UNIT-II

Assembly of Computer, Diagnostic and Troubleshooting of PC

- **POST (Power on Self Test) :-**

A power-on self-test (POST) is a set of routines performed by firmware or software immediately after a computer is powered on, to determine if the hardware is working as expected.

The process would proceed further only if the required hardware is working correctly, else the BIOS(Basic Input Output Software) would issue an error message.

POST sequence is executed irrespective of the Operating System and is handled by the system BIOS.

Once the tests are passed the POST would generally notify the OS with beeps while the number of beeps can vary from system to system. W

hen POST is successfully finalized, bootstrapping is enabled. Bootstrapping starts the initialization of the OS.

The Role of POST in the Boot Sequence

The boot sequence is the process of starting a computer/system. The boot process is initiated when the power button is pressed, it sends power to the boot-loader in the cache memory. The Boot loader performs POST as a preboot sequence and if everything is working well without any errors the BIOS(Basic Input Output System) is activated which finds and loads the operating system.

Finally the software has to interact with the hardware units to complete the process. To avoid any hardware errors while executing a software program, the pre-boot sequence would test the hardware and initiate the OS if and only if the basic hardware units are functioning as expected. Principal duties of the main BIOS during POST are as follows:

1. Find, size, and verify the system main memory.
2. Initialize BIOS.
3. Identify, organize, and select which devices are available for booting.
4. Verify CPU registers.
5. Verify the integrity of the BIOS code itself.
6. Verify some basic components like DMA, timer, and interrupt controller.
7. Pass control to other specialized extensions BIOS (if installed).

The checks are performed majorly on:

- Hardware elements like processor, storage devices and memory.
- Basic System Devices like keyboard, and other peripheral devices.
- CPU Registers
- DMA (Direct Memory Access)
- Timer
- Interrupt controller

- **Identifying problems by Beep codes errors:-**

1 Beep - Refresh Failure

Reseat/replace memory, troubleshoot motherboard.

2 Beeps - Parity Error

Reseat/replace memory, troubleshoot motherboard.

3 Beeps - Memory Error (first 64KB)

Reseat/replace memory.

4 Beeps - Timer Failure

Troubleshoot motherboard.

5 Beeps - Processor Failure

Troubleshoot CPU, motherboard.

6 Beeps - Keyboard Controller Failure

Troubleshoot keyboard, motherboard.

7 Beeps - Virtual Mode Exception Error

Troubleshoot CPU, motherboard.

8 Beeps - Display Memory Failure

Troubleshoot graphics card, motherboard.

9 Beeps - ROM BIOS Checksum Failure

Replace ROM BIOS, troubleshoot motherboard.

10 Beeps - CMOS Shutdown Register Failure

Troubleshoot motherboard.

11 Beeps - L2 Cache Failure

Troubleshoot L2 cache, motherboard.

Continuous Beeps - Memory or Video Failure

Troubleshoot memory, graphics card, and motherboard.

- ## Checking power supply using Multi-meter:-

A properly executed PSU test using a multimeter should confirm whether the power supply is in good working order or should be replaced.

1. Before you begin, read these important PC repair safety tips because of the dangers involved with the process. Manually testing a power supply involves working closely with high voltage electricity.
2. Open your computer's case. In short, this involves turning off the computer, removing the power cable, and unplugging anything else connected to the outside of your computer.
3. Unplug the power connectors from *each and every internal device*.
4. Group all the power cables and connectors together for easy testing.
5. Short out pins 15 and 16 on the 24-pin motherboard power connector with a small piece of wire.
6. Confirm that the power supply voltage switch is properly set for your country.
7. Plug the PSU into a live outlet and flip the switch on the back of the power supply.
8. Turn on your multimeter and turn the dial to the VDC (Volts DC) setting.
9. Test the 24-pin motherboard power connector:

   Connect the negative probe on the multimeter (black) to *any* ground wired pin, and connect the positive probe (red) to the first power line you want to test. The 24-pin main power connector has +3.3 VDC, +5 VDC, -5 VDC (optional), +12 VDC, and -12 VDC lines across multiple pins.

