|  |
| --- |
| D:\SK\FORMAT\SVCET LETTER HEAD.jpg**Department of Computer Science and Engineering**Subject Name: **COMPUTER HARDWARE AND NETWORK TROUBLESHOOTING**Subject Code: **CS T72** **Prepared By :** Dr. N. Balaji, Professor & HOD / CSE**Verified by : Approved by :****UNIT – V** |
| **External I/O Interfaces:** Serial versus Parallel - USB: system, data transfer, and controller – Hot plugging – Low speed connections: RS232C and Parallel port: SPP, EPP, ECP – Local Area Networking: Requirements – Wired – Wireless – Bluetooth – Network Interface Cards – Wired Topologies – Switches/Access Points – Wireless Ethernet hardware – Network Protocols: IP and TCP/IP, IPX, NetBEUI. – Cables and Connections. Troubleshooting network problems.**PC Diagnostics, Testing & Maintenance**: POST – Boot process – Maintenance tools – Preventive Maintenance. |
| **2 Marks**1. **What are the two types of Partitioning?**

Primary and Extended Partitioning are the two major types of hard disk partitioning.1. **Define Extended Partitioning?**

An extended partition is secondary to the primary partition. A hard disk may contain only one extended partition, which can then be sub-divided into logical drives each of which (under dos and windows) assigned additional drive letters. Extended partition is useful if you want more than four partitions on a single physical drive.1. **Define Unix Partitioning?**

An extended partition is secondary to the primary partition. A hard disk may contain only one extended partition, which can then be sub-divided into logical drives each of which (under dos and windows) assigned additional drive letters. Extended partition is useful if you want more than four partitions on a single physical drive.1. **How to install the LinuX?**

To install Linux, you follow a simple, step-by-step procedure that has three main phases:* + Installing the operating system kernel and base system
	+ Configuring the new Linux system
	+ Installing applications

WARNING**:** Although the Linux installation procedure is generally trouble free, errors or malfunctions that occur during the installation of an operating system can result in loss of data. You should not begin the installation procedure until you have backed up all data on your system and determined that your backup is error-free. |

## What are the two types of computer for faults based on the frequency occurrence of the problem? (NOV 2010)

* 1. Permanent (or) Solid fault
	2. Intermittent fault

**Permanent (or) Solid fault**: When there is a permanent fault in a computer, the misbehaves consistently. Any number of times the program is run, the result or symptoms will be the same.

**Intermittent fault:** When there is an intermittent fault in a computer, the computer’s behavior is not consistent. Sometimes it works properly and suddenly it malfunction. After a certain period of time, it recovers from the fault automatically and again starts functioning properly.

## List some of the symptoms of computer faults? (APR 2011)

Peripherals are not working properly Computer will not properly boot.

Long beep when power on the PC. Noisy when power on the system.

## How to Install Network Hardware and Software?

If there is no hardware installed for networking, you will need to purchase a PCI networking card for a wired network or a PCI card for wireless networking. If it has a networking card already installed for a wired network and you are changing to a wireless networking, you can leave the old card in and disable it or remove the card.

If your network is not installed, you will need to install it. If you are using Windows, you should be the following Network components are installed:

* Client for Microsoft Windows
* Internet Protocol (TCP/IP)
* Adapter card software driver

## What do you mean by spyware? (NOV 2012)

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a *spybot* or *tracking software*), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software [virus](http://searchsecurity.techtarget.com/definition/virus) or as the result of installing a new program.

## Define Virus Scanner?

A Virus Scanner is a program that searches files or storage devices for [Virus](http://hitachi-id.com/concepts/virus.html)es. It is a useful preventative measure to avoid contagion.

## Define Interrupt?

An interrupt is a signal from a device attached to a computer or from a program within the computer that causes the main program that operates the computer (the [operating system](http://searchcio-midmarket.techtarget.com/definition/operating-system) ) to stop and figure out what to do next. Almost all personal (or larger) computers today are *interrupt- driven* - that is, they start down the list of computer [instruction](http://searchcio-midmarket.techtarget.com/definition/instruction) s in one program.

## List out the different types of Hardware Interrupts? (NOV 2012)

*Hardware interrupts* are used by devices to communicate that they require attention from the operating system. Some common examples are a hard disk signalling that is has read a series of data blocks, or that a network device has processed a buffer containing network packets. Interrupts are also used for asynchronous events, such as the arrival of new data from an external network. Hardware interrupts are delivered directly to the CPU using a small network of interrupt management and routing devices.

* [Level-signalled interrupts](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/chap-Realtime_Reference_Guide-Hardware_interrupts.html#sect-Realtime_Reference_Guide-Hardware_interrupts-Level_signalled_interrupts)
* [Message-signalled interrupts](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/sect-Realtime_Reference_Guide-Hardware_interrupts-Message_signalled_interrupts.html)
* [Non-maskable interrupts](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/sect-Realtime_Reference_Guide-Hardware_interrupts-Non_maskable_interrupts.html)
* [System management interrupts](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/sect-Realtime_Reference_Guide-Hardware_interrupts-System_management_interrupts.html)
* [Advanced programmable interrupt controller](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_MRG/1.3/html/Realtime_Reference_Guide/sect-Realtime_Reference_Guide-Hardware_interrupts-Advanced_programmable_interrupt_controller.html)

## What are the four levels of troubleshooting approaches? (APR 2011)

The systematic trouble shooting approaches can be divided in to the following steps:

* 1. Symptoms observation
	2. Symptoms analysis
	3. Fault diagnosis
	4. Fault rectification

## Categorize the type of trouble shooting tools? (NOV 2010), (APR 2012), (NOV 2012)

There are two types of trouble shooting tools

* 1. Nodal Testers
	2. System Testers

The nodal testers are simple conventional test equipment to probe in and around the circuit. These tester include oscilloscope, logic probe, logic clip, logic pulser, current tracer and comparator.

## Define Multimeter?

A multimeter or a multitester is an [electronicmeasuring instrument](http://en.wikipedia.org/wiki/Electronics) that combines several functions in one unit. The most basic instruments include an [ammeter](http://en.wikipedia.org/wiki/Ammeter), [voltmeter](http://en.wikipedia.org/wiki/Voltmeter), and [ohmmeter](http://en.wikipedia.org/wiki/Ohmmeter). Analog multimeters are sometimes referred to as "volt-ohm-meters", abbreviated VOM. Digital multimeters are usually referred to as "digital-multi-meters", abbreviated DMM.

## Define Oscilloscope?

A typical oscilloscope can display alternating current ([AC](http://whatis.techtarget.com/definition/0%2C%2Csid9_gci213754%2C00.html)) or pulsating direct current (DC) waveforms having a frequency as low as approximately 1 hertz ([Hz](http://searchmobilecomputing.techtarget.com/definition/hertz)) or as high as several megahertz ([MHz](http://searchnetworking.techtarget.com/definition/MHz)). High-end oscilloscopes can display signals having frequencies up to several hundred gigahertz ([GHz](http://searchnetworking.techtarget.com/definition/gigahertz)). The display is broken up into so-called horizontal divisions (hor div) and vertical divisions (vert div). Time is displayed from left to right on the horizontal scale. Instantaneous voltage appears on the vertical scale, with positive values going upward and negative values going downward.

## What is meant by Logic analyzer?

A **logic analyzer** displays signals in a [digital circuit](http://en.wikipedia.org/wiki/Digital_circuit) that are too fast to be observed by a human being and presents it to a user so that the user can more easily check correct operation of the digital system.

## Define In-Circuit Emulator?

An **in-circuit emulator** (ICE) also called **on-circuit debugger** (OCD) or **background debug module** (BDM) is a hardware device used to [debug](http://en.wikipedia.org/wiki/Debugger) the [software](http://en.wikipedia.org/wiki/Software) of an [embedded system](http://en.wikipedia.org/wiki/Embedded_system). Embedded systems present special problems for a programmer, because they usually lack keyboards, screens, disk-drives and other helpful user interfaces and storage devices that are present on business computers.

## What are the troubleshooting problems of CD-ROM drive?(APR 2012)

* Disk error problem
* CD not recognized
* Noise Problem
* Motor Problem
* Laser Light Problem
* Reader/Writer Problem

## Define Operating System? (NOV 2012)

The operating system is the most important [program](http://www.webopedia.com/TERM/P/program.htm) that [runs](http://www.webopedia.com/TERM/R/run.htm) on a [computer](http://www.webopedia.com/TERM/C/computer.htm). Every general- purpose computer must have an operating system to run other programs and [applications](http://www.webopedia.com/TERM/A/application.html). Operating systems perform basic tasks, such as recognizing [input](http://www.webopedia.com/TERM/I/input.htm)from the [keyboard](http://www.webopedia.com/TERM/K/keyboard.htm), sending [output](http://www.webopedia.com/TERM/O/output.htm) to the [display screen,](http://www.webopedia.com/TERM/D/display_screen.htm) keeping track of [files](http://www.webopedia.com/TERM/F/file.htm) and [directories](http://www.webopedia.com/TERM/D/directory.htm) on the [disk](http://www.webopedia.com/TERM/D/disk.htm), and controlling [peripheral devices](http://www.webopedia.com/TERM/P/peripheral_device.htm) such as [disk drives](http://www.webopedia.com/TERM/D/disk_drive.htm) and [printers](http://www.webopedia.com/TERM/P/printer.htm).

## What are the major functions OS? (NOV 2013)

* An operating system manages hardware, runs applications, provides an interface for users, and stores, retrieves, and manipulates files.
* It manages the hardware and software resources of the system.
* It provides a stable, consistent way for applications to deal with the hardware without having to know all the details of the hardware.
* System tool (programs) used to monitor computer performance,debug,problems, or maintain parts of the system.
* A set of libraries or functions which may use to perform specific tasks especially relating to interfacing with computer system components.

## What is mean by network? (NOV 2013)

A network is a group of two or mor[e computer systems](http://www.webopedia.com/TERM/C/computer_system.html) linked together. There are many types of [computer](http://www.webopedia.com/TERM/C/computer.html) [networks,](http://www.webopedia.com/TERM/N/network.html) including the following:

[**local-area networks (LANs)**](http://www.webopedia.com/TERM/L/local_area_network_LAN.html)**:** The computers are geographically close together (that is, in the same building).

[**wide-area networks (WANs)**](http://www.webopedia.com/TERM/W/wide_area_network_WAN.html)**:** The computers are farther apart and are connected by telephone lines or radio waves.

[**metropolitan-area networks MANs)**](http://www.webopedia.com/TERM/M/MAN.html)**:** A data network designed for a town or city.

## What is the use of logic probe? (NOV 2014)

A **logic probe** is a hand-held pen-like [test probe](https://en.wikipedia.org/wiki/Test_probe) used for analyzing and troubleshooting the logical states ([Boolean](https://en.wikipedia.org/wiki/Boolean_logic) 0 or 1) of a digital circuit. While most are powered by the circuit under test, some devices use batteries. They can be used on either [TTL](https://en.wikipedia.org/wiki/Transistor%E2%80%93transistor_logic) (transistor-transistor logic) or [CMOS](https://en.wikipedia.org/wiki/CMOS) (complementary metal-oxide semiconductor) integrated circuit devices.

