screen similar to the example below. Your CMOS setup may look a little different, depending on the manufacturer, but should still have most of the same options in the menu on the left or along the bottom of the screen.

How do I change and save changes in CMOS setup?

Once in CMOS setup, the method for changing the settings often depends on the BIOS manufacturer. You may use the arrow keys along with the Enter key to select categories and change their values. Some manufacturers may have you press the Page up and Page down keys to change the values.

Tip: All manufacturers show which keys navigate on the bottom or right-hand side of the screen.

I cannot change the values to a setting I want to use.

If you are trying to change the clock, speed, or other settings and do not have the option available, it is because it is not supported by the motherboard. If you believe it should be supported, you may need a BIOS update.

Tip: If changes you made appear to revert back to default settings or the date and time setting in the BIOS keeps falling behind, you may need to replace the CMOS battery.

How do I save the changes?

If any changes are made, you need to save those changes, which is typically done by pressing the F10 key on the keyboard. If F10 does not work, look at the bottom or top of the screen for the key that is used to save the settings.

Older computers

Unlike the computers of today, older computers (before 1995) had numerous methods of entering the BIOS setup. Below is a listing of key sequences to press as the computer is booting to enter the BIOS setup.

- Ctrl+Alt+Esc
- Ctrl+Alt+Ins
- Ctrl+Alt+Enter
- Ctrl+Alt+S
- Page Up key
- Page Down key

ACER BIOS
If your computer cannot boot or you want to restore the BIOS back to its bootable settings and your computer uses an ACER BIOS, press and hold the F10 key as you turn on the computer. While continuing to hold the F10 key, you should hear two beeps indicating that the settings are restored.

AMI BIOS
Older AMI BIOS could be restored back to bootable settings by pressing and holding the Insert key as the computer is booting.

BIOS or CMOS diskettes

Early 486, 386, and 286 computers required a floppy disk to enter the BIOS setup. These diskettes may be referred to as ICU, BBU, or SCU disks. Because these diskettes are unique to your computer manufacturer, you must obtain the diskettes from them. See the computer manufacturers list for contact information.

Early IBM computers

Some early IBM computers require you to press and hold both mouse buttons as the computer boots to enter the BIOS setup.
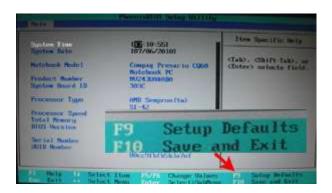
Other suggestions

Finally, if none of the above suggestions allow access to your CMOS setup, you can create a stuck key error, causing the CMOS setup prompt to appear until you press a key to continue. To do this, press and hold any key on the keyboard and do not let go (you may get several beeps as you are doing this). Keep pressing the key until the computer stops booting and you have the option to enter setup.

How to reset CMOS or BIOS settings

If the computer has problems booting, errors during boot, or other abnormal problems that cannot be resolved try resetting the CMOS settings to the default settings as explained below.

Note: If you are seeing an error about a "media test failure", there may be a loose cable inside the computer, or the hard drive might be bad.

Load or Reset defaults

To reset your computers CMOS or BIOS settings back to the default settings follow the steps below.

1. Enter CMOS setup.
2. In CMOS setup, look for an option to reset the CMOS values to the default setting or an option to load the fail-safe defaults. With many CMOS setup screens, there will be a function key to do this. For example, the F5, F6, F9, F11, or F12 key, as shown in the picture, may be set up as a shortcut to load the default settings. Other setups may list an option that you can arrow over to using the arrow keys and pressing Enter.
3. When found and selected, you'll likely be asked if you're sure you want to load the defaults. Press Y for yes or arrow to the yes option.
4. Once the default values have been set, make sure to Save and Exit and not just exit.

Reset Configuration Data

If you've recently added new hardware or resetting the default values did not help resolve your boot issues, you may also want to reset the configuration data.

Note: Not all CMOS setup screens have this feature.

Under advanced

If you're working on a computer with a Phoenix BIOS that has **Main - Advanced - Security** listed at the top of the screen, you can get to this setting by using the right arrow to move over to **Advanced**. Under Advanced, arrow down to the **Reset Configuration Data** option and change the value from *Disabled* or *No* to **Enabled** or **Yes**.

Once the above has been done, press the **F10** key and **Save and Exit** CMOS setup.

In PnP/PCI Configurations

If you're working with a Phoenix BIOS that has different options and one of them is **PnP/PCI Configuration**, move the cursor down to this option and press Enter. Within the PnP/PCI Configurations, change the **Reset Configuration Data** from *Disabled* to **Enabled**.

Once the above has been done press the **F10** key and **Save and Exit** CMOS setup.

Hard reset the CMOS

Caution: When inside your computer, make sure you're aware of ESD and all it's potential dangers.

If the above steps do not reset the CMOS settings, we suggest removing the CMOS battery, like the one in the picture, causing the computer to forget all CMOS settings, including the password. Wait 5 minutes after removing the battery, then put the battery back into the motherboard and turn it on.

- How to remove the CMOS battery

If your computer does not have a CMOS battery or you're unable to find it, you'll need to do a hard reset on the CMOS using a jumper or dip switch on the motherboard. Information on finding these can be found in your computer or motherboard documentation.

TOPIC 7: STORAGE

Introduction to Storage Disks and Drives

Computer data storage, often called **storage** or **memory**, is a technology consisting of computer components and recording media used to retain digital data. It is a core function and fundamental component of computers.

There are two different categories of storage devices:

Primary Storage Devices: Generally smaller in size, are designed to hold data temporarily and are internal to the computer. They have the fastest data access speed, and include RAM and cache memory.

Secondary Storage Devices: These usually have large storage capacity, and they store data permanently. They can be both internal and external to the computer, and they include the hard disk, compact disk drive and USB storage device.

Note: A disk is a device on which data is stored while a drive is a device used to record/read from a disk. Some devices incorporate the disk and drive together (i.e. Hard drive/hard disk drive) but others are in separate (i.e. CD/Floppy disks and drives)

Types of computer storage and Disks

The following are some examples of types of storage devices used with computers.

Magnetic storage/disks devices - Today, magnetic storage are one of the most common types of storage used with computers and are the technology that many computer hard drives use. It uses magnetism as its method of reading and writing data.

- Floppy diskette
- Hard drive
- Super Disk
- Tape cassette
- Zip diskette

Optical storage/disks devices - Another common storage is optical storage, which uses lasers and lights as its method of reading and writing data.

- Blu-Ray disc
- CD-ROM disc
- CD-R and CD-RW disc

- DVD-R, DVD+R, DVD-RW, and DVD+RW disc

Flash memory devices - Flash memory has started to replace magnetic media as it becomes cheaper and more efficient solution.
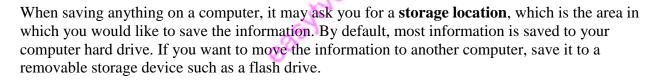
- Jump drive or flash drive
- Memory card
- Memory stick
- SSD

Online and cloud - Storing data online and in cloud storage is becoming popular as people need to access their data from more than one device.

- Cloud storage
- Network media

Paper storage - Early computers had no method of using any of the above technologies for storing information and had to rely on paper. Today, these forms of storage are rarely used or found.

- OMR
- Punch card

When saving anything on a computer, it may ask you for a **storage location**, which is the area in which you would like to save the information. By default, most information is saved to your computer hard drive. If you want to move the information to another computer, save it to a removable storage device such as a flash drive.

Tip: Keep in mind that although these devices do send and receive information, they are not considered an input device or output device.

Meaning of Disk management

Disk Management is an extension of the Microsoft *Management* Console that allows full *management* of the *disk*-based hardware recognized by Windows.

You can use Disk Management in this version of Windows to perform disk-related tasks such as creating and formatting partitions and volumes, and assigning drive letters.

Disk management - Computer *Definition*. An umbrella term for a variety of functions for initializing a hard *disk*, maintaining its health and *managing* its organization

Disk management Techniques

These are tools and methods used in disk management

What is a system utility?

System utilities are programs that are designed to help you fix and enhance your current computer system. Many operating systems include a range of utility programs to perform common tasks such as checking disks, backing up information, restoring information and reorganizing information. Many other system utilities are available as third party software – this means that you purchase and install these utilities separately from the operating system software. Third party system utilities are designed to perform specific functions that the current operating system either does not perform or performs at a lesser standard.

The types of system utilities we'll look at in this reading will allow you to perform these basic tasks:

- disk scan

- disk defragment

- file back up

- file recovery

- get system information.

What is a disk scan?

A disk scan is a useful utility to help identify and repair problems on a hard disk or floppy disk; it is provided with some operating systems. It can perform a thorough check of the disk's surface to ensure that it is able to read and write information on all areas of the disk. If the disk scan utility finds a problem it will usually display a message and offer to fix the problem.

There is a disk scan utility on recent versions of Microsoft Windows and Apple Macintosh operating systems, where if you turn off your computer without exiting the system, the **Scan Disk** utility will run automatically the next time you start your computer.

There are also third party utilities that you are able to use that will perform similar and sometimes more thorough scans of the disk.
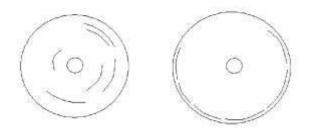
What is defragment?

To a computer, defragment means that all the files on the computer's hard disk will be placed in a neat and tidy order.

Gradually, as a computer hard disk has many files added, updated and deleted, the files can start to become fragmented. **Fragmentation** means that portions of the files are scattered all over the

disk. A defragment will ensure that all files are reordered so that their parts are placed adjacent to one another. This will mean the computer can now read these files much more quickly.

Depending on how many files need to be reorganised, a defragment can take hours. If you use your computer regularly you should try and do a **defragment at least once a month**. A good time to do a defragment may be overnight – when nobody will be using the computer.

Often an operating system will include several system tools, including the defragment utility. If it is not included with the operating system, a defragment program can be purchased as an external software program (a third party utility).

Figure 1: A diagram of a disk before and after a defragment. The picture on the left displays a disk with lines (representing data) that have been randomly placed on the disk. The picture on the right displays a disk after defragmentation — the lines (data) now appear in a consecutive order.

Figure 2: A screenshot of the Disk Defragmenter utility provided with the Microsoft Windows XP operating system

Backing up

Backing up means making a copy of your files, in case your computer hard disk fails and your original files become 'corrupted'. Although for the majority of time the computer's hard disk will not have any problems, occasionally a disk may fail unexpectedly. Some reasons why a hard disk may fail include:

- a sudden power failure

- computer virus damaging the hard disk

- damaged caused by knocking or moving the hard disk.

Backups need to be done on a **regular basis**, so if there is a problem you will still have a recent copy of your files. It is also a good idea to keep backups in another location away from your computer. Make sure where you store your backup information is away from sunlight, dust and magnetic fields.

Choosing a backup media

It is important to choose the most appropriate kind of media to backup data to. When choosing media, be realistic; it is better to store backups using media that has a large capacity. Some suggestions include:

- **Second hard disk**: Some computers may have a second hard disk available that will allow a fast and easy method of backing up data.

- **CD or DVD:** Many computers have CD and DVD burners that will allow you to 'burn' data onto a writeable CD or DVD.

- **Zip disk**: Zip disks are removable disks that hold between 100MB and 250MB of information.

- **Tape drive**: A medium that may be used by a business to backup business information.

What should you backup?