10. Document the number that the multimeter shows for each voltage tested and confirm that the reported voltage is within approved tolerance.
11. Turn off the switch on the back of the power supply and unplug it from the wall.
12. Reconnect all your internal devices to power.
13. Plug in your power supply, flip the switch on the back if you have one, and then turn on your computer as you normally do with the PC's power switch.

- ## Replacement of components:-

1. Prepare your workspace

Before you open your computer case, you need to make sure you have a clean, well-lit, and static-free workspace. You will also need some tools, such as a screwdriver, an anti-static wrist strap, and a soft cloth. Turn off your computer and unplug it from the power source.

2. Ground yourself

One of the biggest risks when working with hardware components is static electricity, which can fry your circuits or damage your devices. To prevent this, you need to ground yourself before touching any component. You can do this by wearing an anti-static wrist strap and attaching it to a metal part of the computer case or a grounded object.

3. Open the computer case

To access the hardware components, you need to open the computer case. This may vary depending on the type and model of your computer, but usually you will need to remove some screws or clips that hold the case together.

4. **Install or replace the component**

Depending on the component you are working with, you may need to follow different steps to install or replace it.

5. **Close the computer case**

After you have installed or replaced the component, you need to close the computer case and reconnect everything. Make sure you have not left any tools, screws, or cables inside the case. Replace the screws or clips that hold the case together and tighten them securely. Reconnect the power cord and any peripherals you disconnected. Turn on your computer and check if the component is working properly.

6. **Troubleshoot any issues**

If you encounter any issues with your new or replaced component, such as error messages, poor performance, or compatibility problems, you may need to troubleshoot them.

- ## CMOS:-

a) The full form of CMOS is **Complementary Metal-Oxide-Semiconductor.** CMOS is an integrated circuit built on a printed circuit board. It is a battery-powered memory chip that effortlessly holds the initialisation data. The BIOS uses this data to turn on the device, i.e., during the bootup process.

b) The complementary word refers to the user charge, that is, either PMOS (positive MOS) or NMOS (negative MOS). CMOS utilises one charge at a time.

c) CMOS consumes less power since charges can remain for a prolonged period of time in one phase and, therefore, only consume energy whenever necessary.

d) Transistors focused on CMOS do not heat up and yield a high speed.

Applications of CMOS

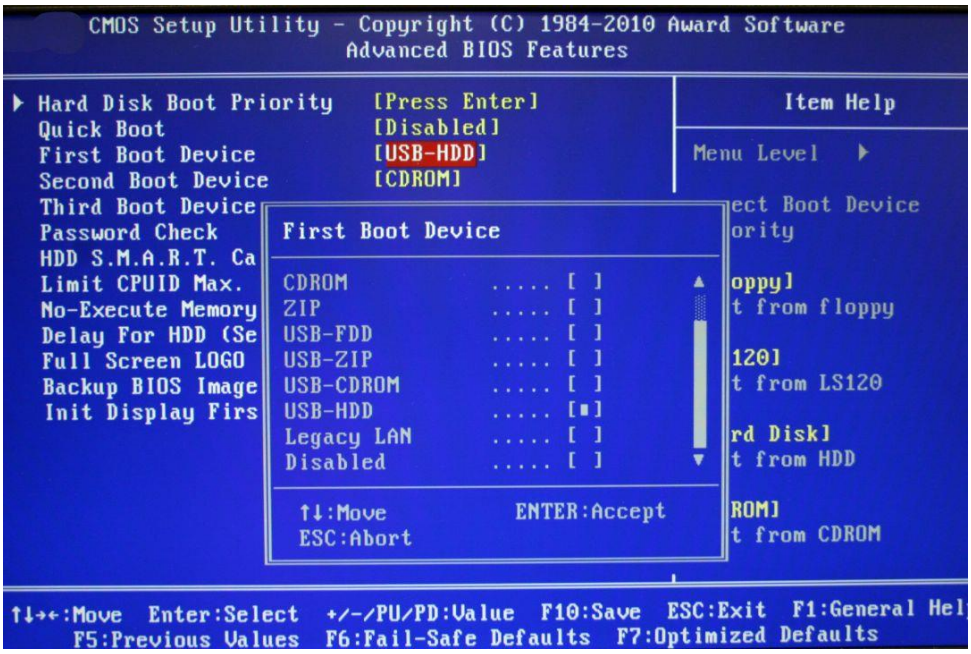
1. Microcontrollers
2. Static RAM
3. Microprocessor
4. Digital logic circuits
5. Image sensor