## What do you mean by Boot virus? (NOV 2014)

A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it. As a result, even non-bootable media can trigger the spread of boot sector viruses. These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table. During start- up, the virus gets loaded to the computer's memory. As soon as the virus is saved to the memory, it infects the non-infected disks used by the system.

## What does Hot Plugging mean?

Hot plugging is the ability to replace or install a device without shutting down the attached computer. Hot plugging is implemented when a peripheral device is added or removed; a device or working system requires reconfiguration; a defective component requires replacement or a device and computer require data synchronization. Hot swapping allows easy accessibility to equipment and the convenience of uninterrupted systems. Also known as hot swapping. True hot plugging device includes USB, high end SCSI devices and FireWire.

## 11 MARKS

1. **Compare Serial Port Vs. Parallel Port**

Serial ports are generally built into the mother board, which is why the connectors behind the casing and connected to the mother board by a wire cable can be used to connect an exterior element. Serial connectors generally have 9 or 25 pins and take the following form (DB9 and DB25 connectors respectively):



A personal computer generally has between one and four serial ports.

## Parallel port

[Parallel](http://ccm.net/contents/transmission/transmode.php3) data transmission involves sending data simultaneously on several channels (wires). The parallel ports on personal computers can be used to send 8 bits (one octet) simultaneously via 8 wires.



The first two-way parallel ports allowed for speeds of 2.4Mb/s. Enhanced parallel ports have been developed however to achieve higher speeds:

* **The EPP** (*Enhanced Parallel Port*) achieves speeds of 8 to 16 Mbps
* **The ECP** (*Enhanced Capabilities Port*), developed by *Hewlett Packard* and *Microsoft*. It has the same characteristics as the EPP with in addition a *Plug and Play* feature, allowing the computer to recognise the connected peripherals.

Parallel ports, like serial ports, are built into the mother board. DB25 connectors allow connection to an exterior element (e.g. a printer).



# Explain briefly about USB.

Universal Serial Bus (USB) is a set of interface specifications for high speed wired communication between electronics systems peripherals and devices with or without PC/computer. The USB was originally developed in 1995 by many of the industry leading companies like Intel, Compaq, Microsoft, Digital, IBM, and Northern Telecom.

The major goal of USB was to define an external expansion bus to add peripherals to a PC in easy and simple manner. The new external expansion architecture, highlights,

* 1. PC host controller hardware and software
	2. Robust connectors and cable assemblies
	3. Peripheral friendly master-slave protocols
	4. Expandable through multi-port hubs.

USB offers users simple connectivity. It eliminates the mix of different connectors for different devices like printers, keyboards, mice, and other peripherals. That means USB- bus allows many peripherals to be connected using a single standardized interface socket. Another main advantage is that, in USB environment, DIP-switches are not necessary for setting peripheral addresses and IRQs. It supports all kinds of data, from slow mouse inputs to digitized audio and compressed video.

USB also allows hot swapping. The "hot-swapping" means that the devices can be plugged and unplugged without rebooting the computer or turning off the device. That means, when plugged in, everything configures automatically. So the user needs not worry about terminations, terms such as IRQs and port addresses, or rebooting the computer. Once the user is finished, they can simply unplug the cable out, the host will detect its absence and automatically unload the driver. This makes the USB a plug-and- play interface between a computer and add-on devices.

The loading of the appropriate driver is done using a PID/VID (Product ID/Vendor ID) combination. The VID is supplied by the USB Implementer's forum



Fig 1: The USB "trident" logo

The USB has already replaced the RS232 and other old parallel communications in many applications. USB is now the most used interface to connect devices like mouse, keyboards, PDAs, game-pads and joysticks, scanners, digital cameras, printers, personal media players, and flash drives to personal computers. Generally speaking, USB is the most successful interconnect in the history of personal computing and has migrated into consumer electronics and mobile products.

USB sends data in serial mode i.e. the parallel data is serialized before sends and de- serialized after receiving.

The benefits of USB are low cost, expandability, auto-configuration, hot-plugging and outstanding performance. It also provides power to the bus, enabling many peripherals to operate without the added need for an AC power adapter.

**Various versions USB:**

As USB technology advanced the new version of USB are unveiled with time. Let us now try to understand more about the different versions of the USB.

**USB1.0:** Version 0.7 of the USB interface definition was released in November 1994. But USB 1.0 is the original release of USB having the capability of transferring 12 Mbps, supporting up to 127 devices. And as we know it was a combined effort of some large players on the market to define a new general device interface for computers. This USB 1.0 specification model was introduced in January1996. The data transfer rate of this version can accommodate a wide range of devices, including MPEG video devices, data gloves, and digitizers. This version of USB is known as full-speed USB.

Since October-1996, the Windows operating systems have been equipped with USB drivers or special software designed to work with specific I/O device types. USB got integrated into Windows 98 and later versions. Today, most new computers and peripheral devices are equipped with USB.

**USB1.1:** USB 1.1 came out in September 1998 to help rectify the adoption problems that occurred with earlier versions, mostly those relating to hubs.

USB 1.1 is also known as full-speed USB. This version is similar to the original release of USB; however, there are minor modifications for the hardware and the specifications. USB version 1.1 supported two speeds, a full speed mode of 12Mbits/s and a low speed mode of 1.5Mbits/s. The 1.5Mbits/s mode is slower and less susceptible to EMI, thus reducing the cost of ferrite beads and quality components.

**USB2.0:** Hewlett-Packard, Intel, LSI Corporation, Microsoft, NEC, and Philips jointly led the initiative to develop a higher data transfer rate than the 1.1 specifications. The USB 2.0 specification was released in April 2000 and was standardized at the end of 2001. This standardization of the new device-specification made backward compatibility possible, meaning it is also capable of supporting USB 1.0 and 1.1 devices and cables.

Supporting three speed modes (1.5, 12 and 480 megabits per second), USB 2.0 supports low-bandwidth devices such as keyboards and mice, as well as high-bandwidth ones like high-resolution Web-cams, scanners, printers and high-capacity storage systems.

USB 2.0, also known as hi-speed USB. This hi-speed USB is capable of supporting a transfer rate of up to 480 Mbps, compared to 12 Mbps of USB 1.1. That's about 40 times as fast! Wow!

**USB3.0:** USB 3.0 is the latest version of USB release. It is also called as Super-Speed USB having a data transfer rate of 4.8 Gbit/s (600 MB/s). That means it can deliver over 10x the speed of today's Hi-Speed USB connections.

The USB 3.0 specification was released by Intel and its partners in August 2008. Products using the 3.0 specifications are likely to arrive in 2009 or 2010. The technology targets fast PC sync-and-go transfer of applications, to meet the demands of Consumer Electronics and mobile segments focused on high-density digital content and media.

USB 3.0 is also a backward-compatible standard with the same plug and play and other capabilities of previous USB technologies. The technology draws from the same architecture of wired USB. In addition, the USB 3.0 specification will be optimized for low power and improved protocol efficiency.

**USB system overview:**

The USB system is made up of a host, multiple numbers of USB ports, and multiple peripheral devices connected in a tiered-star topology. To expand the number of USB ports, the USB hubs can be included in the tiers, allowing branching into a tree structure with up to five tier levels.

The tiered star topology has some benefits. Firstly power to each device can be monitored and even switched off if an overcurrent condition occurs without disrupting other USB devices. Both high, full and low speed devices can be supported, with the hub filtering out high speed and full speed transactions so lower speed devices do not receive them.

The USB is actually an addressable bus system, with a seven-bit address code. So it can support up to 127 different devices or nodes at once (the "all zeroes" code is not a valid address). However it can have only one host: the PC itself. So a PC with its peripherals connected via the USB forms a star local area network (LAN).

On the other hand any device connected to the USB can have a number of other nodes connected to it in daisy-chain fashion, so it can also form the hub for a mini-star sub- network. Similarly it is possible to have a device, which purely functions as a hub for other node devices, with no separate function of its own. This expansion via hubs is possible because the USB supports a tiered star topology. Each USB hub acts as a kind of traffic cop. for its part of the network, routing data from the host to its correct address and preventing bus contention clashes between devices trying to send data at the same time.

On a USB hub device, the single port used to connect to the host PC either directly or via another hub is known as the upstream port, while the ports used for connecting other devices to the USB are known as the downstream ports. USB hubs work transparently as far as the host PC and its operating system are concerned. Most hubs provide either four or seven downstream ports or less if they already include a USB device of their own.

The host is the USB system's master, and as such, controls and schedules all communications activities. Peripherals, the devices controlled by USB, are slaves responding to commands from the host. USB devices are linked in series through hubs. There always exists one hub known as the root hub, which is built in to the host controller.

A physical USB device may consist of several logical sub-devices that are referred to as device functions. A single device may provide several functions, for example, a web- cam (video device function) with a built-in microphone (audio device function). In short, the USB specification recognizes two kinds of peripherals: stand-alone (single function units, like a mouse) or compound devices like video camera with separate audio processor.

The logical channel connection host to peripheral-end is called pipes in USB. A USB device can have 16 pipes coming into the host controller and 16 going out of the controller.

The pipes are unidirectional. Each interface is associated with single device function and is formed by grouping endpoints.



The hubs are bridges. They expand the logical and physical fan-out of the network. A hub has a single upstream connection (that going to the root hub, or the next hub closer to the root), and one to many downstream connections.

Hubs themselves are considered as USB devices, and may incorporate some amount of intelligence. We know that in USB users may connect and remove peripherals without powering the entire system down. Hubs detect these topology changes. They also source power to the USB network. The power can come from the hub itself (if it has a built-in power supply), or can be passed through from an upstream hub.

**USB connectors & the power supply:**

Connecting a USB device to a computer is very simple -- you find the USB connector on the back of your machine and plug the USB connector into it. If it is a new device, the operating system auto-detects it and asks for the driver disk. If the device has already been installed, the computer activates it and starts talking to it.

The USB standard specifies two kinds of cables and connectors. The USB cable will usually have an "A" connector on one end and a "B" on the other. That means the USB devices will have an "A" connection on it. If not, then the device has a socket on it that accepts a USB "B" connector.



Fig 3: USB Type A & B Connectors

The USB standard uses "A" and "B" connectors mainly to avoid confusion:

1. "A" connectors head "upstream" toward the computer.
2. "B" connectors head "downstream" and connect to individual devices.

By using different connectors on the upstream and downstream end, it is impossible to install a cable incorrectly, because the two types are physically different.