Backup anything that you have created yourself — including documents, digital photographs and video. All of these items will have no other way of being replaced if there are problems later on. If there is a problem, you can always reinstall the operating system and the application software using the original software CDs.

How often should you backup?

How often you backup will really depend on how often you use the computer and what is being stored on the computer. If, for example, your computer contains important business information that you are using everyday, it is a good idea to try to back up **everyday**. If, however, you only use your computer occasionally to play games or write the odd letter, a backup will probably only need to be done **once a month**.

How to perform a backup

Some operating systems include special backup utilities that make it easy for you to back up important files. If you don't have a backup utility already installed you could install a third party program that is designed to do backups or manually copy and paste your files from the hard disk to your backup device.

Backup programs allow you to easily select files that you want to back up, then they copy the files to the chosen backup device. A backup program may also compress the files before they are copied so you can fit more files onto the backup device.

Recovery

A recovery utility is used to **undelete** a file that has been accidentally deleted. Many operating systems now include special recovery utilities to help you restore files that have accidentally been removed. Microsoft Windows includes a **Recycle Bin** and Macintosh operating systems include **Trash**. Both of these utilities allow you a second chance to undelete any files on the hard disk.

There is also a recovery utility in recent version of Microsoft Windows called **System Restore**. The System Restore utility keeps a regular log of all current settings so if, for example, a new installation of a program is causing problems System Restore will be able to reset all settings back to how they were before the installation.

Figure 3: A screenshot of the System Restore utility in Microsoft Windows XP operating system

Hard Disk Interface(s)

Hard drives and other devices are connected to a computer motherboard through some type of cable. These cables use multiple smaller wires in parallel to transmit the proper signals for reading and writing to and from the drive. There are multiple types of cables, which transmit at different speeds and use different types of connectors. Here we will look at some of the most common device cables and the differences between them.

SCSI - SCSI stands for Small Computer System Interface and used a parallel cable to attach both internal and external devices. One of the benefits of SCSI interfaces is that multiple devices could be chained together to a single port. Another benefit is that the interface includes features like error checking and hand shake signals between devices.

IDE - IDE stands for Integrated Drive Electronics and refers more to the standard than the cable type itself. The technology is also often referred to as ATA or PATA. ATA cables can only be up to 18 inches in length and are fairly large and flat, which makes them a poor choice for external devices, so the interface is mainly used for internal devices. The cable uses a combination of 40 or 80 wires in parallel.

SATA - SATA stands for Serial ATA and is an evolution of the original ATA (or IDE) interface. The SATA interface is faster in speed, at up to 3GB/s. Another major benefit of the interface is that the cables and connectors are much smaller, taking up less space inside a computer case and not restricting air flow. There is an external version of SATA known as eSATA for connecting external hard drives and other devices.

Interface cables have improved quite a bit over the years, but the basic concept of input and output has remained mainly the same. New interfaces such as Thunderbolt have added even faster transfer speeds and taken some of the benefits from multiple technologies to make an improved connection.

Formatting and Partitioning a Hard Drive

Definitions

There are a few words we need to define before going any further. Don't worry, there *won't* be a test. :-)

- **Partition, partitioning:** Free space on a hard disk must be partitioned before it can be used by an operating system. Creating a partition reserves a physical portion of the hard drive space for use as a logical drive, or volume, that the operating system can address.
- **Volume:** A volume is how the operating system 'sees' your free disk space. Volumes (also called logical drives) are represented in Windows by drive letters such as C:, E:, etc.

Volumes are formed by partitioning the free space of a hard drive. Volumes must be formatted with a file system before data can be stored on them.
- **Formatting:** Formatting is the act of creating a file system on a volume, so that the operating system can store and retrieve data on that volume.
- **File system:** A file system provides a means of organizing and retrieving information written to a hard disk or any other storage medium. A file system is created on a volume when it is formatted. Common Windows file systems include FAT32 (File Allocation Table 32) and NTFS (New Technology File System).

Partition can be thought of as a division or "part" of a real hard disk drive. When you partition a hard drive, you make it available to an operating system. Multiple partitions on a singe hard drive appear as separate drives to the operating system.

A partition also is used to mean the *division* of certain kinds of secondary storage (such as hard disk drives (HDDs)), via the creation of multiple sub-divitions. Partitions are logical containers which are usually used to house file systems, where operating systems, applications, and data are installed on. A single partition may span the entirety of a physical storage device.

Disk formatting is the process of preparing a data storage device such as a hard disk drive, solid-state drive, floppy disk or USB flash drive for initial use.

The first part of the formatting process that performs basic medium preparation is often referred to as "low-level formatting".

The second part, Partitioning is the common term for the part in the process in disc preparation, making the data storage device visible to an operating system.

The third part of the process, usually termed "high-level formatting" most often refers to the process of generating a new file system. In some operating systems all or parts of these three processes can be combined or repeated at different levels and the term "format" is understood to mean an operation in which a new disk medium is fully prepared to store files.

TOPIC 8: POWER SUPPLY

Introduction to Power Supply

Also called a *power supply unit* or *PSU*, the component that supplies power to a computer. Most personal computers can be plugged into standard electrical outlets.

The power supply then pulls the required amount of electricity and converts the AC current to DC current. It also regulates the voltage to eliminate spikes and surges common in most electrical systems. Not all power supplies, however, do an adequate voltage-regulation job, so a computer is always susceptible to large voltage fluctuations.

Power supplies are rated in terms of the number of watts they generate. The more powerful the computer, the more watts it can provide to components.

Functions/importance

1. It provides the driving (electric) power for all essential computer components, such as the processor, motherboard, memory modules, video card and add-in cards, as well as hard drives and optical drives.
2. The computer power supply converts an alternative current (AC, which is obtained from the wall socket) into a specified voltage direct current (DC, which can be used by computer components).
3. Regulates (for some PSU), the voltage to eliminate spikes and surges common in most electrical systems

Power Supplies Types/Form Factors

Like motherboards and computer cases, there are several different power supply form factors, sizes, connector types, output specifications and other important specs. The detailed differences between these power supplies are extremely important and can make the difference between the ability to run a computer at its full potential and having a potentially unstable computer.

ATX

Although there are still AT form factor power supplies available for purchase, AT form factor power supplies are undoubtedly phased out products. Even the later ATX form factor power supply (ATX 2.03 and earlier versions) are falling out of favor. The major differences between the ATX and AT power supply form factors are:

1. ATX power supplies provide an extra +3.3V voltage rail.

2. ATX power supplies use a single 20-pin connector as the main power connector.
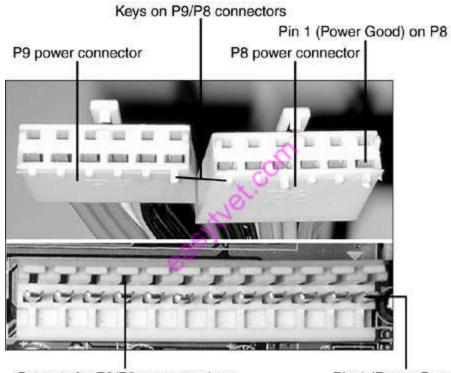
3. ATX power supplies support the soft-off feature, allowing software to turn off the power supply.

Note

There are two major types of power connectors on motherboards:

- 12-pin, modeled after the original IBM PC power connector and used on Baby-AT and LPX motherboards (see Figure 5.5)

Figure 5.5. Twin 6-pin power connectors are used on AT/LPX and other power supply types that attach to motherboards with a 12-pin connector.
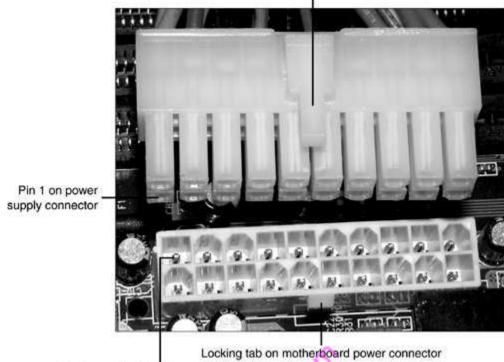
- 20-pin, used by all motherboards in the ATX family (see Figure 5.6) and by the NLX riser card (which provides power to the NLX motherboard)

Figure 5.6. The ATX power supply has a single 20-pin power connector. The extra connectors (compared to the LPX design in Figure 5.5) provide support for 3.3V and for software- or keyboard-controlled power down. Many of these power supplies don't have an external power switch for that reason.

Release lever on ATX/SFX power supply connector

Pin 1 on power supply connector

Locking tab on motherboard power connector

Pin 1 on motherboard power connector

ATX12V

The ATX12V form factor is the mainstream choice now. There are several different versions of the ATX12V form factor, and they can be very different from one another. The ATX12V v1.0 specification added over the original ATX form factor a 4-pin +12V connector to deliver power exclusively to the processor; and a 6-pin auxiliary power connector providing the +3.3V and +5V voltages. The ensuing ATX12V v1.3 specification added on top of that the 15-pin SATA power connector.

A substantial change occurred in the ATX12V v2.0 specification, which changed the main power connector from a 20-pin to a 24-pin format, removing the 6-pin auxiliary power connector. In addition, the ATX12V v2.0 specification also isolated the current limit on the 4-pin processor power connector for the 12V2 rail (+12V current is split into the 12V1 and 12V2 rails). Later, the ATX12V v2.1 and v2.2 specifications also increased efficiency requirements and mandated various other improvements.

All ATX12V form factor power supply units maintain the same physical shape and size as the ATX form factor.

EPS12V, SFX12V and Others

The EPS12V power supply form factor utilizes an 8-pin processor power connector in addition to the 4-pin connector of the ATX12V form factor. (Note: this isn't the only difference between these two form factors, but for most desktop computer users, knowing this should be sufficient).

The EPS12V form factor was originally designed for entry-level servers, but more and more high-end desktop motherboards are featuring the 8-pin EPS12V processor power connector now, which enables users to opt for an EPS12V power supply.

The Small Form Factor (SFF) designation is used to describe a number of smaller power supplies, such as the SFX12V (SFX stands for Small Form Factor), CFX12V (CFX stands for Compact Form Factor), LFX12V (LFX stands for Low Profile Form Factor) and TFX12V (TFX stands for Thin Form Factor). They are all smaller than the standard ATX12V form factor power supply in terms of physical size. SFF power supplies need to be installed in corresponding SFF computer cases.

Table 3.2 Power Supply Connector Types and Form Factors

Modern PS Form Factors	Originated From	Connector Type	Associated MB Form Factors
LPX style* [Low Profile eXtension]	IBM PS/2 Model 30 (1987)	AT	Baby-AT, Mini-AT, LPX
ATX style [Advanced Technology Extended]	Intel ATX, ATX12V (1985/2000)	ATX	ATX, NLX, Micro-ATX
SFX style [Small *Form Factor*]	Intel SFX (1997)	ATX	Flex-ATX, Micro-ATX

Note: LPX is also sometimes called Slimline or PS/2.

Common Power Problems and solutions

Power supply problems Diagnosis

1. The light or fan on the power supply does not work.
2. Nothing in the computer works.(plug something into the USB power to see if there is power going to it)

3. No lights / fans or beeps come from the computer.

   If any of the above happen to you try changing the power supply unit. This can be down by removing the computer case and removing the PSU. The PSU is only held by a few screws.

Here are some of the most common power supply problems and their likely effect on sensitive equipment:

1) Power Surges

A power surge takes place when the voltage is 110% or more above normal. The most common cause is heavy electrical equipment being turned off. Under these conditions, computer systems and other high tech equipment can experience flickering lights, equipment shutoff, errors or memory loss.