- ## Study of BIOS Set-up- Advance set-up

The BIOS contains a setup program used to configure settings for hardware devices. The configuration data is saved to a special memory chip called a complementary metal-oxide semiconductor (CMOS). CMOS is maintained by the battery in the computer. If this battery dies, all BIOS setup configuration data is lost. If this occurs, replace the battery and reconfigure the BIOS settings.

To enter the BIOS setup program, you must press the proper key or key sequence during POST. Most computers use the Delete key. Your computer may use another key or combination of keys, as specified during the boot process.

Figure shows an example of a BIOS setup program. Figure , BIOS Setup Screen Shot



Here are some common BIOS setup menu options:

■ Main: System time, date, HDD type, and so on

■ Advanced: Infrared port settings, parallel port settings, and so on

■ Security: Password settings for the setup utility

■ Others: Low-battery alarm, system beep, and so on

■ Boot: The computer's boot order

■ Exit: Exits the setup utility.

- ## Boot configuration

The boot configuration expands the current kernel command line to support additional key-value data when booting the kernel in an efficient way. This allows administrators to pass a structured-Key config file.

Config File Syntax

The boot config syntax is a simple structured key-value. Each key consists of dot-connected-words, and key and value are connected by =. The value has to be terminated by semi-colon (;) or newline (\n). For array value, array entries are separated by comma (,).

```
KEY[.WORD[...]] = VALUE[, VALUE2[...]][;]
```

Unlike the kernel command line syntax, spaces are OK around the comma and =.

Each key word must contain only alphabets, numbers, dash (-) or underscore (_). And each value only contains printable characters or spaces except for delimiters such as semi-colon (;), new-line (\n), comma (,), hash (#) and closing brace (}).

If you want to use those delimiters in a value, you can use either double- quotes ("VALUE") or single-quotes ('VALUE') to quote it. Note that you can not escape these quotes.

There can be a key which doesn't have value or has an empty value. Those keys are used for checking if the key exists or not (like a boolean).

- ## Boot Menu :-

The **Boot Menu** is a menu accessible when a computer is first starting up. It can contain many different device options to boot to, including CD (compact disc), DVD (digital versatile disc), flash drive, or hard drives, and a LAN (local area network). The Boot Menu allows a user to load up other operating systems or applications, even if the computer already has an operating system. A Boot Menu is also useful for installing a new operating system on a computer because the user can choose what device to use.

How to enter the Boot Menu

When a computer is starting up, the user can access the Boot Menu by pressing one of several keyboard keys. Common keys for accessing the Boot Menu are Esc, F2, F10, or F12, depending on the computer or motherboard manufacturer. The key to press is usually specified on the computer's startup screen. The Boot Menu allows users to select what device to load an operating system or application from as the computer is booting.

If desired, the order of the devices listed in the Boot Menu, also called the boot sequence, can be changed.

To navigate the boot menu, use your up and down arrow keys to move between the available options and then when your option is highlighted press Enter. If the arrow keys don't work, enter the number of the option you want to choose.

Here are some common BIOS setup menu options:

■ Main: System time, date, HDD type, and so on

■ Advanced: Infrared port settings, parallel port settings, and so on

■ Security: Password settings for the setup utility

■ Others: Low-battery alarm, system beep, and so on

■ Boot: The computer's boot order

■ Exit: Exits the setup utility.

- ## Test Sequences:-

Define Test Sequences

A test sequence consists of test steps arranged in a hierarchy. Test steps can contain transitions that define how a test progresses in response to the simulation. Test steps can also have a When decomposition that uses logic similar to an if-elseif-else statement. By default:

- New Test Sequence blocks contain two standard transition test steps.
- New Test Assessment blocks contain a When decomposition test step with two sub-steps.