Individual USB cables can run as long as 5 meters for 12Mbps connections and 3m for 1.5Mbps. With hubs, devices can be up to 30 meters (six cables' worth) away from the host. Here the high-speed cables for 12Mbps communication are better shielded than their less expensive 1.5Mbps counterparts. The USB 2.0 specification tells that the cable delay to be less than 5.2 ns per meter

Inside the USB cable there are two wires that supply the power to the peripherals-- +5 volts (red) and ground (brown)-- and a twisted pair (yellow and blue) of wires to carry the data. On the power wires, the computer can supply up to 500 milliamps of power at 5 volts. A peripheral that draws up to 100ma can extract all of its power from the bus wiring all of the time. If the device needs more than a half-amp, then it must have its own power supply. That means low-power devices such as mice can draw their power directly from the bus. High-power devices such as printers have their own power supplies and draw minimal power from the bus. Hubs can have their own power supplies to provide power to devices connected to the hub.

|  |  |  |
| --- | --- | --- |
| Pin No: | Signal | Color of the cable |
| 1 | +5V power | Red |
| 2 | - Data | White / Yellow |
| 3 | +Data | Green / Blue |
| 4 | Ground | Black/Brown |

Table - 1: USB pin connections

USB hosts and hubs manage power by enabling and disabling power to individual devices to electrically remove ill-behaved peripherals from the system. Further, they can instruct devices to enter the suspend state, which reduces maximum power consumption to 500 microamps (for low-power, 1.5Mbps peripherals) or 2.5ma for 12Mbps devices.



Fig 3: USB Type A & B Connectors

the USB is a serial protocol and physical link, which transmits all data differentially on a single pair of wires. Another pair provides power to downstream peripherals.

Note that although USB cables having a Type A plug at each end are available, they should never be used to connect two PCs together, via their USB ports. This is because a USB network can only have one host, and both would try to claim that role. In any case, the cable would also short their 5V power rails together, which could cause a damaging current to flow. USB is not designed for direct data transfer between PCs. But the "sharing hubs" technique allows multiple computers to access the same peripheral device(s) and work by switching access between PCs, either automatically or manually.

**USB Data transfer**

When a USB peripheral device is first attached to the network, a process called enumeration process gets started. This is the way by which the host communicates with the device to learn its identity and to discover which device driver is required. The enumeration starts by sending a reset signal to the newly connected USB device. The speed of the USB device is determined during the reset signaling. After reset, the host reads the USB device's information, and then the device is assigned a unique 7-bit address (will be discussed in next section). This avoids the DIP-switch and IRQ headaches of the past device communication methods. If the device is supported by the host, the device drivers needed for communicating with the device are loaded and the device is set to a configured state. Once a hub detects a new peripheral (or even the removal of one), it actually reports the new information about the peripheral to the host, and enables communications with it. If the USB host is restarted, the enumeration process is repeated for all connected devices.

In other words, the enumeration process is initiated both when the host is powered up and a device connected or removed from the network.

Technically speaking, the USB communications takes place between the host and endpoints located in the peripherals. An endpoint is a uniquely addressable portion of the peripheral that is the source or receiver of data. Four bits define the device's endpoint address; codes also indicate transfer direction and whether the transaction is a "control" transfer (will be discussed later in detail). Endpoint 0 is reserved for control transfers, leaving up to 15 bi-directional destinations or sources of data within each device. All devices must support endpoint zero. Because this is the endpoint, which receives all of the devices control, and status requests during enumeration and throughout the duration while the device is operational on the bus.

All the transfers in USB occur through virtual pipes that connect the peripheral's endpoints with the host. When establishing communications with the peripheral, each endpoint returns a descriptor, a data structure that tells the host about the endpoint's configuration and expectations. Descriptors include transfer type, max size of data packets, perhaps the interval for data transfers, and in some cases, the bandwidth needed. Given this data, the host establishes connections to the endpoints through virtual pipes.

Though physically configured as a tiered star, logically (to the application code) a direct connection exists between the host and each device.

The host controller polls the bus for traffic, usually in a round-robin fashion, so no USB device can transfer any data on the bus without an explicit request from the host controller.

USB can support four data transfer types or transfer mode, which are listed below.

1. Control
2. Isochronous
3. Bulk
4. Interrupt

Control transfers exchange configuration, setup and command information between the device and the host. The host can also send commands or query parameters with control packets.

Isochronous transfer is used by time critical, streaming device such as speakers and video cameras. It is time sensitive information so, within limitations, it has guaranteed access to the USB bus. Data streams between the device and the host in real-time, and so there will not be any error correction.

Bulk transfer is used by device like printers & scanners, which receives data in one big packet. Here the timely delivery is not critical. Bulk transfers are fillers, claiming unused USB bandwidth when nothing more important is going on. The error correction protects these packets.

Interrupt transfers is used by peripherals exchanging small amounts of data that need immediate attention. It is used by devices to request servicing from the PC/host. Devices like a mouse or a keyboard comes in this category. Error checking validates the data.

As devices are enumerated, the host is keeping track of the total bandwidth that all of the isochronous and interrupt devices are requesting. They can consume up to 90 percent of the 480 Mbps of bandwidth that is available. After 90 percent is used up, the host denies access to any other isochronous or interrupt devices. Control packets and packets for bulk transfers use any bandwidth left over (at least 10 percent).

The USB divides the available bandwidth into frames, and the host controls the frames. Frames contain 1,500 bytes, and a new frame starts every millisecond. During a frame, isochronous and interrupt devices get a slot so they are guaranteed the bandwidth they need. Bulk and control transfers use whatever space is left.

## Explain about RS232C.

RS-232C is a long-established standard ("C" is the current version) that describes the physical interface and [protocol](http://searchnetworking.techtarget.com/definition/protocol) for relatively low-speed [serial](http://searchcio-midmarket.techtarget.com/definition/serial) data communication between computers and related devices. It was defined by an industry trade group, the Electronic Industries Association (EIA), originally for [teletypewriter](http://whatis.techtarget.com/definition/0%2C%2Csid9_gci213663%2C00.html) devices.

RS-232C is the interface that your computer uses to talk to and exchange data with your modem and other serial devices. Somewhere in your PC, typically on a Universal Asynchronous

Receiver/Transmitter ([UART](http://whatis.techtarget.com/definition/0%2C%2Csid9_gci213237%2C00.html)) chip on your motherboard, the data from your computer is transmitted to an internal or external modem (or other serial device) from its Data Terminal Equipment ([DTE](http://searchnetworking.techtarget.com/definition/DTE)) interface. Since data in your computer flows along parallel circuits and serial devices can handle only one bit at a time, the UART chip converts the groups of bits in parallel to a serial stream of bits. As your PC's DTE agent, it also communicates with the modem or other serial device, which, in accordance with the RS-232C standard, has a complementary interface called the Data Communications Equipment ([DCE](http://searchnetworking.techtarget.com/definition/DCE)) interface.



## Explain briefly about Parallel Port.

1. **Describe the structure, operating modes and features of enhanced capabilities port. (NOV 2014)**
2. **Explain parallel and serial interface with block diagram? (NOV 2010)**

A **parallel port** is a type of interface found on [computers](http://en.wikipedia.org/wiki/Computers) ([personal](http://en.wikipedia.org/wiki/Personal_computer) and otherwise) for connecting various peripherals. In [computing](http://en.wikipedia.org/wiki/Computing), a parallel port is a [parallel communication](http://en.wikipedia.org/wiki/Parallel_communication) physical interface. It is also known as a **printer port** or [Centronics port](http://en.wikipedia.org/wiki/Centronics#The_interface). The [IEEE 1284](http://en.wikipedia.org/wiki/IEEE_1284) standard defines the bi-directional version of the port, which allows the transmission and reception of data bits at the same time.

* + **Compatibility Mode**, also known as Centronics standard or **SPP**, is a uni-directional implementation with only a few differences from the original Centronics design. This mode is almost exclusively used for printers. The only signals that the printer can send back to the host are some fixed-meaning status lines that signal common error conditions, such as the printer running out of paper.
	+ **Enhanced Parallel Port** (**EPP**) is a half-duplex bi-directional interface designed to allow devices like printers, scanners, or storage devices to transmit large amounts of data while quickly being able to switch channel direction. EPP can provide up to 2 MByte/s bandwidth, approximately 15 times the speed achieved with normal parallel-port communication with far less CPU overhead.[[1]](http://en.wikipedia.org/wiki/IEEE_1284#cite_note-0)
	+ **Extended Capability Port** (**ECP**) is a half-duplex bi-directional interface similar to EPP, except that PC implementations use [direct memory access](http://en.wikipedia.org/wiki/Direct_memory_access) (usually ISA DMA on channel 3) to provide even faster data transfer than EPP by having the ISA DMA hardware and the parallel port interface hardware handle the work of transferring the data instead of letting the CPU do this work. Many devices that interface using this mode support [RLE](http://en.wikipedia.org/wiki/Run-length_encoding) compression. ECP can provide up to 2.5 MByte/s of bandwidth, which is the natural limit of 8-bit ISA DMA.[[2]](http://en.wikipedia.org/wiki/IEEE_1284#cite_note-1) An ECP interface on a PC can improve transfers to pre-IEEE-1284 printers as well,

by reducing the CPU load during the transfer ; however, the transfer in that case is unidirectional.

## What are the required components to build LAN

A Local Area Networks connects computers together to exchange data. Apart from the computers, and other devices like printers and faxes, a LAN has to have six essential components to function **Network Adapter**

A computer needs a network adapter to connect to a network. It converts computer data into electronic signals. It listens for silence on the network cable and applies the data to it when it has an opportunity. The network access element of its job is called Media Access Control, or MAC. The physical address of every computer on a network is called its MAC address. The MAC address is the network adapter's serial number. Most computers are shipped with the network adapter integrated into the motherboard. However, early PCs didn't include this function and computer owners had to buy it separately and fit it into an expansion slot on the motherboard. These were called "network cards" because they were sold on a separate card. Although network adapters are now integrated, the name network card is still used. The wireless equivalent is called a Wireless Network .

## Network Medium

Wired networks need cable. The most common form of cable used in networks is called the "Unshielded Twisted Pair." In PC shops, it is generally just referred to as "network cable" or "Ethernet cable." Ethernet is the most widely implemented set of standards for the physical properties of networks. UTP is so closely identified with Ethernet that it is often given that name. Other cable types used for networks are twin-axial, Shielded Twisted Pair and single-mode and multi-mode fiber optic cable. Wireless networks don't need cable; they send data on radio waves generated by the WNIC.

## Cable Connectors

In wired networks, the most common form of connector is the RJ45. Every computer with networking capabilities has an RJ45 port. This is sometimes called a "network port" or an "Ethernet port." The RJ45 plug looks like a slightly larger telephone plug and connects the Unshielded Twisted Pair or the Shielded Twisted Pair cable.

## Power Supply

Both wired and wireless networks need a power supply. A wireless network uses the current to generate radio waves. A cabled network sends data interpreted as an electronic pulse.

## Hub/Switch/Router

In wired networks, one computer cannot connect to many others without some form of splitter. A hub is little more than a splitter. It repeats any signals coming into one of its ports out onto all its other ports. A cable leads from each port to one computer. A switch is a more sophisticated version of a hub. It only sends the signal on to the computer with the address written in the arriving message. Routers are much more complicated and are able to forward messages all over the world. Larger networks sometimes use routers for their LAN traffic. The wireless networking device is called a "wireless router."