Possibile Solutions: Surge Suppressors, Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

2) High-Voltage Spikes

High-voltage spikes occur when there is a sudden voltage peak of up to 6,000 volts. These spikes are usually the result of nearby lightning strikes, but there can be other causes as well. The effects on vulnerable electronic systems can include loss of data and burned circuit boards.

Possibile Solutions: Surge Suppressors,Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

3) Transients

Transients are potentially the most damaging type of power quality disturbance that you may encounter. Transients fall into 2 categories.

- Impulsive
- Oscillatory

Possibile Solutions: Surge Suppressors, Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

4) Frequency Variation

A frequency variation involves a change in frequency from the normally stable utility frequency of 50 or 60 Hz, depending on your geographic location. This may be caused by erratic operation of emergency generators or unstable frequency power sources. For sensitive equipment, the results can be data loss, program failure, equipment lock-up or complete shut down.

Possibile Solutions: Voltage Regulators, Power Conditioners

5) Power Sag

A sag is the reduction of AC Voltage at a given frequency for the duration of 0.5 cycles to 1 minute's time. Sages are usually caused by system faults, and often the result of switching on loads with high demand startup currents.

Possibile Solutions: Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

6) Electrical Line Noise

Electrical line noise is defined as Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI) and causes unwanted effects in the circuits of computer systems. Sources of the problems include motors, relays, motor control devices, broadcast transmissions, microwave radiation, and distant electrical storms. RFI, EMI and other frequency problems can cause equipment to lock-up, and data error or loss.

Possibile Solutions: Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

7) Brownouts

A brownout is a steady lower voltage state. An example of a brownout is what happens during peak electrical demand in the summer, when utilities can't always meet the requirements and must lower the voltage to limit maximum power. When this happens, systems can experience glitches, data loss and equipment failure.

Possibile Solutions: Voltage Regulators, Uninterruptable Power Supplies, Power Conditioners

8) Blackouts

A power failure or blackout is a zero-voltage condition that lasts for more than two cycles. It may be caused by tripping a circuit breaker, power distribution failure or utility power failure. A blackout can cause data loss or corruption and equipment damage.

Possibile Solutions: Generators

Power Supply Protection Devices

The following types of power-protection devices are explained in the sections that follow:

- Surge suppressors
- Phone-line surge protectors
- Line conditioners
- Standby power supplies (SPS/UPS)
- Uninterruptible power supplies (UPS)

Surge Suppressors (Protectors)

The simplest form of power protection is any one of the commercially available **surge protectors**—that is, devices inserted between the system and the power line. These devices, can absorb the high-voltage transients produced by nearby lightning strikes and power equipment. They clamp and shunt away all voltages above a certain level.

Line Conditioners

In addition to high-voltage and current conditions, other problems can occur with incoming power. The voltage might dip below the level needed to run the system, resulting in a brownout. Forms of electrical noise other than simple voltage surges or spikes might travel through the power line, such as radio-frequency interference or electrical noise caused by motors or other inductive loads.

Remember two things when you wire together digital devices (such as computers and their peripherals):

- Any wire can act as an antenna and have voltage induced in it by nearby electromagnetic fields, which can come from other wires, telephones, CRTs, motors, fluorescent fixtures, static discharge, and, of course, radio transmitters.
- Digital circuitry responds with surprising efficiency to noise of even a volt or two, making those induced voltages particularly troublesome. The electrical wiring in your building can act as an antenna, picking up all kinds of noise and disturbances.

A **line conditioner** can handle many of these types of problems. It filters the power, bridges brownouts, suppresses high-voltage and current conditions, and generally acts as a buffer between the power line and the system. A line conditioner does the job of a surge suppressor, and much more. It is more of an active device, functioning continuously, rather than a passive device that activates only when a surge is present. A line conditioner provides true power conditioning and can handle myriad problems. It contains transformers, capacitors, and other circuitry that can temporarily bridge a brownout or low-voltage situation.

UPS

Lighting, telephones, mobiles, laptops, chargers, PCs, tablets, peripherals and servers all depend absolutely upon a reliable electricity supply, as do industrial processes. The answer is to use a UPS – a mature technology that is still being improved to cope with ever more difficult power demands. UPS avoid un-planned power outages, save valuable data and provide time (autonomy) to allow safe shutdown of affected equipment.

UPS represent big and growing business because of the increasing reliance on ever greater numbers of digital devices, as well as the demand for cleaner power that they require, and from the changing nature of mains power supplies themselves. For example, as older coal-fired power stations are phased-out, and as more renewable sources are installed, grids will change in ways that are not fully understood – but there will almost certainly be shortfalls. Coming smart grids will also have an effect.

TOPIC 9: COMPPUTER ASSEMBLY & DISASSEMBLY

Introduction to Computer Hardware Inventory

Hardware, in the computer world, refers to the physical components that make up a computer system.

There are many different kinds of hardware that can be installed inside, and connected to the outside, of a computer.

Below is a list of **external hardware** and **internal hardware** that may be found with a computer.

External hardware examples

- **Projector** - a projector is an output device that can take images generated by a computer and reproduce them on a large, flat (usually lightly colored) surface. For example, **projectors** are used in meetings to help ensure that all participants can view the information being presented.
- **Scanner** - a hardware input device that allows a user to take an image or text and convert it into a digital file, allowing the computer to read or display the scanned object.
- Speakers8
- **USB thumb drive** - a portable drive that is often the size of your thumb that connects to the computer USB port.
- **Flat-panel, Monitor, and LCD** - screen displays
  o **Monitor,** alternatively referred to as a **video display terminal (VDT)** and **video display unit (VDU)**, comprised of a CRT (Cathode Ray Tube) and a fluorescent screen as display system.
  o **Liquid-Crystal Display**, **LCD** is a flat display technology. The LCD is made of two sheets of a flexible polarizing material with a layer of liquid crystal solution between the two and available as an active matrix, dual-scan, or passive-matrix display. i.e. in laptops
  o **FPD**, a **flat-panel display** is a thin screen display. Flat-panel displays use Liquid-crystal display (LCD) technology to make them much lighter and thinner when compared with a traditional monitor. I.e. in TFT displays.
- Keyboard
- Microphone
- Mouse
- Printer

Internal hardware examples

- **CPU** - Alternatively referred to as the **brain of the computer**, **processor**, responsible for handling all instructions it receives from hardware and software running on the computer.

- Drive (e.g. Blu-Ray, CD-ROM, DVD, floppy drive, and hard drive)
- **Fan (heatsink)** - A **heat sink** is an electronic device that incorporates either a fan or a peltier device to keep a hot component such as a processor cool.
- **Modem** - Short for **MODulator/DEModulator** The Modem is a hardware device that enables a computer to send and receive information over telephone lines by converting the digital data used by your computer into an analog signal used on phone lines and then converting it back once received on the other end.
- **Motherboard** - printed circuit board , located at the bottom of the computer case. It allocates power to the CPU, RAM, and all other computer hardware components. Most importantly, the motherboard allows hardware components to communicate with one another.
- **Network card** - Short for **Network Interface Card**, the **NIC** is also referred to as an **Ethernet card** and **network adapter**. It is an expansion card that enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable with an RJ-45 connector.
- RAM
- **Sound card** - Alternatively referred to as a **sound board** or **audio card**, a **sound card** is an expansion card or integrated circuit that provides a computer with the ability to produce sound that can be perceived by the user through a peripheral device like speakers or headphones.
- **Video card** - Alternatively referred to as a **display adapter**, **graphics card**, **video adapter**, **video board**, or a **video controller**, a **video card** is an internal circuit board that allows a display device such as a monitor to display images from the computer.

Hardware upgrading

A **hardware upgrade** is any new hardware better than that which it replaced or additional hardware that improves performance. A good example of a common hardware upgrade is a RAM upgrade, where the user increases the computer's total memory. Another good example is a video card upgrade, which is the act of removing an old video card and replacing it with a newer, better one.

Benefits of a hardware upgrade

1. Performance increase, which make the overall computer run faster and more smoothly.
2. Capacity increase. For example, adding a new hard drive allows the computer to store more information, and more memory increases the computers ability to run more.
3. It may be necessary to upgrade the computer to meet a program or games system requirements.

Choosing the Right Upgrade

It's important to understand at least the basics about what's going on inside your computer, and what a hardware upgrade can and cannot do. You can't turn a slow computer into a fast one simply by increasing the size of a hard drive. Likewise, upgrading the computer's processor probably won't make a computer that's prone to crashing more reliable.

Here are some guidelines for deciding what to upgrade.

Type of Upgrade	Guidelines	Difficulty

RAM	To see the biggest increase in performance, increase the amount of RAM in an older computer. A good sign you could benefit from more RAM is if your computer slows down a lot when you try to use several programs simultaneously. Put in as much RAM as the computer will support. Keep in mind that a 32-bit operating system can only handle 4 GB of RAM.	Moderate
Graphics card	Because graphics processing uses RAM, a graphics card upgrade may improve overall performance. If you work with a lot of digital video, you can probably benefit from adding RAM and/or changing from an integrated or "on-board" graphics card to a dedicated graphics card. Be sure that your motherboard can support the new card you are installing.	Moderate
Hard drive	If you're running out of storage space, you can upgrade to a bigger hard drive with more storage capacity. If your computer is slow, upgrading to a faster hard drive may improve overall performance: • In traditional drives, the faster the drive spins, the faster data can be read and written. So upgrading from a drive that spins at 5,400 rotations per minute (rpm) to a 7,200-rpm drive may speed up your computer's performance. • A solid-state drive (SSD) is another option. SSDs don't spin, so their speed isn't measured in rpms. But they are significantly faster and (because they have no moving parts) less prone to mechanical problems than traditional drives. If your old drive is still functional, consider adding a drive instead of removing and replacing the older one. Most desktop computer motherboards can handle up to four hard drives, including the optical drive. Completely replacing a hard drive will involve some additional steps, since you need to transfer all your files from the old drive to the new one, as well as reinstalling the operating system and all the software.	Moderate to Advanced
Optical (CD/DVD) drive	Upgrading from a CD drive to a DVD drive allows you to take advantage of the increased capacity of DVDs over CDs. The additional capacity of DVDs makes copying files or backing up easier and less time-consuming. In terms of difficulty, the mechanical part of replacing an optical	Moderate

	drive is similar to replacing a hard drive, but you don't have to worry about moving files or transferring software.	
Processor (CPU)	A faster processor can help your computer run faster, but this is not an easy upgrade and should be approached with caution. Keep in mind that performance improvements with a faster processor may be negligible without sufficient RAM. When installing a new processor, the key consideration (besides number of cores and speed) is finding one that will work with your motherboard.	Advanced

Disassembling and Assembling the computer system

Disassemble is the process of breaking down a device into separate parts. A device may be disassembled to help determine a problem, to replace a part, or to take the parts and use them in another device or to sell them individually. For example, if a computer has a bad processor a user may need to disassemble the computer to get to the bad processor and replace it with a good processor.

Assemble is to fit or join together (the *parts* of something, such as a computer).

The assembling of the computer system is exactly the opposite of disassembling operation.