- ## Error Messages:-

The following error messages are commonly seen by modern computer users

- **Access denied**
  This error occurs if the user does not have privileges to a file, or if it has been locked by some program or user.
- **Device not ready**
  This error most often occurs when there is no floppy disk (or a bad disk) in the disk drive and the system tries to perform tasks involving that disk.
- **Disk Boot Failure**

This error message is commonly seen when the hard drive of the computer is having problems.

- **File not found**
  The file concerned may have been damaged, moved, deleted, or a bug may have caused the error. Alternatively, the file might not exist, or the user has mistyped its name. This is most commonly seen on the internet with outdated links to web pages that no longer exist. On a local computer, this is more frequent on command line interfaces than on graphical user interfaces where files are presented iconically and users do not type file names.
- **Low Disk Space**
  This error occurs when the hard drive is (nearly) full. To fix this, the user should close some programs (to free swap file usage) and delete some files (normally temporary files, or other files after they have been backed up), or get a bigger hard drive.
- **Out of memory**
  This error occurs when the system has run out of memory or tries to load a file too large to store in RAM. The fix is to close some programs or install more physical memory.
- **[Program name] has stopped working.**
  This message and similar ones are displayed by several operating systems when program causes a general protection fault or invalid page fault.

• Troubleshooting Procedures and Preventative Maintenance:-

Preventive maintenance reduces the probability of hardware or software problems by systematically and periodically checking hardware and software to ensure proper operation.

Hardware

Check the condition of cables, components, and peripherals. Clean components to reduce the likelihood of overheating. Repair or replace any components that show signs of damage or excessive wear.

Use the following tasks as a guide to create a hardware maintenance program:

■ Remove dust from fan intakes.

■ Remove dust from the power supply.

■ Remove dust from components inside the computer.

■ Clean the mouse and keyboard.

■ Check and secure loose cables.

Software

Verify that installed software is current. Follow the policies of the organization when installing security updates, operating system updates, and program updates. Many organizations do not allow updates until extensive testing has been completed. This testing is done to confirm that the update will not cause problems with the operating system and software.

Use the tasks listed as a guide to create a software maintenance schedule that fits the needs of your computer equipment:

■ Review security updates.

■ Review software updates.

■ Review driver updates.

■ Update virus definition files.

■ Scan for viruses and spyware.

■ Remove unwanted programs

■ Scan hard drives for errors.

■ Defragment hard drives.

Troubleshooting requires an organized and logical approach to problems with computers and other components. A logical approach to troubleshooting allows you to eliminate variables in a systematic order. Asking the right questions, testing the right hardware, and examining the right data helps you understand the problem. This helps you form a proposed solution to try.

Troubleshooting is a skill that you will refine over time. Each time you solve another problem, you will increase your troubleshooting skills by gaining more experience. You will learn how and when to combine, as well as skip, steps to reach a solution quickly. The following troubleshooting process is a guideline that you can modify to fit your needs.

■ Explain the purpose of data protection.

■ Identify the problem.

■ Establish a theory of probable causes.

■ Test the theory to determine an exact cause.

■ Establish a plan of action to resolve the problem and implement the solution.

■ Verify full system functionality, and if applicable, implement preventive measures.

■ Document findings, actions, and outcomes.

- **Troubleshooting Tools and Diagnostic software:-**

Here are some the network troubleshooting tools available :

1. Ping (ICMP/ SNMP/ Proxy)
2. Tracert/ Traceroute
3. Browse
4. Telnet/ SSH
5. Remote Desktop
6. Terminal
7. IT workflow automation

1. Ping Tools

The ICMP ping tool is a basic network troubleshooting tool that lets you assess if a device is reachable on the network. It reports on errors such as packet loss, round-trip-time, etc.

a) **SNMP ping:** It is used to check if the simple network management protocol (SNMP) is enabled in a network device. If SNMP is enabled, the device responds with a set of basic information such as DNS name, system name, location, system type, system description, etc.

b) **Proxy ping:** This is used to ping a destination device behind a proxy. Basically, the pinging device sends an SNMP SET command to the proxy router to send an ICMP echo request to the destination device. The response is collected by the proxy device. This response is fetched using the SNMP GET command. This ping also requires SNMP to be enabled in the proxy device with the write community string enabled.

