What happens when we turn on computer?

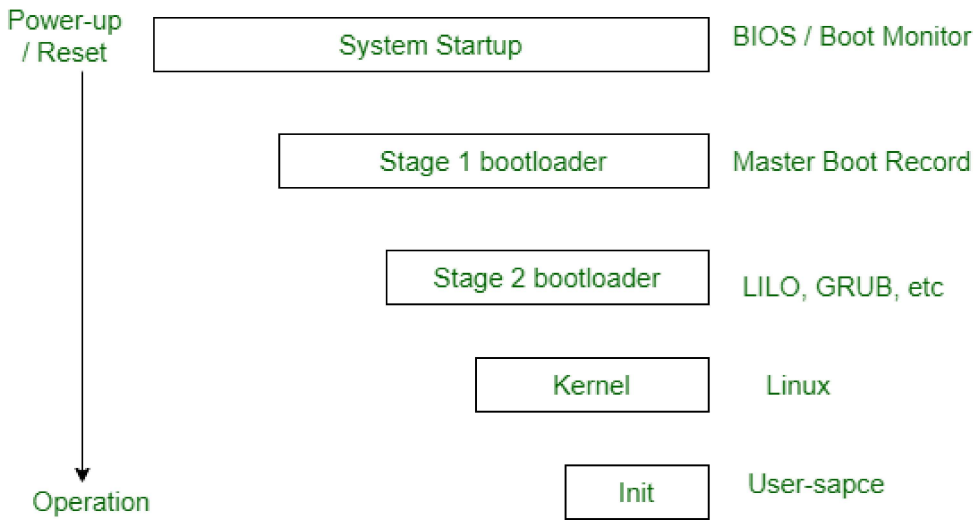
Last Updated : 31 Jul, 2023

A computer without a program running is just an inert hunk of electronics. The first thing a computer has to do when it is turned on is to start up a special program called an operating system. The operating system's job is to help other computer programs work by handling the messy details of controlling the computer's hardware.

What happens when we turn on computer?

1. The power supply sends electricity to the components of the computer, such as the motherboard, hard drive, and fans.
2. The BIOS (basic input/output system) initializes and performs a power-on self-test (POST), which checks the basic hardware components to ensure they are working properly. If any issues are detected, error messages may be displayed.
3. The operating system (OS), such as Windows or macOS, is loaded from the hard drive or another storage device into the computer's RAM (random access memory).
4. The OS then initializes its own components and drivers and presents the login screen or desktop environment to the user.

An overview of the boot process



The boot process is something that happens every time you turn your computer on. You don't really see it, because it happens so fast. You press the power button and come back a few sec (or minutes if on slow storage like HDD) later and Windows 10, or Windows 11, or whatever Operating System you use is all loaded.

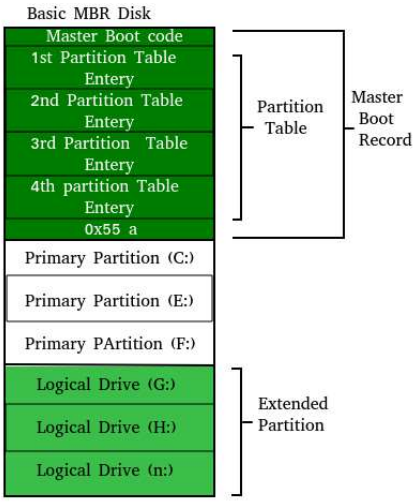
The BIOS chip tells it to look in a fixed place, usually on the lowest-numbered hard disk (the boot disk) for a special program called a boot loader (under Linux the boot loader is called Grub or LILO). The boot loader is pulled into memory and started. The bootloader's job is to start the real operating system.

Functions of BIOS

1. POST (Power On Self Test): The Power On Self Test happens each time you turn your computer on. It sounds complicated and that's because it kind of is. Your computer does so much when it's turned on and this is just part of that.

- It initializes the various hardware devices.
- It is an important process to ensure that all the devices operate smoothly without any conflicts. BIOSes following ACPI create tables describing the devices in the computer.
- The POST first checks the bios and then tests the CMOS RAM.
- If there is no problem with this then POST continues to check the CPU, hardware devices such as the Video Card, and the secondary storage devices such as the Hard Drive, Floppy Drives, Zip Drive, or CD/DVD Drives.
- If some errors are found then an error message is displayed on the screen or a number of beeps are heard.
- These beeps are known as POST beep codes.

2. Master Boot Record: The Master Boot Record (MBR) is a special boot sector at the beginning of the disk. The MBR contains the code that loads the rest of OS, known as bootloader. This complicated process (called the Boot Process) starts with the POST (Power On Self Test) and ends when the Bios searches for the MBR on the Hard Drive, which is generally located in the first sector, first head, first cylinder (cylinder 0, head 0, sector 1). A typical structure looks like this:



The bootstrap loader is stored in the computer's EPROM, ROM, or another non-volatile memory. When the computer is turned on or restarted, it first performs the power-on-self-test, also known as POST. If the POST is successful and no issues are found, the bootstrap loader will load the operating system for the computer into memory. The computer will then be able to quickly access, load, and run the operating system.

3. init: init is the last step of the kernel boot sequence. It looks for the file */etc/inittab* to see if there is an entry for *initdefault*. It is used to determine the initial run level of the system. A run-level is used to decide the initial

state of the operating system.
Some of the run levels are:

- **Level 0:** System Halt.
- **Level 1:** Single user mode.
- **Level 2:** Full multiuser mode without network.
- **Level 3:** Full multiuser mode with network.
- **Level 4:** user definable.
- **Level 5:** Full multiuser mode with network and X display manager.
- **Level 6:** Reboot.

The above design of init is called SysV- pronounced as System five. Several other implementations of init have been written now. Some of the popular implementations are systemd and upstart. Upstart is being used by ubuntu since 2006. More details of the upstart can be found here.

The next step of init is to start up various daemons that support networking and other services. X server daemon is one of the most important daemons. It manages the display, keyboard, and mouse. When X server daemon is started you see a Graphical Interface and a login screen is displayed.

4. System Configuration:
The BIOS allows the user to configure various system settings, such as:

1. Boot order: This determines the order in which the computer checks for bootable devices. For example, if the boot order is set to “hard drive” first, the computer will try to boot from the hard drive before checking other devices such as a CD/DVD drive or a USB drive.
2. Time and date: The BIOS stores the time and date information, which can be set and adjusted by the user. This information is used by the operating system and various applications.
3. Hardware settings: The BIOS provides options to configure various hardware settings such as CPU voltage, clock speed, and memory timings. These settings can be used to optimize system performance, but should only be changed by advanced users with the proper knowledge.

5. Security:
The BIOS can also provide security features such as:

1. Password protection: The BIOS can be set to require a password to access certain features or to prevent unauthorized booting of the computer. This can be useful in preventing unauthorized access to sensitive data.
2. Secure boot: Secure boot is a feature that ensures that only trusted operating system boot loaders, drivers, and firmware are loaded during the boot process. This helps to prevent malware and other unauthorized software from running on the system.
3. TPM (Trusted Platform Module): Some modern motherboards have a built-in TPM that provides hardware-based security features such as encryption, digital certificates, and secure key storage. This can help to protect sensitive data and prevent unauthorized access to the system.