Steps on how to disassemble a computer

1. *The first thing you do, is unplug every cable that's plugged in to your computer.*
2. Now that your computer is fully unplugged, move your PC to a clean work space, preferably a carpet. The carpet is better than tile, because screws and other small parts will roll around.
3. Remove outer Shell/Casing
4. Now that the case is off, begin to remove the internal components which is system fan. Remove the CPU fan.
5. Unscrew the power supply.
6. Unscrew or disassemble DVD or CD Drive.
7. Remove or unscrew the Card reader (Available in new computer)
8. Remove the hard Disk Drive.
9. Remove the Expansion Card slots.
10. Remove the Connectivity Center Cables
11. Remove RAM (Random Access Memory)
12. Remove Power Button & Power LED + HDD LED
13. Remove the Connectivity Center
14. Remove Motherboard.

TOPIC 10: SOFTWARE INSTALLATION

Introduction to Computer software installation

Installation (or **setup**) of a **computer program** (including device drivers and plugins), is the act of making the **program** ready for execution.

File System

A file system can be thought of as an index or database containing the physical location of every piece of data on the hard drive or other storage device.

Any place that a computer or other electronic device stores data is employing the use of some type of file system. A file system is setup on a drive during a format.

Windows File Systems
1.   The Microsoft Windows operating systems have always supported, and still do support, various versions of the **FAT** file system.
2.   In addition to FAT, all Microsoft Windows operating systems since Windows NT support a newer file system called **NTFS**.
3.   All modern versions of Windows also support **exFAT**, a file system designed for flash drives.

File Allocation Table (FAT) is a file system that was created by Microsoft in 1977. FAT is still in use today as the preferred file system for floppy drive media and portable, high capacity storage devices like flash drives.

The File Allocation Table file system has seen advancements over time primarily due to the need to support larger hard disk drives and larger file sizes.

Below is more information on the versions of the FAT file system:

- **FAT12** - The initial version of the FAT file system, FAT12 was introduced in 1977, even before MS-DOS, and was the primary file system for Microsoft operating systems up to MS-DOS 4.0. FAT12 supports drive sizes up to 32MB.

- **FAT16** - The second implementation of FAT was FAT16, introduced in 1988. FAT16 was the primary file system for MS-DOS 4.0 up to Windows 95. FAT16 supports drive sizes up to 2GB.

- **FAT32** - FAT32 is the latest version of the FAT file system. It was introduced in 1996 for Windows 95 OSR2 users and was the primary file system for consumer Windows versions through Windows ME. FAT32 supports drive sizes up to 8TB.

NTFS, an acronym for *New Technology File System*, is a file system first introduced by Microsoft in 1993 with the release of Windows NT 3.1.

NTFS is the primary file system used in Microsoft's Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT operating systems.

The Windows Server line of operating systems also primarily use NTFS.

NTFS File System Features

1. Theoretically, NTFS can support hard drives up to just under 16 EB. Individual file size is capped at just under 256 TB, at least in Windows 8 and Windows 10, as well as in some newer Windows Server versions.
2. NTFS supports disk usage quotas. Disk usage quotas are set by an administrator to restrict the amount of disk space that a user can take up.
3. It's used mainly to control the amount of shared disk space someone can use, usually on a network drive.
4. File attributes previously unseen in Windows operating systems, like the compressed attribute and indexed attribute, are available with NTFS-formatted drives.
5. Encrypting File System (EFS) is another feature supported by NTFS. EFS provides file-level encryption, which means that *individual* files and folders can be encrypted. This is a different feature than *full-disk encryption*, which is the encryption of an entire drive.
6. NTFS is a *journaling* file system, which means it provides a way for system changes to be written to a log, or a journal, before the changes are actually written. This allows the file system to revert to previous, well-working conditions in the event of a failure because the new changes have yet to be committed.
7. Volume Shadow Copy Service (VSS) is an NTFS feature that can be used by online backup service programs and other backup software tools to back up files that are currently being used, as well as by Windows itself to store backups of your files.
8. Another feature introduced in this file system is called *transactional NTFS*. This feature allows software developers to build applications that either completely succeed or completely fail. Programs that take advantage of transactional NTFS don't run the risk of applying a few changes that *do* work as well as a few changes that *don't*, a recipe for serious problems.
9. NTFS includes other features as well, such as *hard links*, *sparse files*, and *reparse points*.

Computer Software Installation Procedure

Installation (or **setup**) of a computer program (including device drivers and plugins), is the act of making the program ready for execution. Because the process varies for each program and each computer, programs (including operating systems) often come with an *installer*, a specialized program responsible for doing whatever is needed for their installation. Installation may be part of a larger software deployment process.

Installation typically involves code being copied/generated from the installation files to new files on the local computer for easier access by the operating system.

Materials Needed:
- Computer
- CD or DVD drive
- Installation disc
- Internet connection
- Web browser

PROCEDURE
Step 1: The first most important step in software installation is to verify that the target system meets the general hardware requirements of the application. Beginning the installation in a computer machine which does not possess the minimum requirements can lead to either an unsuccessful installation or failure of the program to run after installing it.
Step 2: Since programs in general are written to be Operating System dependent, make sure that the version of the application you are installing corresponds to the Operating System platform running on your machine.
Step 3: Aside from the general hardware requirements, some computer programs also have software requirements prior to installation. Double check if you need to update or upgrade your Operating System or if there is a need to download other tools or utilities.
Step 4: Once all the initial requirements have been met, make sure that there are no unnecessary programs running before beginning the installation procedure. In some instances, applications may require that the antivirus programs be disabled. Make sure that you are installing a legitimate application before disabling your protection software.
Step 5: Software installation can be done either from the Internet (skip to step 8) or from an installation disc provided by the software manufacturer. To install from the disc, simply open the CD or DVD drive and insert the installer.
Step 6: A setup wizard window should be launched. In case there is none, open the Explorer and navigate to the optical drive. Double click on either the Autorun or Setup file.
Step 7: Once the wizard is running, simply follow the prompts until the installation process is completed. For novice users, accept the default values to minimize potential problems during the procedure. Jump to step 10.
Step 8: For installation from the Web, launch your browser application and download the setup file to your hard drive.
Step 9: After completion of the downloading process, run the setup program to execute the setup wizard that will handle the automatic installation of the software. Do step 7.
Step 10: After the installation procedure has been completed and the setup wizard has terminated, reboot your machine before launching the newly installed software.

TOPIC 11: TROUBLESHOOTING

Introduction to Computer Fault finding & troubleshooting

Fault finding is the investigation of the cause of malfunction in machinery, especially electronic equipment.

Troubleshooting is a form of problem solving, often applied to repair failed products or processes on a machine or a system.

Fault finding methods and Principles

There are literally hundreds of hardware and software tools that have the ability to help diagnose and solve problems. These tools are somewhat limited unless you can use them in conjunction with sound fault-finding methods.

The scientific method to fault-finding

Fault-finding is a skill required in just about every industry, not just in IT support. If you do a search on the Internet looking for fault-finding information, you are likely to encounter massive amounts of literature for many industries, not just IT. In general, those areas of industry which demands high-level technical skills have developed well-documented fault-finding methods. It is not surprising though that all of these methods have similar principles. Enter the scientific method to fault-finding.

The scientific method is not specific to any technology. The scientific method is an investigative process that uses logic to test theories or hypotheses through observation and methodical experimentation. In fact, the scientific method has been around since the beginning of time, when people began to derive knowledge from the world around them.

The scientific method proposes to use logical and systematic steps (procedures), to analyse available information, such as symptoms, in the hope to find information that is useful and relevant whilst discarding what is not. This procedure will enable you to draw conclusions and hopefully arrive at the source of the problem. Generally, the method is repeated (cyclic), until the source of the problem has been identified.

The **principles** of the scientific method are summarised in the following steps:

1. Gather Information
2. State the Problem
3. Form a hypothesis
4. Test the hypothesis
5. Draw conclusions
6. Repeat when necessary

The next part of this reading will introduce fault-finding techniques, based on the scientific method.

Cyclic fault-finding

Cyclic fault-finding is the preferred method for problem determination used in the IT industry. The myriad of hardware and software tools available for fault finding will help you gather useful information, but generally, the tool won't fix the problem for you. You will need to make your own decisions in terms of what is the best course of action.

Generally, companies develop their own cyclic methods, or choose to adhere to someone else's method i.e. Cisco's Troubleshooting guidelines (see the Cisco website www.cisco.com and search for "troubleshooting"). The most important part of troubleshooting any problem is to divide the tasks of problem resolution into a systematic process of elimination. In general, cyclic fault-finding involves taking a series of steps, varying from 5 to 8 steps, and then repeating these steps until the problem is solved.

It is important to note that cyclic method rely on technicians formulating a hypothesis (probable cause – step 3), and then testing the hypothesis (steps 4 and 5). If the desired outcome if not achieved, the process is repeated (new hypothesis). Take a look at the following steps introduced below:
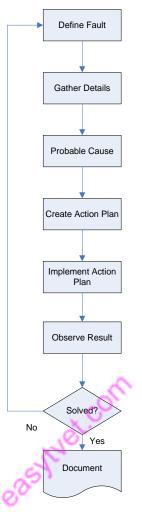
Figure 1: Steps in Cyclic Fault Finding

Strictly speaking, the above process only requires 7 steps for troubleshooting, but best-practice is to update/create appropriate documentation – good quality documentation will only aid fault-finding in the future!

Fault-finding decision trees
Quite often, IT support companies will develop fault analysis trees or fault finding decision trees. Fault finding decision trees are aides for support people to use as guidelines when troubleshooting.
With time, you will be able to create your own decision trees to help the fault-finding process. The following is an example of a decision tree aimed at helping someone troubleshoot a network access fault (i.e. user cannot log in or access her email).
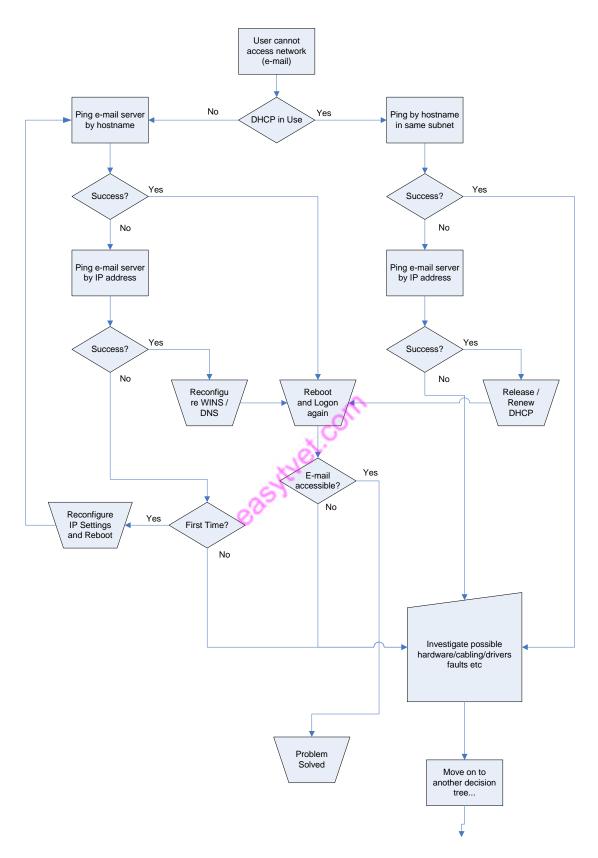
Figure 2: Sample decision tree to help someone troubleshoot a network access fault

The steps in the tree above can be explained as follows:

The tree begins by defining the problem: The user cannot access e-mail. Then a question is asked (diamond shape). Only two answers are possible: Yes or No. Depending on the response a process takes place (rectangular shape), which leads on to another question. No matter how complicated, all decision trees work in the same manner:

1. State Problems (Begin)
2. Ask Questions (Diamond Shape)
3. Analyse Response (Yes or No)
4. Take Action (Rectangular shape)
5. Ask more questions
6. Analyse response
7. Take action
8. And so on until problem is solved or a different course is deemed necessary

It is not unusual for software and hardware manufacturers to include such charts with their products, as additional support information. The general idea is that people may, with the help of these trees, perform first-level support, potentially cutting down on the number of support calls made to companies. Effectively, vendor supplied charts become a form of fault finding tool.