## Network Software

Software on a communicating computer packages data into segments and puts that data into a structure called a "packet." The source and destination addresses of the packet are written into the header of the packet. The receiving computer needs to interpret these packets back into meaningful data and deliver it to the appropriate application.

## Explain briefly about Wired and Wireless Networks.

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of

two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network

interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today. (Homenthelp.com)

The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify

which computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another. (Laudon)

The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.

Typically the range of a wired network is within a 2,000-foot- radius. The disadvantage of this is that data transmission over this

distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved. (Laudon)

## Wireless Networks

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows

for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi- fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.

An infrastructure wireless network consists of an access point or a base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity. (compnetworking.about.com)

There are four basic types of transmissions standards for wireless networking. These types are produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.

The basic differences between these four types are connection speed and radio frequency.

802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions. (Wi-fi.com)

Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency. Usually if your wireless range is compromised considerably, more than likely, interference is to blame. (Laudon)

A major cause of interference with any radio signals are the materials in your surroundings, especially metallic substances, which have a tendency to reflect radio signals. Needless to say, the potential sources of metal around a home are numerous--things like metal studs, nails, building insulation with a foil backing and even lead paint can all possibly reduce the quality of the wireless radio signal. Materials with a high density, like concrete, tend to be harder for radio signals to penetrate, absorbing more of the energy. Other devices utilizing the same frequency can also result in interference with your wireless. For example, the 2.4GHz frequency used by 802.11b-based wireless products to communicate with each other. Wireless devices don't have this frequency all to themselves. In a business environment, other devices that use the 2.4GHz band include microwave ovens and certain cordless phones. (Laundon)

On the other hand, many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency

from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed will be slowed.

There are many benefits to a wireless network. The most important one is the option to expand your current wired network to other areas of your organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired network. (Wi-Fi.org) Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so.

## What is Bluetooth?

**Bluetooth** is a [wireless](https://en.wikipedia.org/wiki/Wireless) technology standard for exchanging data over short distances (using short- wavelength [UHF](https://en.wikipedia.org/wiki/UHF) [radio waves](https://en.wikipedia.org/wiki/Radio_waves) in the [ISM band](https://en.wikipedia.org/wiki/ISM_band) from 2.4 to 2.485 GHz) from fixed and mobile devices, and building [personal area networks](https://en.wikipedia.org/wiki/Personal_area_network) (PANs). Invented by telecom vendor [Ericsson](https://en.wikipedia.org/wiki/Ericsson) in 1994, it was originally conceived as a wireless alternative to [RS-232](https://en.wikipedia.org/wiki/RS-232) data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the [Bluetooth Special Interest Group](https://en.wikipedia.org/wiki/Bluetooth_Special_Interest_Group) (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics.[[6]](https://en.wikipedia.org/wiki/Bluetooth#cite_note-autogenerated1-6) The [IEEE](https://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers) standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks.[[7]](https://en.wikipedia.org/wiki/Bluetooth#cite_note-7) A manufacturer must make a device meet [Bluetooth SIG](https://en.wikipedia.org/wiki/Bluetooth_Special_Interest_Group#Qualification) [standards](https://en.wikipedia.org/wiki/Bluetooth_Special_Interest_Group#Qualification) to market it as a Bluetooth device[.[8]](https://en.wikipedia.org/wiki/Bluetooth#cite_note-8) A network of [patents](https://en.wikipedia.org/wiki/Patent) apply to the technology, which are licensed to individual qualifying devices.

## Explain the detail about network interface card (NIC) with neat diagram. (APR 2012)

A **network card**, **network adapter** or **NIC** (network interface controller) is a piece of [computer hardware](http://en.wikipedia.org/wiki/Computer_hardware) designed to allow computers to communicate over a [computer network](http://en.wikipedia.org/wiki/Computer_network). It is both an [OSI layer](http://en.wikipedia.org/wiki/OSI_model) 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of [MAC addresses](http://en.wikipedia.org/wiki/MAC_address). It allows users to connect to each other either by using cables or wirelessly.

Every network card has a unique 48-bit serial number called a [MAC address](http://en.wikipedia.org/wiki/MAC_address), which is stored in [ROM](http://en.wikipedia.org/wiki/Read-only_memory) carried on the card. Every computer on a network must have a card with a unique MAC address. No two cards ever manufactured share the same address. This is accomplished by the Institute of Electrical and Electronics Engineers ([IEEE](http://en.wikipedia.org/wiki/IEEE)), which is responsible for assigning unique MAC addresses to the vendors of network interface controllers.

Whereas network cards used to be [expansion cards](http://en.wikipedia.org/wiki/Expansion_card) that plug into a computer bus, the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the [motherboard.](http://en.wikipedia.org/wiki/Motherboard) These motherboards either have Ethernet capabilities integrated into the motherboard chipset, or implemented via a low cost dedicated Ethernet chip, connected through the [PCI](http://en.wikipedia.org/wiki/Peripheral_Component_Interconnect) (or the newer [PCI express](http://en.wikipedia.org/wiki/PCI_express) bus). A separate network card is not required unless multiple interfaces are needed or some other type of network is used. Even newer motherboards may have built-in dual network (Ethernet) interfaces.

The card implements the electronic circuitry required to communicate using a specific [physical layer](http://en.wikipedia.org/wiki/Physical_layer) and [data link layer](http://en.wikipedia.org/wiki/Data_link_layer) standard such as [Ethernet](http://en.wikipedia.org/wiki/Ethernet) or [token ring.](http://en.wikipedia.org/wiki/Token_ring) This provides a base for a full network [protocol stack](http://en.wikipedia.org/wiki/Protocol_stack), allowing communication among small groups of computers on the same [LAN](http://en.wikipedia.org/wiki/LAN) and large-scale network communications through routable protocols, such as [IP.](http://en.wikipedia.org/wiki/Internet_Protocol) There are four techniques used to transfer data, the NIC may use one or more of these techniques.

* + Polling is where the [microprocessor](http://en.wikipedia.org/wiki/Microprocessor) examines the status of the [peripheral](http://en.wikipedia.org/wiki/Peripheral) under program control.
	+ Programmed [I/O](http://en.wikipedia.org/wiki/I/O) is where the [microprocessor](http://en.wikipedia.org/wiki/Microprocessor) alerts the designated [peripheral](http://en.wikipedia.org/wiki/Peripheral) by applying its address to the system's [address bus](http://en.wikipedia.org/wiki/Address_bus).
	+ Interrupt-driven [I/O](http://en.wikipedia.org/wiki/I/O) is where the [peripheral](http://en.wikipedia.org/wiki/Peripheral) alerts the [microprocessor](http://en.wikipedia.org/wiki/Microprocessor) that it's ready to transfer data.
	+ DMA is where the intelligent [peripheral](http://en.wikipedia.org/wiki/Peripheral) assumes control of the [system bus](http://en.wikipedia.org/wiki/System_bus) to access memory directly. This removes load from the CPU but requires a separate processor on the card.

A network card typically has a [twisted pair](http://en.wikipedia.org/wiki/Twisted_pair), [BNC](http://en.wikipedia.org/wiki/BNC_connector), or [AUI](http://en.wikipedia.org/wiki/Attachment_Unit_Interface) socket where the network cable is connected, and a few [LEDs](http://en.wikipedia.org/wiki/Light-emitting_diode) to inform the user of whether the network is active, and whether or not there is data being transmitted on it. The Network Cards are typically available in 10/100/1000 [Mbits/s](http://en.wikipedia.org/wiki/Megabit_per_second)(Mbps). This means they can support a transfer rate of 10 or 100 or 1000 Megabits per second.

## Explain briefly about network topology.

Each computer on the network is connected to the other computers with cable (or some other medium, such as wireless using radio frequency signals). The physical arrangement of the cables connecting computers on a network is called the **network topology**.

The three basic topologies used in computer networks have been as follows:

* + **Bus—**Connects each computer on a network directly to the next computer in a linear fashion. The network connection starts at the server and ends at the last computer in the network.
	+ **Star—**Connects each computer on the network to a central access point.
	+ **Ring—**Connects each computer to the others in a loop or ring.

## Bus Topology

The earliest type of network topology was the bus topology, which uses a single cable to connect all the computers in the network to each other, as shown in the image below. This network topology was adopted initially because running a single cable past all the computers in the network is easier and uses less wiring than other topologies. Because early bus topology networks used bulky coaxial cables, these factors were important advantages. Both 10BASE-5 (thick) and 10BASE-2 (thin) Ethernet networks are based on the bus topology.

However, the advent of cheaper and more compact unshielded twisted-pair cabling, which also supports faster networks, has made the disadvantages of a bus topology apparent. If one computer or cable connection malfunctions, it can cause all the stations beyond it on the bus to lose their network connections. Thick Ethernet (10BASE-5) networks often failed because the vampire tap connecting the AUI device to the coaxial cable came loose.



A 10BASE-2 network is an example of a linear bus topology, attaching all network devices to a common cable.

In addition, the T-adapters and terminating resistors on a 10BASE-2 Thin Ethernet network could come loose or be removed by the user, causing all or part of the network to fail. Another drawback of Thin Ethernet (10BASE-2) networks was that adding a new computer to the network between existing computers might require replacement of the existing network cable between the computers with shorter segments to connect to the new computer’s network card and T-adapter, thus creating downtime for users on that segment of the network.

## Ring Topology

Another topology often listed in discussions of this type is a ring, in which each workstation is connected to the next and the last workstation is connected to the first again (essentially a bus topology with the two ends connected). Two major network types use the ring topology:

* **Fiber Distributed Data Interface (FDDI)**—A network topology used for large, high-speed networks using fiber-optic cables in a physical ring topology
* **Token-Ring**—Uses a logical ring topology

A Token-Ring network resembles a 10BASE-T or 10/100 Ethernet network at first glance because both networks use a central connecting device and a physical star topology. Where is the ―ring‖ in Token-Ring?

The ring exists only within the device that connects the computers, which is called a multistation access unit (MSAU) on a Token-Ring network (see the following image).



A Token-Ring network during the sending of data from one computer to another.

Signals generated from one computer travel to the MSAU, are sent out to the next computer, and then go back to the MSAU again. The data is then passed to each system in turn until it arrives back at the

computer that originated it, where it is removed from the network. Therefore, although the physical wiring topology is a star, the data path is theoretically a ring. This is called a logical ring.

A logical ring that Token-Ring networks use is preferable to a physical ring network topology because it affords a greater degree of fault tolerance. As on a bus network, a cable break anywhere in a physical ring network topology, such as FDDI, affects the entire network. FDDI networks use two physical rings to provide a backup in case one ring fails. By contrast, on a Token-Ring network, the MSAU can effectively remove a malfunctioning computer from the logical ring, enabling the rest of the network to function normally.

## Star Topology

By far the most popular type of topology in use today has separate cables to connect each computer to a **central wiring nexus**, often called a **switch** or **hub**. The following figure shows this arrangement, which is called a star topology.