2. Tracert/ Trace Route

Tracert (Windows) or traceroute (Linux) is a network diagnostic and troubleshooting tool to view the route and measure transit delays of data packets in a network. It displays the number of hops between the source and destination devices based on the hop limit concept, modifying the Time To Live (TTL) values.

3. Browse

Browse allows you to connect to the built-in GUI of most network devices using a 'http/ https' request. This allows you to access the device settings or configuration to troubleshoot network issues with ease.

4. Telnet/ SSH

Telnet or Secure Shell (SSH) utility allows you to troubleshoot issues by establishing a CLI session with Linux/Unix devices. It is a simple yet effective network troubleshooting tool that enables you to act on any alert by executing CLI commands to remediate L1/L2 network problems.

5. Remote Desktop

The remote desktop utility allows you authenticate and access the desktop environment of any remote Windows devices in the network, from OpManager's user interface (UI). This allows for quick network troubleshooting like in the case of Telnet/ SSH for Linux/Unix based devices.

6. Terminal

The terminal allows you to establish a secure and encrypted connection with the remote device to execute various commands, diagnose and troubleshoot network problems.

7. IT workflow automation

IT workflow automation is a powerful and adept network troubleshooting automation tool that executes Level 1 troubleshooting and repetitive maintenance tasks based on predefined workflows. The network administrator can easily drag-and-drop actions into the workflow builder to create a troubleshooting flow. This will initiate step-by-step troubleshooting for network faults on a regular basis based on the scheduled time or when alarms are triggered on associated devices or groups.

- ## Device drivers:-

What Is a Device Driver?

A device driver is a software program without a user interface (UI) that manages hardware components or peripherals attached to a computer and enables them to function with the computer smoothly.

A device driver is a specialized software that operates a particular computer-connected device—offering a software interface to the hardware allows operating systems and other computer applications to access hardware functionalities.

1. Kernel device drivers

Kernel device drivers consist of some generic hardware loaded with the operating system (OS) as part of the OS. They include motherboards, processors, and BIOS. They are invoked and loaded into the random-access memory (RAM) when required. When several of them are operating at the same time, the machine can slow down. Thus, there is a minimum requirement for each OS.

2. User-mode device drivers

User mode device drivers execute in user mode. They refer to device drivers that users may trigger during a session. When using a system, users may have their own external devices that they bring to use, such as

external plug-and-play devices. These devices also require drivers to function.

3. Character drivers

Character device drivers provide unstructured access to the hardware. They transfer data to and from devices without using a specific device address. They allow the reading or writing of one byte at a time as a stream of sequential data.

4. Block drivers

Block device drivers provide structured access to the hardware. They use file system block-sized buffers from a buffer cache supplied by the kernel to perform I/O. A buffer cache is a memory pool established by the kernel to store frequently accessed blocks via block devices. The buffer cache reduces the amount of I/O queries that need an I/O operation from the device.

5. Original equipment manufacturer (OEM) drivers

Device drivers can be categorized as generic or OEM-related. Generic drivers refer to device drivers with their operating software bundled into the OEM hardware. One can use generic drivers with different brands of a particular device type. For instance, Linux works with several generic drivers that function without the need to install any other software manually.

7. BIOS

The basic input output system (BIOS) is the most fundamental driver on a computer. It is located in a read-only memory (ROM) chip, which ensures that BIOS will be available even when the hard disk is formatted. It is in charge of booting a computer and providing it with a set of instructions during this process.

8. Motherboard drivers

Motherboard drivers are simple applications that both Windows and Linux may utilize. They exist within the operating system and enable fundamental computer operations. These drivers comprise applications that allow the keyboard and mouse’s USB devices and I/O ports to work. Some motherboards have drivers that support video and audio.