About system problems

Critical problems

Not all problems have the same impact on a business. Some problems have low impact; which means that the problem does not have the potential to disrupt business operations. Some problems have a very high impact; which means that the problem has the potential to stop business operations, incur revenue loss and possibly damage their reputation.
For example, if a part time worker cannot use her computer because the keyboard won't work; this would not be regarded as critical to the business. Surely, it is disruptive to this worker's routine, but it probably won't stop business. If the CEO's (Chief Executive Officer) keyboard stops functioning, this problem is more significant given the stature of this person in the business. The criticality of the latter problem is higher than in the former.

If instead of a problem with a keyboard or even a person's desktop, we find ourselves facing a problem with the file server; the criticality stakes are raised again. This is the time of problem that is likely to bring a business to its knees. Business cannot continue when critical components, software or hardware, go down or become unusable. When critical or indispensable components are struck by problems, this is regarded as the most critical type of fault.

Classifying problems

Faults need to be classified according to their criticality – this is what sort of impact a specific problem may have on business operations. The questions that will need to be answered may include:

- How critical is this problem?

- What is the impact on the overall operations of a business?

- Should the contingency and disaster recovery plan be enacted?

- Does the business have the expertise to deal with the problem and provide a satisfactory solution?

Problems that are regarded as non-critical (low criticality), won't represent a threat to the daily operations of a business. Operations will continue with some level of disruption. This disruption may affect a standalone system, a series of systems or an entire network. An example of a problem regarded as non-critical would be an Internet server going down due to a hardware failure – this is certainly non-routine, but assuming that the business does not use the Internet for their core business operations, business operations may continue, but without Internet access.

Problems that are regarded as critical are certainly serious. These problems have the potential to seriously impair the function of a business. These types of faults will generally require IT personnel to enact a contingency and disaster recovery plan. Business that are not prepared for these types of faults and that have not formulated a sound contingency and disaster recovery strategy will suffer serious consequences, including a total halt of business operations and loss of revenue. An example of this type of fault would be an inaccessible database server holding inventory, ordering and sales data, without which business cannot proceed.

Quite often, IT support managers and supervisors are responsible for assessing the criticality of faults. Many companies have different scales for representing criticality. The following is a suggestion of how this could be implemented:

Table 1: Sample scale for representing criticality of faults

Criticality Level or Risk	Definition	Disaster Recovery
1	High potential impact to large number of users It involves network/system down time	Enact Disaster Recovery Plan
2	High potential impact to large number of users or business critical service. May result in some down time	May require enacting Disaster Recovery Plan
3	Medium potential impact to	Disaster Recovery Plan

	smaller number of users or business service Resolution may require some down time.	enactment not warranted. Remedial action required.
4	Lower potential service or user impact. Change may require some down time.	Disaster Recovery Plan enactment not warranted. Remedial action required.
5	No user or service impact. No down time.	Disaster Recovery Plan enactment not warranted. Remedial action optional.

Computer Hardware & Software Faults

Hardware faults

Apart from faults being classified as critical and non-critical, you will need to use other classifications in order to aid the troubleshooting process. One of the typical classifications of faults is whether the source of the fault is a hardware device or component, or whether the source of the fault is found on software – system or application.

Hardware faults are reasonably easy to troubleshoot, as the symptoms of the fault are fairly obvious. For example, if the power supply unit of a computer fails, the computer will not power up. Sometimes though, hardware faults can be difficult if the fault and symptoms only appear intermittently – that is, the fault is not present all the times. For example, some hardware components only develop faults under certain conditions, such as when the temperature of the device reaches a certain threshold.

Hardware faults sometimes can be rectified fairly quickly, by replacing the failed component. Usually, technicians will have common Field-Replaceable-Units (FRU) available. FRUs are simply common components that can be replaced on the field with reasonable ease. Examples of FRU may include:

- Hard Disk Drives
- Floppy Disk Drives
- Optical Drives (CD, CDR, DVD etc)
- Memory (RAM)
- Sound Cards,
- Video Cards,
- Keyboard & Mouse
- Network Interface Cards
- Network Patch Leads

Software faults

As you might have guessed, software faults are those faults that are caused by a software component. The software component may be part of the system's software or may be applications software.

Software faults sometimes can be tricky to troubleshoot. Even though the source of the problem is found to be software, not always it is crystal clear which software component is actually causing the fault.

System Software Faults – are those faults that are caused by system software. Generally speaking, the operating system is regarded as system software. However, some application software might also install some system components it needs to run, which could become [and quite frequently are] the source of faults. The source of software faults can be caused by:

- Software components corruption

- System incorrect configuration

- Documented and undocumented bugs

- Compatibility issues (hardware and software)

System software faults can have system-wide implications, which might hinder the operations of the whole system.

Application Software Faults – these types of faults are rooted in application software components. Generally, these types of faults only affect the application software in question – the rest of the system operates normally. Similar to system software faults the source of these faults can be tracked down to one or more of the following reasons:

- Software components corruption

- Application incorrect configuration

- Documented and undocumented bugs

- Compatibility issues (hardware and software)

Security-related faults

These faults are faults that develop in systems, and might have their source in hardware, software, configuration or design.

More often than not, security related faults are the consequence of:

- Other faults (for instance, a hardware fault with a firewall device might expose systems that would normally be protected by the firewall device)

- improper configuration,

- un-patched software bugs

- system design flaws

- undiscovered security holes/backdoors

Generally, the occurrence of any of the above issues, will result in security being compromised, possibly exposing confidential and private information. Generally, to rectify this type of fault requires engaging personnel with expertise in the area.

Security faults are sometimes referred to as 'exploits' since, the security fault does not in itself represent a real threat unless someone malicious discovers and chooses to exploit the fault. It is imperative that proactive action be taken to minimise the effect of security compromises.

Boot time faults
Boot time faults are faults that occur during the start-up sequence of a computer system. Boot time faults are critical in that they can potentially halt the boot sequence possibly halting the system altogether, rendering it unusable.
Boot time faults can have their source in software – usually due to improper configuration, missing system files or incompatibilities (usually after new software has been deployed), or hardware – usually due to boot device (typically hard disk drive) failure, or other major component failure such as RAM, Video etc. Failed hardware peripherals might have an impact on booting up, but not necessarily halt the system or make it unbootable.

Computer Fault diagnosis & Tools

1. A message output by a computer <u>diagnosing</u> an error in a computer program, computer system, or component device.
2. A program or subroutine that produces such messages.

Using troubleshooting tools to gather diagnostic information
The fault-finding process is a constant process for gathering data (or feedback) and making decisions based on this data. Hence, it is critical to understand how to use tools to gather data, or access data which may already be available from logs, data trails, databases etc.

Using utilities

There is a range of utilities which produce an output or feedback that are commonly used for troubleshooting purposes. Many fault-finding tools, particularly command-line utilities, do not generally produce exhaustive reports for analyse. Instead they produce a small message to confirm the success [or otherwise] of an action.
For example the ping command simply sends a series of requests to a network destination and reports whether the requests were successful or not. It may report on data such as response-time

(how long it took our request to be answered), but the tool will not produce an exhaustive report. Please analyse the following sample of using the Ping tool from the command line.
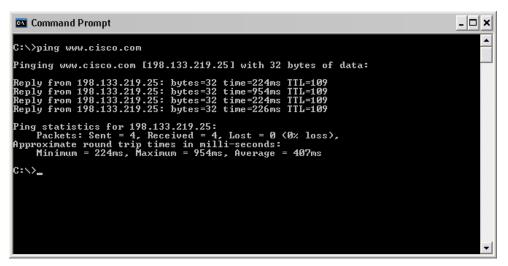

Figure 4: Screen shot of use of Ping tool

The following is another example of a utility that performs a task and generates incidental information, which although not comprehensive, is certainly very useful. The utility presented here is the 'Format' command.

Figure 5: Screen shot of use of Format command

Debug/auditing features

Many computer operating systems and applications feature a 'Debugging' facility. If you are not familiar with debugging, it is a concept borrowed from programmers aimed at getting the systems to produce as much information as possible, in a stepped-through way, with the aim of capturing lots of information which might help get rid of 'bugs' or design/flaws. The concept of

debugging has filtered through many areas of IT and today many systems feature debugging as a standard troubleshooting tool which can be turned on as needed.

Additionally, many network hardware components such as high-end switches and routers, feature debugging. They are able to debug since many managed network devices run an actual operating system. For example, Cisco routers and switches run an operating system called the IOS which, allows full debugging support.

Debugging usually is a fairly intense process which generates lots of information (sometimes more than one can handle!), putting additional processing demands on the systems; therefore, debugging is usually only enabled when troubleshooting is required. Data/Information produced by debugging can either be output to the screen (which means you have to be in front the actual screen), or more commonly redirected to a database system, where data can be stored for later viewing and analysis.

Another feature that can be useful for gathering and collecting useful system information is auditing. Auditing is usually is not turn on by default, because as in with debugging, the amount of information being generated is great; hence, auditing is usually only enabled for specific data gathering requirements - i.e. when a technician is trying to get to the bottom of an elusive fault.

Windows 2000/XP/2003 allow you enable auditing by turning on a policy (usually called a Group Policy Object (GPO). A GPO gives you control of certain aspects of the system which you may audit. The following image is a sample of a GPO in Windows XP.

Figure 6: Screen shot of GPO in Windows XP

The resulting event audit information can be viewed in an event log, accessible via the Windows Event Viewer. See example below.

Figure 7: Screen shot of Windows Event Viewer

Using diagnostic and troubleshooting tools to gather data

Usually diagnostic and troubleshooting tools are particularly effective in generating oodles of information. Most diagnostic tools are capable of generating reports that can be used as a way of documenting the configuration of a system.

Third party tools also can be very useful, especially if they are non-operating system dependant. The Belarc **Adviser** is one such tool that can run on just about any version of windows (generally, you will need a separate tool to audit across platforms i.e. Windows, Linux, and Mac). Belarc Adviser will profile a computer system and output its report as a HTML file, which can be viewed on any web browser, and possibly be uploaded to a central location. This program is available for free for personal use at www.belarc.com.

Summary

This learning pack has introduced you to a variety of faults and problems that you are likely to encounter at some point in your career. You have learnt to gather data, assess the status of a computer system, identify different types of faults, classify them, and choose the most

appropriate course of action and tools. You have also learnt how to document the fault-finding process.

TOPIC 12: COMPUTER USER SUPPORT

Technical support

Technical support (often shortened to **tech support**) refers to a plethora of services by which enterprises provide assistance to users of technology products such as mobile phones, televisions, computers, software products or other informatic, electronic or mechanical goods. In general, technical support services address specific problems with a product or service rather than the provision of training, customization, or other support services.