The star topology, linking the LAN’s computers and devices to one or more central hubs, or access units.

Because each computer uses a separate cable, the failure of a network connection affects only the single machine involved. The other computers can continue to function normally. Bus cabling schemes use less cable than the star but are harder to diagnose or bypass when problems occur. At this time, Fast Ethernet and gigabit Ethernet in a star topology are the most commonly implemented types of wired LAN.

## What are the hardware requirements needs to form wireless Ethernet.

The most common type of network technology is wireless. When choosing network technology considers the location of the computer, speed of the network and the cost of these technologies are similar.

|  |  |
| --- | --- |
| Need | Purpose |
| DSL or Cable Modem | A DSL or cable modem connects your computer to a high-speed DSL or cable Internet connection. Although dial-up modems are still available for slower dial-up Internet connections, the connection speeds are far too slow for a home network. |
| Wired or wireless router | A wired or wireless router connects your DSL or cable modem to your home network. Many DSL/cable modems now have built-in routers that |

|  |  |
| --- | --- |
|  | allow you to connect your network directly to your Internet connection. |
| Wired or wireless network adapters | A wired or wireless network adapter is the device in your computer (or printers, gaming consoles, and other networking equipment) that connects your computer to your network. |
| Ethernet cabling | Ethernet cabling is used to connect your wired network adapters to a router or network switch. Even if you are using a wireless router, you will need at least one Ethernet cable to connect your wireless router to your DSL or cable modem. |

## What is access point and switch or Hub?

**Access Point (AP):**

1. Access points, also called as **Base Stations**, provide wireless access to a wired Ethernet network
2. An access point plugs into a hub, switch, or wired router and sends out wireless signals
3. This enables computers and devices to connect to a wired network wirelessly
4. Some routers are equipped with a wireless access point capability, in this case you don’t need a wireless access Point
5. Access points by themselves don't have any built-in technology for sharing Internet connections. To share an Internet connection, you must plug an access point into a router or a modem with a built- in router - this is what you get whenever you buy a wireless router

Remember, a hub or switch is just to create a network without any back-haul... By using a router, you connect to a back-haul.

## Hub:

1. Works within the same network - connect multiple computers within one network to each other
2. Each computer plugs into the hub with a cable, and information sent from one computer to another passes through the hub
3. A hub doesn't know have any information of who's sending info or requesting info and whom it is intended to. It can't identify the source or destination of the information it receives, so it sends the information to all of the computers connected to it, including the one that sent it
4. A hub can send or receive information but it can't do both at the same time, so hubs are the slowest and cheapest of all network devices, especially comparing with switches

## Switch:

1. Works within the same network - connect multiple computers within one network to each other
2. Each computer plugs into the switch with a cable, and information sent from one computer to another passes through the switch
3. A switch knows who's sending info or requesting info and whom it is intended to. So, it identifies the source and destination of the information it receives. So it intelligently sends the correct info to the right requester
4. Switches can send and receive information at the same time, and faster than hubs can
5. Switches are best recommended on a home or office network where you have more computers and want to use the network for activities that require passing a lot of information between computers

So, using only a hub or switch, you'll NOT be able to connect to the internet or go beyond your own network

## Router:

1. Routers are better known as intermediary devices that enable computers and other network components to communicate or pass information between two networks e.g. between a home network and the Internet
2. The wonderful thing about routers is their capability to direct network traffic, which is why, the name Router. Routers can be wired (using cables) or wireless
3. Routers also typically provide built-in security, such as a firewall
4. Routers are more expensive than hubs and switches

## Explain briefly about network Protocols.

When two humans converse, they may have to use the same language but they generally understand each other without having to adhere to rigid rules of grammar or formal language frameworks. Computers, on the other hand, have to have everything explicitly defined and structured. If computers wish to communicate with one another, they have to know in advance exactly how information is to be exchanged and precisely what the format will be. Therefore, standard methods of transmitting and processing various kinds of information are used and these methods are called "protocols". Protocols are established by international agreement and ensure that computers everywhere can talk to one another. There are a variety of protocols for different kinds of information and functions. This article will discuss some of the common protocols that the average PC user is likely to encounter.

## IP and TCP/IP

TCP (Transmission Control Protocol) and IP (Internet Protocol) are two different procedures that are often linked together. The linking of several protocols is common since the functions of different protocols can be complementary so that together they carry out some complete task. The combination of several protocols to carry out a particular task is often called a "stack" because it has layers of operations. In fact, the term "TCP/IP" is normally used to refer to a whole suite of protocols, each with different functions. This suite of protocols is what carries out the basic operations of the Web. TCP/IP is also used on many local area networks. The details of how the Web works are beyond the scope of this article but I will briefly describe some of the basics of this very important group of protocols. More details can be found in the references in the last section.

When information is sent over the Internet, it is generally broken up into smaller pieces or "packets". The use of packets facilitates speedy transmission since different parts of a message can be sent by different routes and then reassembled at the destination. It is also a safety measure to minimize the chances of losing information in the transmission process. TCP is the means for creating the packets, putting them back together in the correct order at the end, and checking to make sure that no packets got lost in transmission. If necessary, TCP will request that a packet be resent.

Internet Protocol (IP) is the method used to route information to the proper address. Every computer on the Internet has to have its own unique address known as the [IP address](http://vlaurie.com/computers2/Articles/Name.htm). Every packet sent will contain an IP address showing where it is supposed to go. A packet may go through a number of computer routers before arriving at its final destination and IP controls the process of getting everything to the designated computer. Note that IP does not make physical connections between computers but relies on TCP for this function. IP is also used in conjunction with other protocols that create connections.

## IPX/SPX

IPX/SPX and NetBEUI are two alternatives to TCP/IP for communication across a network. However, they are proprietary and limited in their use to networks running the software on each host. They are not used on the Internet at large, only on private LANs that have instigated them. IPX (Internetwork Packet Exchange) is a networking protocol from Novell that interconnects networks that use Novell's NetWare clients and servers. IPX is a datagram or packet protocol. IPX works at the network layer of communication protocols and is connectionless (that is, it doesn't require that a connection be set up before packets are sent to a destination as, for example, a regular voice phone call does). Packet acknowledgment is managed by another Novell protocol, the Sequenced Packet Exchange(tm) (SPX). Other related Novell NetWare protocols are: the Routing Information Protocol (RIP), the Service Advertising Protocol (SAP), and the NetWare Link Services Protocol(NLSP).

## NetBEUI

NetBEUI (NetBIOS Extended User Interface) is a new, extended version of NetBIOS, the program that lets computers communicate within a local area network. NetBEUI (pronounced net- BOO-ee) formalizes the frame format (or arrangement of information in a data transmission) that was not specified as part of NetBIOS. NetBEUI was developed by IBM for its LAN Manager product and has been adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. Hewlett-Packard and DEC use it in comparable products. NetBEUI is the best performance choice for communication within a single LAN. Because, like NetBIOS, it does not support the routing of messages to other networks, its interface must be adapted to other protocols such as IPX or TCP/IP. A recommended method is to install both NetBEUI and TCP/IP in each computer and set the server up to use NetBEUI for communication within the LAN and TCP/IP for communication beyond the LAN.

## Discuss about various types of cables and connectors. (NOV 2012)

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The types of cables used in networks are:

Unshielded Twisted Pair (UTP) Cable Shielded Twisted Pair (STP) Cable Coaxial Cable

Fiber Optic Cable

## Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.



Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

|  |  |  |
| --- | --- | --- |
| Category | Speed | Use |
| 1 | 1 Mbps | Voice Only (Telephone Wire) |
| 2 | 4 Mbps | LocalTalk & Telephone (Rarely used) |
| 3 | 16 Mbps | 10BaseT Ethernet |
| 4 | 20 Mbps | Token Ring (Rarely used) |
| 5 | 100 Mbps (2 pair) | 100BaseT Ethernet |
|  | 1000 Mbps (4 pair) | Gigabit Ethernet |
| 5e | 1,000 Mbps | Gigabit Ethernet |
| 6 | 10,000 Mbps | Gigabit Ethernet |

## Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



RJ-45 connector

## Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in

extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations: Each pair of wires is individually shielded with foil.

There is a foil or braid shield inside the jacket covering all wires (as a group).

There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

## Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

## Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T- connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.



BNC connector

## Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.



Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification Cable Type

10BaseT Unshielded Twisted Pair

10Base2 Thin Coaxial

10Base5 Thick Coaxial

100BaseT Unshielded Twisted Pair

100BaseFX Fiber Optic

100BaseBX Single mode Fiber

100BaseSX Multimode Fiber

1000BaseT Unshielded Twisted Pair

1000BaseFX Fiber Optic

1000BaseBX Single mode Fiber

1000BaseSX Multimode Fiber

## How to troubleshoot network problems?

Because of the variety of network hardware, network configurations, operating systems, and setups, not all of the below information may apply to your network or operating system.

## Adapter resources

Verify that the network adapter is properly installed and detected by the computer with no conflicts. In Microsoft Windows, open the [Device Manager](http://www.computerhope.com/jargon/d/devicema.htm) and verify there are no errors. "Network adapters" should be present for each network adapter installed in the computer, similar to the example on the right.

If conflicts exist or the network adapter is being detected as an "Other device", the network card has likely not been properly installed in the computer. Try letting Windows re-detect and install the network card by removing the network adapter and any other conflict devices from Device Manager and then rebooting the computer. If Windows re-detects the card but does not find the drivers, download the latest network card drivers from the computer manufacturer's website or the network card manufacturer's website.

## Verify connections Wired Network

If this is a wired network, verify that the network cable is properly connected and make sure the [LEDs](http://www.computerhope.com/jargon/l/led.htm) next to the network jack are properly illuminated. For example, a network card with a **solid** green LED or light usually indicates that the card is either connected or receiving a signal. If the green light is flashing, this is an indication of data being sent or received. The picture to the right is an example of a LAN port with two LED indicators next to the [RJ-45](http://www.computerhope.com/jargon/r/rj45.htm) port. With this port, one LED will light up if connected properly and the other will flash when transmitting data.



If there are no lights or the lights are orange or red, the card may be bad, not connected properly, or may not be receiving a signal from the network. If you are on a small or local network and have the capability of checking a [hub](http://www.computerhope.com/jargon/h/hub.htm), [switch](http://www.computerhope.com/jargon/s/switch.htm), or [router](http://www.computerhope.com/jargon/r/router.htm), verify that the cables are properly connected and that it has power. If after checking the connections, the LED indicators appear bad, the network adapter, port, or cable may be defective.

## Wireless Network

If you're using a laptop with a wireless network, look for the laptop's Wi-Fi button and make sure it is turned on. Many laptops have a Wi-Fi button that allows the wireless network to be turned on and off. The Wi-Fi button is often located just above the keyboard or on the front edge of the laptop, but it also may be integrated with a [F key](http://www.computerhope.com/jargon/f/funckeys.htm) as well. The pictures to the right are examples of a Wi-Fi button and Wi-Fi indicator on a F key that are enabled.

