1.What is BIOS

BIOS stands for Basic Input Output System

BIOS is non-volatile firmware used to perform hardware initialization during the booting process, and to provide runtime services for operating systems and programs. The BIOS firmware comes pre-installed on a personal computer's system board, and it is the first software to run when powered on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse and printer

2.What is the purpose of BIOS

BIOS enables computers to perform certain operations as soon as they are turned on. The principal job of a computer's BIOS is to govern the early stages of the startup process, ensuring that the operating system is correctly loaded into memory.

The first job of the BIOS after you switch your computer on is to perform the Power On Self Test. During the POST, the BIOS checks the computer's hardware in order to ensure that it is able to complete the startup process. If the POST is completed successfully, the system usually emits a beep. If the test fails, however, the system generally emits a series of beeps. You can use the number, duration and pattern of these beeps to identify the cause of the test failure.With the POST completed, the BIOS then attempts to load the operating system through a program known as a bootstrap loader, which is designed to locate any available operating systems; if a legitimate OS is found, it is loaded into memory. BIOS drivers are also loaded at this point. These are programs designed to give the computer basic control over hardware devices such as mice, keyboards, network hardware and storage devices.

3.Booting process of the system

All the booting instructions are built into chip called BIOS(Basic Input Output System) chip.The program in BIOS looks for a program called Boot Loader which is generally present in Boot Disk. ... It is the first process started during booting of the computersystem and runs continuosly until the system is shut down. In computing, booting is starting up a computer or computer appliance until it can be used. It can be initiated by hardware such as a button press or by software command. After the power is switched on, the computer is relatively dumb and can read only part of its storage called read-only memory.

4.Booting process in Linux and windows

A Linux boot process is the initialization of the Linux open source operating system on a computer. Also known as the Linux startup process, a Linux boot process covers a number of steps from the initial bootstrap to the launch of the initial user-space application.

6 Stages of Linux Boot Process

1. BIOS

- BIOS stands for Basic Input/Output System
- Performs some system integrity checks
- Searches, loads, and executes the boot loader program.
- It looks for boot loader in floppy, cd-rom, or hard drive. You can press a key (typically F12 of F2, but it depends on your system) during the BIOS startup to change the boot sequence.
- Once the boot loader program is detected and loaded into the memory, BIOS gives the control to it.
- So, in simple terms BIOS loads and executes the MBR boot loader.

2. MBR

- MBR stands for Master Boot Record.
- It is located in the 1st sector of the bootable disk. Typically /dev/hda, or /dev/sda
- MBR is less than 512 bytes in size. This has three components 1) primary boot loader info in 1st 446 bytes 2) partition table info in next 64 bytes 3) mbr validation check in last 2 bytes.
- It contains information about GRUB (or LILO in old systems).
- So, in simple terms MBR loads and executes the GRUB boot loader.

3. GRUB

- GRUB stands for Grand Unified Bootloader.
- If you have multiple kernel images installed on your system, you can choose which one to be executed.
- GRUB displays a splash screen, waits for few seconds, if you don’t enter anything, it loads the default kernel image as specified in the grub configuration file.

- GRUB has the knowledge of the filesystem (the older Linux loader LILO didn’t understand filesystem).

5. Init

- Looks at the /etc/inittab file to decide the Linux run level.
- Following are the available run levels
  - 0 – halt
  - 1 – Single user mode
  - 2 – Multiuser, without NFS
  - 3 – Full multiuser mode
  - 4 – unused
  - 5 – X11
  - 6 – reboot
- Init identifies the default initlevel from /etc/inittab and uses that to load all appropriate program.
- Execute ‘grep initdefault /etc/inittab’ on your system to identify the default run level
- If you want to get into trouble, you can set the default run level to 0 or 6. Since you know what 0 and 6 means, probably you might not do that.
- Typically you would set the default run level to either 3 or 5.

6. Runlevel programs

When the Linux system is booting up, you might see various services getting started. For example, it might say “starting sendmail …. OK”. Those are the runlevel programs, executed from the run level directory as defined by your run level.

Windows Server Boot Process!!!

1. System is powered on.
2. The CMOS loads the BIOS and then runs POST.
3. Looks for the MBR on the **bootable** device.
4. Through the MBR the **boot** sector is located and the BOOTMGR is loaded.
5. BOOTMGR looks for active partition.
6. BOOTMGR reads the BCD file from the **\boot** directory on the active partition.

5.What is UEFI

The Unified Extensible Firmware Interface is a specification that defines a software interface between an operating system and platform firmware. UEFI originated as the Intel Boot Initiative in the late 1990s before being turned over to the Unified EFI Forum, and today the forum and specification remain the result of a collaborative effort between computer processor manufacturers like AMD and Intel and software operating system companies like Microsoft and Apple.

In many ways, UEFI serves as a software-driven, bare-bones operating system that can sit on top of the legacy BIOS boot process, and like BIOS, UEFI is responsible for initializing the hardware of a device or computer before passing control of the hardware to the operating system. Most newer computer platforms support both UEFI and legacy BIOS booting in order to ease the transition to UEFI and accommodate older operating systems that don't have built-in UEFI support.

6.Difference between RAID and LVM

RAID

- RAID is used for redundancy.
- A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.
- RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.
- RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.
- RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.

LVM

- LVM is a way in which you partition the hard disk logically and it contains its own advantages.
- LVM is a logical layer that that can be anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
- LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc
- LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
- LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.

7.Encryption in WhatsApp

WhatsApp has no ability to see the content of messages or listen to calls onWhatsApp. That's because the encryption and decryption of messages sent onWhatsApp occurs entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys

End-to-end encryption

Privacy and security is in our DNA, which is why we have end-to-end encryption. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, status updates and calls are secured from falling into the wrong hands.WhatsApp end-to-end encryption ensures only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. For added protection, every message you send has an unique lock and key. All of this happens automatically: No need to turn on settings or set up special secret chats to secure your messages.End-to-end encryption is always activated. There's no way to turn off end-to-end encryption.