Most companies offer technical support for the products they sell, either freely available or for a fee. Technical support may be delivered over by e-mail, live support software on a website, or a tool where users can log a call or incident. Larger organizations frequently have internal technical support available to their staff for computer-related problems. The Internet can also be a good source for freely available tech support, where experienced users help users find solutions to their problems. In addition, some fee-based service companies charge for premium technical support services.

Safe computer use (Good working practices)

There are some "good housekeeping" procedures that you should carry out regularly:

- Keep your anti-virus software up to date.
- Keep regular backups of all your important documents.
- Make sure your "In" mailbox doesn't get too large - delete messages or transfer them to other mailboxes.
- If you have web pages, make sure they are up to date and that the hyperlinks still work.
- Do not allow out of date information about students to accumulate on your hard disk: get the latest version of student-related information from the Data Warehouse.

These are guidelines and advice on good working practices, some of which are practical and some legal or standards-based; most are liable to change over time.

Types of User Support offered by IT Services

IT Services does not have the resources to support everything computer-related: you must use the hardware, software and network services supported by us whenever possible.

If you install hardware or software other than that recommended by IT Services on your own equipment you must be prepared to manage and support this yourself.

<u>How IT Support Can Help Your Business?</u>

With more businesses deploying different types of technology to increase productivity, it can become a monumental challenge to stay current with every new IT process that requires support. If you are struggling to keep up with the next generation IT services, the good news is that there are professional IT support services available that can help you relieve the burden of trying to stay on top of every aspect of your IT infrastructure.

It is important to note that the size of your business will be the key factor which determines the type of IT support you require. If you are a small business it is less likely you have a comprehensive IT support staff. For medium to large sized businesses you may have a partial IT support team or a full-fledged department that may be over extended.

To choose the approach that is best for your business it helps to know what options are available to you when it comes to outsourcing IT support. Many quality IT support services will work with you to plan the best approach however, here is an overview of the different types of IT support services to help you get started.

IT Support

While some companies prefer to employ an in-house IT team others find it more cost effective to outsource IT support. This leaves more time for new IT initiatives which support company growth and revenue. Here are some of the ways that you can outsource IT support to a qualified IT support provider:

- **Network Setup and Administration:** If your business has less than 50 employees it is likely you may not have the staff resources to setup a network and oversee network administration on a routine basis. In this case, you can seek the services of a qualified network administration to oversee this important aspect of your business for much less than the cost of employing an IT staff around the clock.
- **Network Security:** Network security can be a significant challenge for any businesses and at the same time it is a necessity in today's business environment. By outsourcing network security tasks to a quality IT provider, you can rest a little easier knowing your network is safe from the latest threats and your network is continually monitored for vulnerabilities. Outsourced IT support for network security also means that your network stays updated with the latest security patches, firewalls, and intrusion detection systems which ensure critical data stays secure.
- **Desktop and End-User Support:** Providing ongoing desktop and end-user support can be a costly but necessary part of maintaining business continuity. Tapping into a professional IT support provider in this area provides an affordable way for you to ensure your employees remain productive with proactive monitoring and managing of your desktop environment.
- **Data Backup and Recovery:** Data backup and recovery can be a costly venture. By using an IT support provider which offers data backup and recovery you can securely backup critical data and obtain access to it in the event disaster strikes. Also, when you use a cloud solution, it is much more cost effective than deploying other offsite methods for protecting data.
- **Email Services:** Most businesses rely heavily on email for daily communications and quality customer service. Around the clock email productivity and protection is a must but the costs of monitoring the architecture can take a big bite out of small business profits. IT support providers which provide email services can help you to manage, monitor, and protect your email systems at a much lower cost than if you deployed the necessary infrastructure in-house.

Requirement for User Support

1. 24/7 technical support improves operational efficiencies by reducing time users spend to fix incidents or problems.

2. Speaking with a certified technical support specialist makes resolving IT issues quick and easy, which can reduce crankiness in the workplace.
3. US based Help Desk support provides immediate response time to support tickets and communication with an actual person (not a recording) the same day.
4. Having a support system in place provides a smooth and easy mechanism for users to receive service while eliminating internal technical service requests, which can reduce downtime for multiple employees.
5. With diverse credentials, training and experience, technical support specialists have resources to fix a wide variety of system errors – not just basic speed bumps.
6. Reports indicate increasing interest in technical certifications in 2015, showing organizations are utilizing Help Desk services more and more to stay competitive.
7. While assisting users, Help Desk engineers practice incident management to help spot problems before they occur, identifying the root cause of frequent recurring incidents.
8. Support specializes have experience working with organizations similar to your business, so they understand your industry vertical, which provides a strategic advantage.
9. Technical specialists not only support users, they recommend tools that make it easier to communicate and collaborate on tasks.
10. Educating the end user provides an overall positive experience and faster resolution.
11. Small businesses outsource Help Desk services through Managed Service agreements so they could focus on their business and have full 24/7 support for their users.
12. Mid-size and large businesses partner with IT companies that offer Help Desk support to provide an additional resource for their IT staff.
13. When you apply the cost per call for the various call flow models for Help Desk services, you can see financial impact. Cost calculations for typical call flow support models indicate 48% more cost effective saving.
14. Help Desk support services can give your business a new way to generate revenue, attract and retain clients and compete in a quickly changing IT environment.

End User Training

Definition: Process of teaching a person to interact and communicate with a computer.

Training is teaching, or developing in oneself or others, any skills and knowledge that relate to specific useful competencies. Training has specific goals of improving one's capability, capacity, productivity and performance.

End user is used to distinguish the person for whom a hardware or software product is designed from the developers, installers, and servicers of the product.

Develop a staff training program

Businesses with a culture of training are seen as quality organizations. Having a 'training champion' in senior management is essential for successfully implementing your training

initiatives. To develop a strong training culture, you must understand the benefits of training. This knowledge will help you make informed decisions, and will support members of staff who will be responsible for managing the training.

Check your legal obligations

As an employer, you have certain obligations in relation to training your staff. You need to ensure that staff are trained to do their jobs safely and, in certain industries, you may be legally obliged to provide staff with specific training.

Assess your staff training needs

To implement the right training for your business, you need to identify your business and employee training needs. You can do this yourself, or you can recruit a human resources (HR) consultant or training organization to help you assess your training needs and advise on training options.

Review your business plan

Your staff training program should be described in your business plan. You need to make sure you know what training your staff need, how much it will cost you and how frequently you will offer it. You should also decide how often you will undertake staff performance reviews.

If you decide to exit your business or hand it over to a family member, training may be an important part of your succession planning. In your business plan, you should:

- assess your business goals and the skills you need to meet them
- work out if you are on track to achieve your goals, and identify any gaps
- think about whether your staff are happy in their jobs, and if your customers are happy with your products and services
- consider how you are doing compared to your competitors
- review any existing training
- Identify areas that need improvement and find out who may benefit from training (e.g. staff may need more knowledge of your products and services or your business processes).

Talk to your staff

Close collaboration and open communication between management and staff on training issues improves working relationships and, in most cases, productivity.

When you are assessing your training needs, you should ask your staff what sort of training they want or need. You can talk to them in one-on-one interviews or in a group meeting.

Engaging your staff in the process will help you make sure the training is suitable and that staff are likely to want to participate. This will help both you and your staff get the most out of training. You may also consider undertaking a staff skills assessment as part of performance planning, to work out what training individual staff members need.

Consider your training options

Once you have reviewed your business plan and discussed training with your staff, you should update your business plan with a new training program. Make sure you consider whether any imminent changes in your business will make training necessary for any of your staff.

Training delivery methods

- Individual hands-on instructor
- Hands-on classroom style instructor-led training
- Seminar style group demonstration
- Computer Based Training (CBT)
- Book-based self-paced training

Record your staff feedback, taking note of any training needs or requests. Work out how each type of training would be delivered, such as on-the-job, internally, or with an external training provider. Include details of all of the courses scheduled and the staff who are participating, as well as the dates, venues and times.

Communicate your training program

Let staff know what training you have booked for them. Communicate the training program to all staff so they are aware of what is happening in your business. Make sure you offer all staff equal opportunities for training and that you are not breaching anti-discrimination laws by excluding any staff. You should also take the opportunity to identify training opportunities during staff performance reviews.

TOPIC 13: ELECTRONIC WASTE MANAGEMENT

Definitions

E-waste is electrical and electronic equipment of any kind that has been discarded. Proper treatment of e-waste helps to prevent environmental degradation and avoids potential threats to human health.
What Is E-Waste?

E-waste is electrical and electronic equipment of any kind that has been discarded. This includes practically anything powered by an electrical source (e.g., from a power socket or a battery). Common types of e-waste include, but are not limited to, the following:-

- Infocomm technology (ICT) equipment, such as desktop, laptop and tablet computers, mobile phones, computer and mobile phone batteries, printers, peripherals and accessories such as keyboards, modems, monitors, computer mice, docking stations, hard disk drives, battery chargers, etc.
- Home appliances, such as TVs, refrigerators, air conditioners, washing machines, rice cookers, microwave and toaster ovens, electric kettles, food processors and blenders, electric fans, DVD/video/music players, radios, hi-fis, vacuum cleaners, etc.
- Other types of e-waste include lamps & lighting, batteries, electronic toys, sports and leisure equipment, etc.

E-waste is mostly made up of metal and plastic components, but also contains small amounts of heavy metals and substances of concern (e.g., in printed circuit boards). The wide variety of e-waste makes it hard to generalise the material content – for example, fridges and air conditioners in particular contain refrigerants to enable cooling to take place, but these refrigerants may also contribute to ozone layer depletion or climate change; the material composition of a mobile phone is very different from that of an electric kettle.

"E-waste" is a popular, informal name for electronic products nearing the end of their "useful life. "E-wastes are considered dangerous, as certain components of some electronic products contain materials that are hazardous, depending on their condition and density. The hazardous content of these materials pose a threat to human health and environment. Discarded computers, televisions, VCRs, stereos, copiers, fax machines, electric lamps, cell phones, audio equipment and batteries if improperly disposed can leach lead and other substances into soil and groundwater. Many of these products can be reused, refurbished, or recycled in an environmentally sound manner so that they are less harmful to the ecosystem. This paper highlights the hazards of e-wastes, the need for its appropriate management and options that can be implemented.

Introduction to E-Waste

Industrial revolution followed by the advances in information technology during the last century has radically changed people's lifestyle. Although this development has helped the human race, mismanagement has led to new problems of contamination and pollution. The technical prowess acquired during the last century has posed a new challenge in the management of wastes. For

example, personal computers (PCs) contain certain components, which are highly toxic, such as chlorinated and brominated substances, toxic gases, toxic metals, biologically active materials, acids, plastics and plastic additives. The hazardous content of these materials pose an environmental and health threat. Thus proper management is necessary while disposing or recycling ewastes.

These days computer has become most common and widely used gadget in all kinds of activities ranging from schools, residences, offices to manufacturing industries. E-toxic components in computers could be summarized as circuit boards containing heavy metals like lead & cadmium; batteries containing cadmium; cathode ray tubes with lead oxide & barium; brominated flame-retardants used on printed circuit boards, cables and plastic casing; poly vinyl chloride (PVC) coated copper cables and plastic computer casings that release highly toxic dioxins & furans when burnt to recover valuable metals; mercury switches; mercury in flat screens; poly chlorinated biphenyl's (PCB's) present in older capacitors; transformers; etc. Basel Action Network (BAN) estimates that the 500 million computers in the world contain 2.87 billion kgs of plastics, 716.7 million kgs of lead and 286,700 kgs of mercury. The average 14-inch monitor uses a tube that contains an estimated 2.5 to 4 kgs of lead. The lead can seep into the ground water from landfills thereby contaminating it. If the tube is crushed and burned, it emits toxic fumes into the air.