If the button is turned on, make sure you're using the correct Wi-F[i hotspot](http://www.computerhope.com/jargon/h/hotspot.htm) by right-clicking on the Network icon in the [Windows Notification Area](http://www.computerhope.com/jargon/n/notiarea.htm) and clicking "Connect to a network". Usually, the network with the strongest connection (the most bars) will be your wireless router.

Finally, when connecting to most wireless networks, you need to enter the proper [SSID](http://www.computerhope.com/jargon/s/ssid.htm) password to connect to the network. If the incorrect password has been entered, you will not be able to access the network.

## Adapter functionality

Verify that the network card is capable of pinging itself by using the [ping command](http://www.computerhope.com/jargon/p/ping.htm). Windows users can ping the computer from a [Windows command line](http://www.computerhope.com/issues/chusedos.htm). Unix and Linux users can ping from the [shell](http://www.computerhope.com/jargon/s/shell.htm). To ping the card or the localhost, type either of the following commands:

ping 127.0.0.1

or ping localhost

Executing either of the above commands should get replies from the network card. If you receive an error, or the transmission fails, the network card is not physically installed into the computer correctly, has the incorrect or outdated drivers installed, or is defective.

Make sure the network card is physically installed in the computer correctly by removing it and re- inserting it again. Check the network card manufacturer's website for the latest drivers and install those drivers. If the network card is defective, it needs to be replaced.

## Connect to the router

If all of the above steps have been checked, and your network has a [router](http://www.computerhope.com/jargon/r/router.htm), make sure the computer can connect to the router by performing the below commands.

## Determine the routers address

Using the [ipconfig command](http://www.computerhope.com/ipconfig.htm) (or [ifconfig command](http://www.computerhope.com/unix/uifconfi.htm) for Linux), determine the router's address by looking at the Gateway address. Below are the steps for Microsoft Windows users. Linux users can substitute ipconfig for ifconfig.

* 1. [Open the Windows command line.](http://www.computerhope.com/issues/chusedos.htm)
	2. At the command prompt, type **ipconfig** and press Enter. You should see output similar to the example below.

Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . :

|  |  |  |
| --- | --- | --- |
| IP | Address. . . . . . . | . . . . . : 192.168.1.103 |
| Subnet | Mask . . . . . . | . . . . . : 255.255.255.0 |

## Default Gateway . . . . . . . . . : 192.168.1.1

The Default Gateway is the address of your router. Most home routers have a gateway address that starts with 192.168, like the address shown above. Assuming your gateway address is 192.168.1.1, attempt to ping the router to see if it can send and receive information by running the below command.

ping 192.168.1.1

If you get replies back from the router, the connection between your router and computer are good, and you ca[n skip to the next step](http://www.computerhope.com/issues/ch000445.htm#firewall).

If you do not receive any replies back from the router, either the router is not set up properly, or your connection between the router and the computer is not correct. Reset your router to make sure it is not a problem with your router by following the steps below.

1. Turn off the power to the computer and leave it off.
2. Unplug the power to you[r router](http://www.computerhope.com/jargon/r/router.htm) and [cable modem](http://www.computerhope.com/jargon/c/cablemod.htm) or [DSL modem](http://www.computerhope.com/jargon/d/dslmodem.htm).
3. Leave the power cables disconnected for 10-15 seconds and then plug in your modem and then your router again.
4. Finally, turn on your computer again and repeat this step to see if you can ping your router.

If you have a wireless network and followed the above steps, but cannot ping the router, turn the computer off again and connect the computer to the router using a network cable instead of wirelessly. If a wire also does not work, contact the manufacturer of the router for additional support or replacement.

## Firewall

If your computer network utilizes a [firewall,](http://www.computerhope.com/jargon/f/firewall.htm) make sure all required [ports](http://www.computerhope.com/jargon/p/port.htm) are open, especially port 80, which is the [HTTP](http://www.computerhope.com/jargon/h/http.htm) port. If possible, disable the firewall software or disconnect the computer from the firewall to make sure it is not causing the network problems.

## The Internet is not working

If you're able to ping the router, but are still unable to connect to the Internet, either your router is improperly configured, or the [ISP](http://www.computerhope.com/jargon/i/isp.htm) is having issues.

**Note:** Some ISPs, such as [Comcast](http://www.computerhope.com/comp/comcast.htm), require special software to be installed. Make sure any software included with your Modem or other hardware has been installed on at least one computer if you are setting up a new Internet connection.

If your Internet has been working but recently stopped working, give it a few minutes to make sure it is not a temporary outage. If after waiting a few minutes, you still have problems, and you have not already disconnected the power to your router and modem, follow the steps below.

1. Turn off the power to the computer and leave it off.
2. Unplug the power cable to your [router](http://www.computerhope.com/jargon/r/router.htm) and [cable modem](http://www.computerhope.com/jargon/c/cablemod.htm) or [DSL modem.](http://www.computerhope.com/jargon/d/dslmodem.htm)
3. Leave the power cables disconnected for 10-15 seconds, plug in your modem again, and then plug in your router again.
4. Finally, turn on your computer and see if you can ping your router.

If after following the above steps, the Internet is still not working, [open the Windows command line](http://www.computerhope.com/issues/chusedos.htm) and run the below command.

ping google.com

Running the above command should get a reply from Google. If you get a reply, this is an indication that the Internet is working, but you may be encountering a problem with the [Internet browser](http://www.computerhope.com/jargon/b/browser.htm) you are using to browse the Internet. Try an alternative browser, such as [Firefox](http://www.computerhope.com/jargon/f/firefox.htm) or [Chrome](http://www.computerhope.com/jargon/c/chrome.htm).

If you're getting no reply from Google, your router or modem is not reaching the Internet. If you have a router, make sure your router has [DHCP](http://www.computerhope.com/jargon/d/dhcp.htm) enabled and that the [WAN](http://www.computerhope.com/jargon/w/wan.htm) or [Gateway](http://www.computerhope.com/jargon/g/gateway.htm) address is the proper ISP address.

Finally, if trying the above steps has not helped, contact your [ISP](http://www.computerhope.com/jargon/i/isp.htm) to make sure there is no problem on their end and to assist you further with any special configurations.

## Additional troubleshooting

Another method of determining network issues is to use the [tracert command](http://www.computerhope.com/tracert.htm) if you are a Windows user or the [traceroute command](http://www.computerhope.com/unix/utracero.htm) if you are a Linux or Unix variant user. This command gives you an overview of each of the devices (routers) a packet travels ([hops](http://www.computerhope.com/jargon/h/hops.htm)) over a network and can give you an idea of where a problem exists in your network or outside of your network.

To use this command, you must be at the command line and type one of the below commands depending on your operating system.

tracert google.com or

traceroute google.com

If successful, you should begin to see each hop between the computer and network devices. When the connection fails, determine what device is causing the issue by reviewing the traceroute listing.

## List and explain the various test performed by POST sequence? (APR 2011), (NOV 2012)

When the computer's power is first turned on, the [CPU](http://www.webopedia.com/TERM/C/CPU.html) initializes itself, which is triggered by a series of [clock ticks](http://www.webopedia.com/TERM/C/clock_tick.html) generated by the system clock. Part of the CPU's initialization is to look to the system's [ROM](http://www.webopedia.com/TERM/R/ROM.html) BIOS for its first instruction in the startup program. The ROM BIOS stores the first instruction, which is the instruction to run the [power-on self test](http://www.webopedia.com/TERM/P/power_on_self_test.html) (POST), in a predetermined [memory address](http://www.webopedia.com/TERM/M/memory_address.html).

POST (Power-On Self-Test) is the diagnostic testing sequence that a computer's [basic input/output](http://whatis.techtarget.com/definition/BIOS-basic-input-output-system) [system](http://whatis.techtarget.com/definition/BIOS-basic-input-output-system) (or "starting program") runs to determine if the computer keyboard, [random access memory,](http://searchmobilecomputing.techtarget.com/definition/RAM) disk drives, and other hardware are working correctly.

If the necessary hardware is detected and found to be operating properly, the computer begins to [boot](http://searchwinit.techtarget.com/definition/boot). If the hardware is not detected or is found not to be operating properly, the BIOS issues an error message which may be text on the display screen and/or a series of coded beeps, depending on the nature of the problem. Since POST runs before the computer's video card is activated, it may not be possible to progress to the display screen. The pattern of beeps may be a variable numbers of short beeps or a mixture of long and short beeps, depending on what type of BIOS is installed.

The patterns of beeps contain messages about the nature of the problem detected. For example, if the keyboard is not detected, a particular pattern of beeps will inform you of that fact. An error found in the POST is usually fatal (that is, it causes current program to stop running) and will halt the boot process, since the hardware checked is absolutely essential for the computer's functions.

Once the POST has determined that all components are functioning properly and the CPU has successfully initialized, the BIOS looks for an OS to load.

## Explain about BIOS Services. BIOS:

ROM-BIOS is a set of programs built into the computer that perform the most basic, low level and intimate control and supervision operations for the computer. The basic purpose of the ROM- BIOS is to take care of the immediate needs of the computer’s hardware and to isolate all other programs from the details of how the hardware works. BIOS is partly software and partly hardware. It is a bridge between the computer hardware and other software.

## BIOS Services

ROM-BIOS is divided into three functional parts:

1. Startup routines
2. Service handling and
3. Hardware interrupt handling



## Startup routines:

The start-up-routines get the computer going when power is turned on. The main parts of start- up-routines are POST and initialization. POST (Power On Self Test) routines test that the computer is in good working order. The initialization involves routines like creating the interrupt vectors so that when interrupts occur, the computer switches to the proper interrupt-handling routine. Many of the parts of the computer need to have registers set, parameters loaded and other things done to get them in their ready-to-go condition. All these are handled by the initialization routine.

The last part of the start-up-routine. The boot-strap process involves the ROM-BIOS attempting to read a boot record from the beginning of a disk. The BIOS first tries drive A and if that doesn’t succeed it tries to read a boot record from the hard disk if the computer has a hard disk, and then hands over the control of the computer to the short program on the boot record. The boot program begins the process of loading DOS into the computer.

## Service handling:

The service handling routines are there to perform work for the programs. The programs may seek service request to clear the display screen, or to switch the screen from text mode to graphics mode or to read information from the disk or write information onto the printer. To carry out the service requests the ROM-BIOS has to work directly with the computer’s I/O devices.

## Hardware interrupt handling:

The hardware interrupt handling part takes care of the independent needs of the PC hardware. It operates separately, but in co-operation with the service handling portion. When a key is pressed on the keyboard, the keyboard raises an interrupt. The hardware interrupt routines service the interrupt and keep ready the character pressed. When out programs send a request to display the character, the service routine passes the request to the hardware interrupt handling routine. The character is then displayed. ROM BIOS services are organized in groups with each group having its own dedicated interrupt.

