# 3.10.3 BIOS/UEFI Facts

You should know the following facts about the UEFI, BIOS, EEPROM, and CMOS:

| Component | Description |
|---|---|
| Unified Extensible Firmware Interface (UEFI) | The UEFI was designed to replace the BIOS. Important things about UEFI are:<br>▪ The UEFI is firmware.<br>▪ The UEFI program controls the startup process and loads the operating system into memory.<br>▪ The UEFI design improves the software interoperability and the address limitations of BIOS.<br>▪ The UEFI provides better security to protect against bootkit (malware attacks on the boot process) attacks.<br>▪ The UEFI provides faster startup times.<br>▪ The UEFI supports drives larger than 2.2 terabytes.<br>▪ The UEFI supports 64-bit firmware device drivers.<br>▪ The UEFI is compatible with both BIOS and UEFI hardware.<br>▪ You should frequently check for UEFI updates from the manufacturer. Updating the UEFI (called flashing the UEFI) makes new features available. |
| Basic Input/Output System (BIOS) | The BIOS is a legacy program stored in a read-only memory (ROM) chip that the CPU automatically loads and executes when it receives power. Important things to know about the BIOS are:<br>▪ The BIOS program controls the startup process and loads the operating system into memory.<br>▪ The BIOS is firmware.<br>▪ You should frequently check for BIOS updates from the manufacturer. Updating the BIOS (called flashing the BIOS) makes new features available, such as allowing the BIOS to recognize newer hardware devices.<br>▪ Most BIOS chips vary from 265 KB to 1 MB in size.<br>▪ Video cards include a BIOS chip on the device. These devices have their own ROM chip called an option ROM (OpROM). |
| Electrically Erasable Programmable Read-Only Memory (EEPROM) | The EEPROM is a RAM chip that replaced the CMOS chip. Important things about EEPROM are:<br>▪ EEPROM is a type of non-volatile memory used in computers and other electronic devices to store relatively small amounts of data.<br>▪ EEPROM allows individual bytes to be erased and reprogrammed.<br>▪ EEPROM replaced EPROM chips and are used for computer BIOS built after 1994.<br>▪ EEPROM chips allow you to update the BIOS/UEFI in your computer without having to open the computer and remove any chips. |
| Complementary Metal-Oxide Semiconductor (CMOS) | CMOS is legacy computer chip technology that has become a general term used for the program that stores important system information related to the starting of a computer. It is often used synonymously with BIOS. Data held in CMOS includes the hard disk type and configuration, the order of boot devices, and other configurable settings related to the system hardware. The following are important things to know about CMOS: |

| | |
|---|---|
| | ▪ You changed the data stored in CMOS using a CMOS editor program that was part of the BIOS.<br>▪ CMOS used to refer to the real-time clock and the CMOS chip that stored system information. Both were powered by a CMOS battery. Now, the EEPROM chip stores the system information that used to be stored on the CMOS chip. EEPROM requires no power to maintain data storage.<br>▪ The CMOS battery is still used to keep the real-time system clock running when the computer is powered off. It can be a low-voltage dry cell, lithium mounted on the motherboard, or even AA batteries in a housing clipped on a wall inside of the case. The electric current is about 1 millionth of an amp and can provide effective power for years. |

During the computer's startup procedure, you can press one or more keys to open a CMOS editor so you can change the data stored in CMOS memory. This CMOS setup program is part of the BIOS program. The key or keys you press to open the CMOS editor depend on the BIOS manufacturer. The easiest way to find out which key to press is to read the screen as it boots or to consult the motherboard documentation. The most common keys are Delete, Insert, F1, and F2.

Common reasons for editing the CMOS settings are:

- To change the boot device order.
- To enable or disable motherboard devices.
- To add a password to the setup program to prevent unauthorized access.

  If you set a BIOS/UEFI password and then forget it, you will be unable to edit CMOS settings.

  To remove the password for most motherboards, move or remove a jumper, then replace it after a specific period of time.
- To configure processor or memory settings (e.g., when you need to set operating speeds or when you want to overclock hardware settings).
- (In rare cases) To manually configure device properties for legacy devices.

One of the main jobs of the BIOS/UEFI is to help start the system. The following process is used when you turn a computer on:

1. Power is supplied to the processor. The processor is hard-coded to look at a special memory address for the code to execute.
2. This memory address contains a pointer or jump program which instructs the processor where to find the BIOS program.
3. The processor loads the BIOS program. The first BIOS process to run is the power-on self-test (POST) process. POST does the following:
   1. Verifies the integrity of the BIOS/UEFI code.
   2. Looks for the BIOS on the video card and loads it. This powers the video card and results in information being shown on the monitor.
   3. Looks for BIOS programs on other devices, such as hard disk controllers and loads those.
   4. Tests system devices, such as verifying the amount of memory on the system.
4. After POST tests complete, the BIOS identifies other system devices. It uses CMOS settings and information supplied by the devices themselves to identify and configure hardware devices. Plug-and-play devices are allocated system resources.

5. Then the BIOS searches for a boot drive using the boot order specified in the CMOS.
6. On the boot device, the BIOS/UEFI searches for the master bootloader, then loads the bootloader program. At this point, the BIOS/UEFI stops controlling the system and passes control to the bootloader program.
7. The bootloader program is configured to locate and load the operating system.
8. As the operating system loads, additional steps are taken to load all additional programs and configure devices for use by the operating system.

From time to time, your PC's manufacturer may release updates to your BIOS firmware. To update the BIOS, you will need to download the update along with a utility provided by your PC manufacturer that is used to rewrite data stored in the BIOS chip. This process is called *flashing* the BIOS. The actual steps you follow to flash the BIOS will vary by manufacturer.

> You should connect your PC to a UPS before flashing the BIOS. If a power outage occurs during the flash process, it will irrecoverably damage the BIOS and prevent your system from booting.

---