Effects on Environment & Human Health

Disposal of e-wastes is a particular problem faced in many regions across the globe. Computer wastes that are landfilled produces contaminated leachates which eventually pollute the groundwater. Acids and sludge obtained from melting computer chips, if disposed on the ground causes acidification of soil. For example, Guiyu, Hong Kong a thriving area of illegal e-waste recycling is facing acute water shortages due to the contamination of water resources.

This is due to disposal of recycling wastes such as acids, sludges etc. in rivers. Now water is being transported from faraway towns to cater to the demands of the population. Incineration of e-wastes can emit toxic fumes and gases, thereby polluting the surrounding air. Improperly monitored landfills can cause environmental hazards. Mercury will leach when certain electronic devices, such as circuit breakers are destroyed. The same is true for polychlorinated biphenyls (PCBs) from condensers. When brominated flame retardant plastic or cadmium containing plastics are landfilled, both polybrominated dlphenyl ethers (PBDE) and cadmium may leach into the soil and groundwater. It has been found that significant amounts of lead ion are dissolved from broken lead containing glass, such as the cone glass of cathode ray tubes, gets mixed with acid waters and are a common occurrence in landfills.

Not only does the leaching of mercury poses specific problems, the vaporization of metallic mercury and dimethylene mercury, both part of Waste Electrical and Electronic Equipment (WEEE) is also of concern. In addition, uncontrolled fires may arise at landfills and this could be a frequent occurrence in many countries. When exposed to fire, metals and other chemical substances, such as the extremely toxic dioxins and furans (TCDD tetrachloro dibenzo-dioxin, PCDDs-polychlorinated dibenzodioxins. PBDDs-polybrominated dibenzo-dioxin and PCDFs-poly chlorinated dibenzo furans) from halogenated flame retardant products and PCB containing condensers can be emitted. The most dangerous form of burning e-waste is the open-air burning

of plastics in order to recover copper and other metals. The toxic fall-out from open air burning affects both the local environment and broader global air currents, depositing highly toxic byproducts in many places throughout the world.

Table: Effects of E-Waste constituent on health - summarizes the health effects of certain constituents in e-wastes. If these electronic items are discarded with other household garbage, the toxics pose a threat to both health and vital components of the ecosystem. In view of the ill-effects of hazardous wastes to both environment and health, several countries exhorted the need for a global agreement to address the problems and challenges posed by hazardous waste. Also, in the late 1980s, a tightening of environmental regulations in industrialized countries led to a dramatic rise in the cost of hazardous waste disposal. Searching for cheaper ways to get rid of the wastes, "toxic traders" began shipping hazardous waste to developing countries. International outrage following these irresponsible activities led to the drafting and adoption of strategic plans and regulations at the Basel Convention. The Convention secretariat, in Geneva, Switzerland, facilitates and implementation of the Convention and related agreements. It also provides assistance and guidelines on legal and technical issues, gathers statistical data, and conducts training on the proper management of hazardous waste.

BASEL CONVENTION

The fundamental aims of the Basel Convention are the control and reduction of transboundary movements of hazardous and other wastes including the prevention and minimization of their generation, the environmentally sound management of such wastes and the active promotion of the transfer and use of technologies.

A Draft Strategic Plan has been proposed for the implementation of the Basel Convention. The Draft Strategic Plan takes into account existing regional plans, programmes or strategies, the decisions of the Conference of the Parties and its subsidiary bodies, ongoing project activities and process of international environmental governance and sustainable development. The Draft requires action at all levels of society: training, information, communication, methodological tools, capacity building with financial support, transfer of know-how, knowledge and sound, proven cleaner technologies and processes to assist in the concrete implementation of the Basel Declaration. It also calls for the effective involvement and coordination by all concerned stakeholders as essential for achieving the aims of the Basel Declaration within the approach of common but differentiated responsibility.

Table : Effects of E-Waste constituent on health

Source of e-wastes	Constituent	Health effects
Solder in printed circuit boards, glass panels and gaskets in computer monitors	Lead (PB)	• Damage to central and peripheral nervous systems, blood systems and kidney damage. • Affects brain development of children.
Chip resistors and semiconductors	Cadmium (CD)	• Toxic irreversible effects on human health. • Accumulates in kidney and liver.

		• Causes neural damage. • Teratogenic.
Relays and switches, printed circuit boards	Mercury (Hg)	• Chronic damage to the brain. • Respiratory and skin disorders due to bioaccumulation in fishes.
Corrosion protection of untreated and galvanized steel plates, decorator or hardner for steel housings	Hexavalent chromium (Cr) VI	• Asthmatic bronchitis. • DNA damage.
Cabling and computer housing	Plastics including PVC	Burning produces dioxin. It causes • Reproductive and developmental problems; • Immune system damage; • Interfere with regulatory hormones
Plastic housing of electronic equipments and circuit boards.	Brominated flame retardants (BFR)	• Disrupts endocrine system functions
Front panel of CRTs	Barium (Ba)	Short term exposure causes: • Muscle weakness; • Damage to heart, liver and spleen.
Motherboard	Beryllium (Be)	• Carcinogenic (lung cancer) • Inhalation of fumes and dust. Causes chronic beryllium disease or beryllicosis. • Skin diseases such as warts.

A set. of interrelated and mutually supportive strategies are proposed to support the concrete implementation of the activities as indicated in the website (www.basel.int/DraftstrateKJcpian4Seot.pdf) is described below:

1. To involve experts in designing communication tools for creating awareness at the highest level to promote the aims of the Basel Declaration on environmentally sound management and the ratification and implementation of the Basel Convention, its amendments and protocol with the emphasis on the short-term activities.
2. To engage and stimulate a group of interested parties to assist the secretariat in exploring fund raising strategies including the preparation of projects and in making full use of expertise in non-governmental organizations and other institutions in joint projects.
3. To motivate selective partners among various stakeholders to bring added value to making progress in the short-term.

4. To disseminate and make information easily accessible through the internet and other electronic and printed materials on the transfer of know-how, in particular through Basel Convention Regional Centers (BCRCs).
5. To undertake periodic review of activities in relation to the agreed indicators;
6. To collaborate with existing institutions and programmes to promote better use of cleaner technology and its transfer, methodology, economic instruments or policy to facilitate or support capacity-building for the environmentally sound management of hazardous and other wastes.

The Basel Convention brought about a respite to the transboundary movement of hazardous waste. India and other countries have ratified the convention. However United States (US) is not a party to the ban and is responsible for disposing hazardous waste, such as, e-waste to Asian countries even today. Developed countries such as US should enforce stricter legislations in their own country for the prevention of this horrifying act.

In the European Union where the annual quantity of electronic waste is likely to double in the next 12 years, the European Parliament recently passed legislation that will require manufacturers to take back their electronic products when consumers discard them. This is called Extended Producer Responsibility. It also mandates a timetable for phasing out most toxic substances in electronic products.

Management of E-Wastes

It is estimated that 75% of electronic items are stored due to uncertainty of how to manage it. These electronic junks lie unattended in houses, offices, warehouses etc. and normally mixed with household wastes, which are finally disposed off at landfills. This necessitates implementable management measures.

In industries management of e-waste should begin at the point of generation. This can be done by waste minimization techniques and by sustainable product design. Waste minimization in industries involves adopting:

- inventory management,
- production-process modification,
- volume reduction,
- recovery and reuse.

Inventory management
Proper control over the materials used in the manufacturing process is an important way to reduce waste generation (Freeman, 1989). By reducing both the quantity of hazardous materials used in the process and the amount of excess raw materials in stock, the quantity of waste generated can be reduced. This can be done in two ways i.e. establishing material-purchase review and control procedures and inventory tracking system.

Developing review procedures for all material purchased is the first step in establishing an inventory management program. Procedures should require that all materials be approved prior

to purchase. In the approval process all production materials are evaluated to examine if they contain hazardous constituents and whether alternative non-hazardous materials are available.

Another inventory management procedure for waste reduction is to ensure that only the needed quantity of a material is ordered. This will require the establishment of a strict inventory tracking system. Purchase procedures must be implemented which ensure that materials are ordered only on an as-needed basis and that only the amount needed for a specific period of time is ordered.

Production-process modification
Changes can be made in the production process, which will reduce waste generation. This reduction can be accomplished by changing the materials used to make the product or by the more efficient use of input materials in the production process or both. Potential waste minimization techniques can be broken down into three categories:

i) Improved operating and maintenance procedures,

ii) Material change and

iii) Process-equipment modification.

Improvements in the operation and maintenance of process equipment can result in significant waste reduction. This can be accomplished by reviewing current operational procedures or lack of procedures and examination of the production process for ways to improve its efficiency. Instituting standard operation procedures can optimise the use of raw materials in the production process and reduce the potential for materials to be lost through leaks and spills. A strict maintenance program, which stresses corrective maintenance, can reduce waste generation caused by equipment failure. An employee-training program is a key element of any waste reduction program. Training should include correct operating and handling procedures, proper equipment use, recommended maintenance and inspection schedules, correct process control specifications and proper management of waste materials.

Hazardous materials used in either a product formulation or a production process may be replaced with a less hazardous or non-hazardous material. This is a very widely used technique and is applicable to most manufacturing processes. Implementation of this waste reduction technique may require only some minor process adjustments or it may require extensive new process equipment. For example, a circuit board manufacturer can replace solvent-based product with water-based flux and simultaneously replace solventvapor degreaser with detergent parts washer.

Installing more efficient process equipment or modifying existing equipment to take advantage of better production techniques can significantly reduce waste generation. New or updated equipment can use process materials more efficiently producing less waste. Additionally such efficiency reduces the number of rejected or off-specification products, thereby reducing the amount of material which has to be reworked or disposed of. Modifying existing process equipment can be a very cost-effective method of reducing waste generation. In many cases the modification can just be relatively simple changes in the way the materials are handled within

the process to ensure that they are not wasted. For example, in many electronic manufacturing operations, which involve coating a product, such as electroplating or painting, chemicals are used to strip off coating from rejected products so that they can be recoated. These chemicals, which can include acids, caustics, cyanides etc are often a hazardous waste and must be properly managed. By reducing the number of parts that have to be reworked, the quantity of waste can be significantly reduced.

Volume reduction

Volume reduction includes those techniques that remove the hazardous portion of a waste from a non-hazardous portion. These techniques are usually to reduce the volume, and thus the cost of disposing of a waste material. The techniques that can be used to reduce waste-stream volume can be divided into 2 general categories: source segregation and waste concentration. Segregation of wastes is in many cases a simple and economical technique for waste reduction. Wastes containing different types of metals can be treated separately so that the metal value in the sludge can be recovered. Concentration of a waste stream may increase the likelihood that the material can be recycled or reused. Methods include gravity and vacuum filtration, ultra filtration, reverse osmosis, freeze vaporization etc.

For example, an electronic component manufacturer can use compaction equipments to reduce volume of waste cathode ray-tube.