## What are the service routines provided by BIOS to handle mouse and printers? Explain. (NOV 2014)

**BIOS** [**interrupt**](http://en.wikipedia.org/wiki/Interrupt) **calls** are a facility that operating systems and application programs use to invoke the facilities of the [Basic Input/Output System](http://en.wikipedia.org/wiki/BIOS) on [IBM PC compatible](http://en.wikipedia.org/wiki/IBM_PC_compatible) computers. Traditionally, BIOS calls are mainly used by [MS-DOS](http://en.wikipedia.org/wiki/MS-DOS) programs and some other software such as [boot loaders](http://en.wikipedia.org/wiki/Boot_loader). BIOS only runs in the [real address mode (Real Mode)](http://en.wikipedia.org/wiki/Real_mode) of the x86 CPU, so programs that call BIOS either must also run in real mode or must switch from protected mode to real mode before calling BIOS and then switch back again. For this reason, modern [operating systems](http://en.wikipedia.org/wiki/Operating_system) that use the CPU in [Protected](http://en.wikipedia.org/wiki/Protected_Mode) [Mode](http://en.wikipedia.org/wiki/Protected_Mode) generally do not use the BIOS to support system functions, although some of them use the BIOS to probe and initialize hardware resources during their early stages of [booting](http://en.wikipedia.org/wiki/Booting).

In all computers, software instructions control the physical hardware (screen, disk, keyboard, etc.) from the moment the power is switched on. In a PC, the BIOS, preloaded in ROM on the mainboard, takes control immediately after the processor is reset, including during power-up or when a hardware reset button is pressed. The BIOS initializes the hardware, finds, loads and runs the boot program (usually, but not necessarily, an OS loader), and provides basic hardware control to the operating system running on the machine, which is usually an operating system but may be a directly booting single software application.

Many modern operating systems (such as newer versions of [Windows](http://en.wikipedia.org/wiki/Windows) and [Linux](http://en.wikipedia.org/wiki/Linux)) bypass the built-in BIOS interrupt communication system altogether, preferring to use their own software to control the attached hardware directly. The original reason for this was primarily that these operating systems run the processor in protected mode, whereas calling BIOS requires switching to real mode and back again, and switching to real mode is slow. However, there are also serious security reasons not to switch to real mode, and the BIOS code has limitations both in functionality and speed that motivate operating system designers to find a replacement for it. In fact, the speed limitations of the BIOS

made it common even in the MS-DOS era for programs to circumvent it in order to avoid its performance limitations, especially for video graphics display and fast serial communication. The problems with BIOS functionality include limitations in the range of functions defined, inconsistency in the subsets of those functions supported on different computers, and variations in the quality of BIOSes (i.e. some BIOSes are complete and reliable, others are abridged and buggy). By taking matters into their own hands and avoiding reliance on BIOS, operating system developers can eliminate some of the risks and complications they face in writing and supporting system software. On the other hand, by doing so those developers become responsible for providing "bare-metal" driver software for every different system or peripheral device they intend for their operating system to work with (or for inducing the hardware producers to provide those drivers). Thus it should be apparent that compact operating systems developed on small budgets would tend to use BIOS heavily, while large operating systems built by huge groups of software engineers with large budgets would more often opt to write their own drivers instead of using BIOS—that is, even without considering the compatibility problems of BIOS and protected mode.

For IBM's part, they provided all the information needed to use their BIOS fully or to directly utilize the hardware and avoid BIOS completely, when programming the early IBM PC models (prior to the PS/2). From the beginning, programmers had the choice of using BIOS or not, on a per-hardware- peripheral basis. Today, the BIOS in a new PC still supports most, if not all, of the BIOS interrupt function calls defined by IBM for the [IBM AT](http://en.wikipedia.org/wiki/IBM_AT) (introduced in 1984), along with many more newer ones, plus extensions to some of the originals (e.g. expanded parameter ranges). This, combined with a similar degree of hardware compatibility, means that most programs written for an IBM AT can still run correctly on a new PC today, assuming that the faster speed of execution is acceptable (which it typically is for all but games that use CPU-based timing). Despite the considerable limitations of the services accessed through the BIOS interrupts, they have proven extremely useful and durable to technological change.

## Purpose of BIOS calls

BIOS interrupt calls perform hardware control or I/O functions requested by a program, return system information to the program, or do both. A key element of the purpose of BIOS calls is abstraction— the BIOS calls perform generally defined functions, and the specific details of how those functions are executed on the particular hardware of the system are encapsulated in the BIOS and hidden from the program. So, for example, a program that wants to read from a hard disk does not need to know whether the hard disk is an [ATA,](http://en.wikipedia.org/wiki/Parallel_ATA) [SCSI](http://en.wikipedia.org/wiki/SCSI), or [SATA](http://en.wikipedia.org/wiki/SATA) drive (or in earlier days, an [ESDI](http://en.wikipedia.org/wiki/Enhanced_Small_Disk_Interface) drive, or an [MFM](http://en.wikipedia.org/wiki/Modified_Frequency_Modulation) or [RLL](http://en.wikipedia.org/wiki/Run_Length_Limited) drive with perhaps a Seagate [ST-506](http://en.wikipedia.org/wiki/ST-506) controller, perhaps one of the several [Western Digital](http://en.wikipedia.org/wiki/Western_Digital#1980s) controller types, or with a different proprietary controller of another brand). The program only needs to identify the number of the drive it wishes to access and the address of the sector it needs to read or write, and the BIOS will take care of translating this general request into the specific sequence of elementary operations required to complete the task through the particular disk controller hardware that is connected to that drive. The program is freed from needing to know how to control at a low level every type of hard disk (or display adapter, or port interface, or real-time clock peripheral) that it may need to access. This both makes programming operating systems and applications easier and makes the programs smaller, reducing the duplication of program code, as the functionality that is included in the BIOS does not need to be included in every program that needs it; relatively short calls to the BIOS are included there instead. (In operating systems where the BIOS is not used, service calls provided by the operating system itself generally fulfill the same function and purpose.)

The BIOS also frees computer hardware designers (to the extent that programs are written to use the BIOS exclusively) from being constrained to maintain exact hardware compatibility with old systems when designing new systems, in order to maintain compatibility with existing software. For example, the keyboard hardware on the [IBM PCjr](http://en.wikipedia.org/wiki/IBM_PCjr) works very differently than the keyboard hardware on earlier IBM PC models, but to programs that use the keyboard only through the BIOS, this difference is nearly invisible. (As a good example of the other side of this issue, a significant share of the PC programs in use at the time the PCjr was introduced did not use the keyboard through BIOS

exclusively, so IBM also included hardware features in the PCjr to emulate the way the [original IBM](http://en.wikipedia.org/wiki/IBM_Personal_Computer) [PC](http://en.wikipedia.org/wiki/IBM_Personal_Computer) and [IBM PC XT](http://en.wikipedia.org/wiki/IBM_Personal_Computer_XT) keyboard hardware works. The hardware emulation is not exact, so not all programs that try to use the keyboard hardware directly will work correctly on the PCjr, but all programs that use only the BIOS keyboard services will.)

In addition to giving access to hardware facilities, BIOS provides added facilities that are implemented in the BIOS software. For example, the BIOS maintains separate cursor positions for up to eight text display pages and provides for [TTY](http://en.wikipedia.org/wiki/Computer_terminal)-like output with automatic line wrap and interpretation of basic control characters such as carriage return and line feed, whereas the CGA- compatible text display hardware has only one global cursor and cannot automatically advance the cursor or interpret control characters.

## Keyboard

|  |  |
| --- | --- |
| Interrupt vector Description | Interrupt vector Description |
| 17h | Printer services |
|  | **AH** | **Description** |  |
| 00h | Print Character to Printer |  |
| 01h | Initialize Printer |  |
| 02h | Check Printer Status |  |

**Cursor Control**

* + Each display of the current time by INT 21h, function 9, will advance the cursor
		- If a new time is displayed, it appears at a different screen position
		- So, to view the time updated at the same screen position we must restore the cursor to its original position before we display the time
		- This is achieved by first determining the current cursor position; then, after each print string operation, we move the cursor back
	+ We use INT 10h, functions 2 and 3, to save the original cursor position and to move the cursor to its original position after each print string operation

## INT 10h, Function 2

*Described in I/O module, repeated here for convenience*

## Move Cursor

* + Input:
		- AH = 2
		- DH = new cursor row (0-24)
		- DL = new cursor column (0-79 for 80x25 mode)
		- BH = page number
	+ Output: none

## INT 10h, Function 3

*Described in I/O module, repeated here for convenience*

## Get Cursor Position and Size

* + Input:
		- AH = 3
		- BH = page number
	+ Output:
		- DH = cursor row
		- DL = cursor column
		- CH = cursor starting scan line
		- CL = cursor ending scan line

## Write short notes on the following the network interfaces: i) Ethernet ii) Token Ring. (NOV 2010)

**Token ring interfaces**

Cabling is generally IBM "Type-1" [shielded twisted pair](http://en.wikipedia.org/wiki/Twisted_pair), with unique [hermaphroditic connectors](http://en.wikipedia.org/wiki/Hermaphroditic_connector), commonly referred to as **IBM data connectors** in formal writing or colloquially as [**Boy George**](http://en.wikipedia.org/wiki/Boy_George) **connectors**. The connectors have the disadvantage of being quite bulky, requiring at least 3 x 3 cm panel space, and being relatively fragile. The advantages of the connectors being that they are genderless and have superior shielding over standard unshielded RJ45. Connectors at the computer were usually [DE-9](http://en.wikipedia.org/wiki/D-subminiature) female.

In later implementations of Token ring RJ45 connectors were used on both of the MAUs, CAUs and NICs; with many of the network cards supporting both RJ45 and DE-9 for backwards compatibility.

## Ethernet networking interface

Ethernet networking interface refers to a circuit board or card installed in a personal computer or workstation, as a network client. A networking interface allows a computer or mobile device to connect to a local area network (LAN) using Ethernet as the transmission mechanism.

There are many Ethernet standards that an Ethernet networking interface must comply with with varying transmission speeds and error correction types/rates available. Ethernet is a standard for the transmission of binary data and although the hardware characteristics are defined, it is hardware independent so an Ethernet networking interface can use all manner of transmission hardware from fiber optic, to co-axial copper to wireless, depending on the capabilities of the hardware that the interface is sending to/receiving from and the network transfer rates required.

## Explain parallel and serial interface with block diagram? (NOV 2010) parallel interface

A parallel interface refers to a multiline channel, each line capable of transmitting several bits of data simultaneously. Most commonly, personal computers (PCs) have at least one parallel interface for connecting a printer using a parallel port. In contrast, a "serial interface" uses a serial port, a single line capable of only transmitting one bit of data at a time; a computer mouse connection is a good example.

## Parallel Ports

A **parallel port** is a type of interface found on [computers](http://en.wikipedia.org/wiki/Computers) ([personal](http://en.wikipedia.org/wiki/Personal_computer) and otherwise) for connecting various peripherals. In [computing](http://en.wikipedia.org/wiki/Computing), a parallel port is a [parallel communication](http://en.wikipedia.org/wiki/Parallel_communication) physical interface. It is also known as a **printer port** or [Centronics port](http://en.wikipedia.org/wiki/Centronics#The_interface). The [IEEE 1284](http://en.wikipedia.org/wiki/IEEE_1284) standard defines the bi-directional version of the port, which allows the transmission and reception of data bits at the same time.