Recovery and reuse

This technique could eliminate waste disposal costs, reduce raw material costs and provide income from a salable waste. Waste can be recovered on-site, or at an off-site recovery facility, or through inter industry exchange. A number of physical and chemical techniques are available to reclaim a waste material such as reverse osmosis, electrolysis, condensation, electrolytic recovery, filtration, centrifugation etc. For example, a printed-circuit board manufacturer can use electrolytic recovery to reclaim metals from copper and tin-lead plating bath.

However recycling of hazardous products has little environmental benefit if it simply moves the hazards into secondary products that eventually have to be disposed of. Unless the goal is to redesign the product to use nonhazardous materials, such recycling is a false solution.

Sustainable product design

Minimization of hazardous wastes should be at product design stage itself keeping in mind the following factors*

- *Rethink the product design:* Efforts should be made to design a product with fewer amounts of hazardous materials. For example, the efforts to reduce material use are reflected in some new computer designs that are flatter, lighter and more integrated. Other companies propose centralized networks similar to the telephone system.
- *Use of renewable materials and energy:* Bio-based plastics are plastics made with plant-based chemicals or plant-produced polymers rather than from petrochemicals. Bio-based toners, glues and inks are used more frequently. Solar computers also exist but they are currently very expensive.

- ***Use of non-renewable materials that are safer:*** Because many of the materials used are non-renewable, designers could ensure the product is built for re-use, repair and/or upgradeability. Some computer manufacturers such as Dell and Gateway lease out their products thereby ensuring they get them back to further upgrade and lease out again.

MANAGEMENT OPTIONS

Considering the severity of the problem, it is imperative that certain management options be adopted to handle the bulk e-wastes. Following are some of the management options suggested for the government, industries and the public.

Responsibilities of the Government

(i) Governments should set up regulatory agencies in each district, which are vested with the responsibility of co-ordinating and consolidating the regulatory functions of the various government authorities regarding hazardous substances.

(ii) Governments should be responsible for providing an adequate system of laws, controls and administrative procedures for hazardous waste management (Third World Network. 1991). Existing laws concerning e-waste disposal be reviewed and revamped. A comprehensive law that provides e-waste regulation and management and proper disposal of hazardous wastes is required. Such a law should empower the agency to control, supervise and regulate the relevant activities of government departments.

Under this law, the agency concerned should

  o Collect basic information on the materials from manufacturers, processors and importers and to maintain an inventory of these materials. The information should include toxicity and potential harmful effects.
  o Identify potentially harmful substances and require the industry to test them for adverse health and environmental effects.
  o Control risks from manufacture, processing, distribution, use and disposal of electronic wastes.
  o Encourage beneficial reuse of "e-waste" and encouraging business activities that use waste". Set up programs so as to promote recycling among citizens and businesses.
  o Educate e-waste generators on reuse/recycling options

(iii) Governments must encourage research into the development and standard of hazardous waste management, environmental monitoring and the regulation of hazardous waste-disposal.

(iv) Governments should enforce strict regulations against dumping e-waste in the country by outsiders. Where the laws are flouted, stringent penalties must be imposed. In particular, custodial sentences should be preferred to paltry fines, which these outsiders / foreign nationals can pay.

(v) Governments should enforce strict regulations and heavy fines levied on industries, which do not practice waste prevention and recovery in the production facilities.

(vi) Polluter pays principle and extended producer responsibility should be adopted.

(vii) Governments should encourage and support NGOs and other organizations to involve actively in solving the nation's e-waste problems.

(viii) Uncontrolled dumping is an unsatisfactory method for disposal of hazardous waste and should be phased out.

(viii) Governments should explore opportunities to partner with manufacturers and retailers to provide recycling services.

Responsibility and Role of industries

1. Generators of wastes should take responsibility to determine the output characteristics of wastes and if hazardous, should provide management options.

2. All personnel involved in handling e-waste in industries including those at the policy, management, control and operational levels, should be properly qualified and trained. Companies can adopt their own policies while handling
e-wastes. Some are given below:

- Use label materials to assist in recycling (particularly plastics).
- Standardize components for easy disassembly.
- Re-evaluate 'cheap products' use, make product cycle 'cheap' and so that it has no inherent value that would encourage a recycling infrastructure.
- Create computer components and peripherals of biodegradable materials.
- Utilize technology sharing particularly for manufacturing and de manufacturing.
- Encourage / promote / require green procurement for corporate buyers.
- Look at green packaging options.

3. Companies can and should adopt waste minimization techniques, which will make a significant reduction in the quantity of e-waste generated and thereby lessening the impact on the environment. It is a "reverse production" system that designs infrastructure to recover and reuse every material contained within e-wastes metals such as lead, copper, aluminum and gold, and various plastics, glass and wire. Such a "closed loop" manufacturing and recovery system offers a win-win situation for everyone, less of the Earth will be mined for raw materials, and groundwater will be protected, researchers explain.

4. Manufacturers, distributors, and retailers should undertake the responsibility of recycling/disposal of their own products.

5. Manufacturers of computer monitors, television sets and other electronic devices containing hazardous materials must be responsible for educating consumers and the general public regarding the potential threat to public health and the environment posed by their products. At minimum, all computer monitors, television sets and other electronic devices containing hazardous materials must be clearly labeled to identify environmental hazards and proper materials management.

Responsibilities of the Citizen

Waste prevention is perhaps more preferred to any other waste management option including recycling. Donating electronics for reuse extends the lives of valuable products and keeps them out of the waste management system for a longer time. But care should be taken while donating such items i.e. the items should be in working condition.

Reuse, in addition to being an environmentally preferable alternative, also benefits society. By donating used electronics, schools, non-profit organizations, and lower-income families can afford to use equipment that they otherwise could not afford.

E-wastes should never be disposed with garbage and other household wastes. This should be segregated at the site and sold or donated to various organizations.

While buying electronic products opt for those that:

- are made with fewer toxic constituents
- use recycled content
- are energy efficient
- are designed for easy upgrading or disassembly
- utilize minimal packaging
- offer leasing or take back options
- have been certified by regulatory authorities. Customers should opt for upgrading their computers or other electronic items to the latest versions rather than buying new equipments.

NGOs should adopt a participatory approach in management of e-wastes.

TOPIC 14: EMERGING TRENDS IN COMPUTER MAINTENANCE AND SUPPORT

Technology trends that are altering hardware maintenance requirements

IT managers are facing many new challenges as emerging technologies push them to set aside long-held strategies and operations in favor of new ways to get the job done. This is happening in a variety of IT segments, and the movement toward new methodologies is particularly clear in the hardware maintenance industry. IT managers increasingly find themselves in a fiscal or operational climate where traditional OEM extended warranty models are unable to work as a viable option, making third-party hardware maintenance plans a necessary part of operations.

Taking advantage of a dedicated maintenance and support partnership can help IT managers keep pace with a variety of technological trends, but three really stand out:

1. Cloud computing

The cloud is enabling IT teams to move hardware out of the internal data center and reduce their day-to-day management burden. The end result is a situation in which fiscal plans are also changed, with many companies putting more funds into the cloud and less to the internal data center. This presents major problems for IT managers because many of the data sets and applications that cannot be moved to the cloud exist on legacy hardware. The issue occurs, in most cases, for one of two reasons – the legacy applications are critical, but they won't translate into a virtual environment, or the storage systems offer unique functionality, such as built-in redundancy, that make them too valuable to replace with cloud solutions.

The end result is a situation in which IT managers still have plenty of legacy hardware to support, but less money to put into maintenance plans. Third-party hardware maintenance vendors can offer services for much lower costs than the OEMs, relieving IT leaders of the fiscal challenges that come with managing legacy systems in a cloudified IT world.

2. Big data

The big data analytics movement is emerging as a key trend across a diverse range of business sectors. For IT managers, this often means finding ways to resolve major storage challenges. Central to this issue is a need to balance high-performance systems for active data and high-capacity arrays for archived information. Many businesses lack the fiscal resources to pour into new systems in both of these areas, but big data requirements make it extremely difficult to skimp on either. One solution is to use legacy storage systems to support archiving and purchase new arrays to meet ongoing performance needs.

This option can reduce the costs of big data plans without forcing organizations to make sacrifices in terms of quality. In such a setup, hardware maintenance partnerships can prove invaluable to ensuring reliability for the legacy systems used to archive data.

3. Green IT

Sustainability is moving from being a secondary, or even tertiary, concern for IT leaders to a primary issue. The reality is that power and electronics waste issues are growing exponentially as technology demands rise. Green IT strategies are becoming a priority with this problem facing companies in just about every sector. Dealing with waste is a particularly challenging issue because computer, server, storage and network components can feature a combination of hazardous chemicals, materials that require special disposal methods and precious metals that need to be recycled.

A third-party hardware maintenance plan can enable IT managers to deal with waste more effectively through supplementary services that support equipment disposal. This is particularly valuable for storage systems because companies must not only consider environmental factors when casting aside solutions, they must also enact data protection strategies to ensure information is inaccessible when hard disks are thrown away. Many hardware maintenance providers offer specialized services in this area, making them a valuable asset for sustainability-minded IT leaders.

The Alignment of Technology and Corporate Planning

In the digital age, information technology plays an important role in the success of an organization. Technology provides edge in this globalized world. Companies are facing competition not only from local companies but from international companies as well.

In such a scenario, it is important that company invest in technology which is aligned with overall strategy of the company. This calls for technology strategy formulation.

Technology Strategy Formulation

Technology strategy formulation talks about alignment between technology strategy and the overall strategy of the organization. Here the role of the Chief Information Officer comes into prominence. The CIO should have short term as well as long term vision of technology advancement. CIO should bridge implication of technology advancement and organization strategy. A clear communication of technology impact on organization needs to reach executive leadership.

This alignment between CIO and CEO revolves around issues like:

- CIO roles and involvement in overall strategy formulation of organization.
- Financial resources available to make investment in technology.
- Earlier results of alignment between technology and organization strategy.
- External business conditions.

CIO faces challenge to provide technology value adds for organization in achieving its objective.

Planning

Corporate planning plays an important role in alignment of technology with organization strategy. In a perfect scenario CIO and CEO will have a same planning horizon. However, it is observed that the CEO and CIO do not share same vision, from planning to execution.

This introduces the concept of planning lead time. In some organization, strategy execution does not match to technology planning horizon and execution. By the time technology strategy is executed, more advancement is observed in that system, thus competitive edge is lost.

In the above scenario, companies become reactive rather than pro-active. Companies need to adjust with challenges posed by market leaders and trend setters. A strong CIO-CEO relationship ensure organization develop understanding of technological challenges and its impact on overall organization.

Organizational Structure

Organization needs to ensure that their structure is agile and flexible as to accommodate changes in the technology. They should be efficient and effective enough to deal demands of the market change.

Organization needs to develop and maintain technology systems, which are flexible and adaptive. There are three types of technology infrastructure available with companies' ERP, data warehousing and knowledge management.

All three dimensions ERP, Data Warehousing and Knowledge Management provide cutting edge to the organization.

Organizational Systems

Organization invests in technology looking at its present needs; future requirements and its capability to provide a competitive edge. Systems can be classified into three categories depending upon technology timeline, new systems, matured systems and declining systems.

New systems have latest technology and provide a competitive edge. As time progresses system and technology are adopted by more companies, thus losing competitive edge. Finally, systems and technology reach the obsolete stage where its usage has declined and is to be phased out.

Executive leadership of organizations is responsible to manage new systems range as to enjoy competitive edge. However, this requires substantial investment and clear vision of future technology state. Therefore, organization has to walk a tight rope in investment in new technology and phasing out the obsolete.