* + **Compatibility Mode**, also known as Centronics standard or **SPP**, is a uni-directional implementation with only a few differences from the original Centronics design. This mode is almost exclusively used for printers. The only signals that the printer can send back to the host are some fixed-meaning status lines that signal common error conditions, such as the printer running out of paper.
	+ **Enhanced Parallel Port** (**EPP**) is a half-duplex bi-directional interface designed to allow devices like printers, scanners, or storage devices to transmit large amounts of data while quickly being able to switch channel direction. EPP can provide up to 2 MByte/s bandwidth, approximately 15 times the speed achieved with normal parallel-port communication with far less CPU overhead.[[1]](http://en.wikipedia.org/wiki/IEEE_1284#cite_note-0)
	+ **Extended Capability Port** (**ECP**) is a half-duplex bi-directional interface similar to EPP, except that PC implementations use [direct memory access](http://en.wikipedia.org/wiki/Direct_memory_access) (usually ISA DMA on channel 3) to provide even faster data transfer than EPP by having the ISA DMA hardware and the parallel port interface hardware handle the work of transferring the data instead of letting the CPU do this work. Many devices that interface using this mode support [RLE](http://en.wikipedia.org/wiki/Run-length_encoding) compression. ECP can provide up to 2.5 MByte/s of bandwidth, which is the natural limit of 8-bit ISA DMA[.[2]](http://en.wikipedia.org/wiki/IEEE_1284#cite_note-1) An ECP interface on a PC can improve transfers to pre-IEEE-1284 printers as well, by reducing the CPU load during the transfer ; however, the transfer in that case is unidirectional.



Parallel Interface block diagram

## Serial Port



In serial transmission, bits are sent **sequentially** on the same channel (wire) which reduces costs for wire but also slows the speed of transmission. Also, for serial transmission, some overhead time is needed since bits must be assembled and sent as a unit and then disassembled at the receiver.

Serial transmission can be either synchronous or **asynchronous** . In synchronous transmission, groups of bits are combined into frames and frames are sent continuously with or without data to be transmitted. In asynchronous transmission, groups of bits are sent as independent units with start/stop flags and no data link synchronization, to allow for arbitrary size gaps between frames. However, start/stop bits maintain physical bit level synchronization once detected.

## Write short notes on: i) windows, ii) Unix, iii) Linux (NOV 2012)

1. **Windows**

**Microsoft Windows** is a metafamily of graphical operating developed, marketed, and sold by [Microsoft.](https://en.wikipedia.org/wiki/Microsoft) It consists of several families of operating systems, each of which cater to a certain sector of the computing industry. Active Windows families include [Windows NT](https://en.wikipedia.org/wiki/Windows_NT), [Windows](https://en.wikipedia.org/wiki/Windows_Embedded) [Embedded](https://en.wikipedia.org/wiki/Windows_Embedded) and [Windows Phone](https://en.wikipedia.org/wiki/Windows_Phone); these may encompass subfamilies, e.g. [Windows Embedded](https://en.wikipedia.org/wiki/Windows_Embedded_Compact) [Compact](https://en.wikipedia.org/wiki/Windows_Embedded_Compact)(Windows CE) or [Windows Server](https://en.wikipedia.org/wiki/Windows_Server).Defunct Windows families include[Windows](https://en.wikipedia.org/wiki/Windows_9x) [9x](https://en.wikipedia.org/wiki/Windows_9x) and [Windows Mobile](https://en.wikipedia.org/wiki/Windows_Mobile).

Microsoft introduced an [operating environment](https://en.wikipedia.org/wiki/Operating_environment) named *Windows* on November 20, 1985 as a graphical [operating system shell](https://en.wikipedia.org/wiki/Operating_system_shell) for [MS-DOS](https://en.wikipedia.org/wiki/MS-DOS)in response to the growing interest in [graphical user](https://en.wikipedia.org/wiki/Graphical_user_interface) [interfaces](https://en.wikipedia.org/wiki/Graphical_user_interface) (GUIs).Microsoft Windows came to [dominate](https://en.wikipedia.org/wiki/Dominance_%28economics%29) the world's [personal computer](https://en.wikipedia.org/wiki/Personal_computer)market with [over 90% market share,](https://en.wikipedia.org/wiki/Usage_share_of_operating_systems) overtaking [Mac OS](https://en.wikipedia.org/wiki/Mac_OS), which had been introduced in 1984. However, since 2012, it sells less than[Android,](https://en.wikipedia.org/wiki/Android_%28operating_system%29) which became the most popular operating system in 2014, when counting all of the computing platforms Windows runs on (same as Android); in 2014, the number of Windows device sold were less than 25% of Android devices sold.As of April 2014, the most recent versions of Windows for [personal computers](https://en.wikipedia.org/wiki/Personal_computer), [smart phones](https://en.wikipedia.org/wiki/Smartphone), [server computers](https://en.wikipedia.org/wiki/Server_%28computing%29) and [embedded](https://en.wikipedia.org/wiki/Embedded_system) [devices](https://en.wikipedia.org/wiki/Embedded_system) are respectively [Windows 8.1](https://en.wikipedia.org/wiki/Windows_8.1), [Windows Phone 8.1](https://en.wikipedia.org/wiki/Windows_Phone_8.1), [Windows Server 2012 R2](https://en.wikipedia.org/wiki/Windows_Server_2012_R2) and [Windows](https://en.wikipedia.org/wiki/Windows_Embedded_8) [Embedded 8.](https://en.wikipedia.org/wiki/Windows_Embedded_8) A specialized version of Windows runs on the [Xbox One](https://en.wikipedia.org/wiki/Xbox_One) [game console](https://en.wikipedia.org/wiki/Game_console).

The next version of Windows is [Windows 10](https://en.wikipedia.org/wiki/Windows_10) and is currently available as a [technical preview](https://en.wikipedia.org/wiki/Technical_preview); it is set for release for phones, tablets, laptops, and PCs on July 29, 2015. The next server version of Windows is[Windows Server 2016](https://en.wikipedia.org/wiki/Windows_Server_2016), which is expected to be released in early 2016.

## Unix

**Unix** is a family o[f multitasking,](https://en.wikipedia.org/wiki/Computer_multitasking) [multi user](https://en.wikipedia.org/wiki/Multiuser) computer [operating systems](https://en.wikipedia.org/wiki/Operating_system) that derive from the original [AT&T](https://en.wikipedia.org/wiki/American_Telephone_%26_Telegraph) Unix, developed in the 1970s at the [Bell Labs](https://en.wikipedia.org/wiki/Bell_Labs) research center by [Ken Thompson](https://en.wikipedia.org/wiki/Ken_Thompson), [Dennis Ritchie](https://en.wikipedia.org/wiki/Dennis_Ritchie), and others.

Initially intended for use inside the [Bell System,](https://en.wikipedia.org/wiki/Bell_System) AT&T licensed Unix to outside parties from the late 1970s, leading to a variety of both academic and commercial variants of Unix from vendors such as the [University of California, Berkeley](https://en.wikipedia.org/wiki/University_of_California%2C_Berkeley) ([BSD](https://en.wikipedia.org/wiki/Berkeley_Software_Distribution)), Microsoft ([Xenix](https://en.wikipedia.org/wiki/Xenix)), [IBM](https://en.wikipedia.org/wiki/IBM) ([AIX](https://en.wikipedia.org/wiki/AIX)) and [Sun](https://en.wikipedia.org/wiki/Sun_Microsystems) [Microsystems](https://en.wikipedia.org/wiki/Sun_Microsystems) ([Solaris](https://en.wikipedia.org/wiki/Solaris_%28operating_system%29)). AT&T finally sold its rights in Unix to [Novell](https://en.wikipedia.org/wiki/Novell) in the early 1990s, which then sold its Unix business to the [Santa Cruz Operation](https://en.wikipedia.org/wiki/Santa_Cruz_Operation) (SCO) in 1995,[[4]](https://en.wikipedia.org/wiki/Unix#cite_note-4) but the UNIX trademark passed

to the industry standards consortium [The Open Group](https://en.wikipedia.org/wiki/The_Open_Group), which allows the use of the mark for certified operating systems compliant with the [Single UNIX Specification.](https://en.wikipedia.org/wiki/Single_UNIX_Specification) Among these is [Apple](https://en.wikipedia.org/wiki/Apple%2C_Inc)'s [OS X,](https://en.wikipedia.org/wiki/OS_X) which is the Unix version with the largest installed base as of 2014.

From the power user's or programmer's perspective, Unix systems are characterized by a modular design that is sometimes called the "[Unix philosophy](https://en.wikipedia.org/wiki/Unix_philosophy)", meaning that the operating system provides a set of simple tools that each perform a limited, well-defined function, with a unified [file system](https://en.wikipedia.org/wiki/Unix_filesystem) as the main means of communication and a [shell](https://en.wikipedia.org/wiki/Unix_shell) scripting and command language to combine the tools to perform complex workflows. Aside from the modular design, Unix also distinguishes itself from its predecessors as the first [portable](https://en.wikipedia.org/wiki/Software_portability) operating system: almost the entire operating system is written in the [C programming language](https://en.wikipedia.org/wiki/C_%28programming_language%29) that allowed Unix to reach numerous platforms.

Many [clones of Unix](https://en.wikipedia.org/wiki/Unix-like) have arisen over the years, of which [Linux](https://en.wikipedia.org/wiki/Linux) is the most popular, having overtaken the popularity of "true" Unix on server platforms since its inception in the early 1990s.

## Linux

**Linux** is a [Unix-like](https://en.wikipedia.org/wiki/Unix-like) and mostly [POSIX](https://en.wikipedia.org/wiki/POSIX)-compliant computer [operating system](https://en.wikipedia.org/wiki/Operating_system) (OS) assembled under the model of [free and open-source software](https://en.wikipedia.org/wiki/Free_and_open-source_software)development and distribution. The defining component of Linux is the [Linux kernel](https://en.wikipedia.org/wiki/Linux_kernel) an [operating system kernel](https://en.wikipedia.org/wiki/Kernel_%28computing%29) first released on 5October 1991 by [Linus](https://en.wikipedia.org/wiki/Linus_Torvalds) [Torvalds](https://en.wikipedia.org/wiki/Linus_Torvalds) The [Free Software Foundation](https://en.wikipedia.org/wiki/Free_Software_Foundation) uses the name [*GNU*](https://en.wikipedia.org/wiki/GNU)*/Linux* to describe the operating system, which has led to some [controversy.](https://en.wikipedia.org/wiki/GNU/Linux_naming_controversy)

Linux was originally developed as a free operating system for [personal computers](https://en.wikipedia.org/wiki/Personal_computer) based on the [Intel](https://en.wikipedia.org/wiki/Intel_x86) [x86](https://en.wikipedia.org/wiki/Intel_x86) architecture, but has since been [ported](https://en.wikipedia.org/wiki/Porting) to more computer hardware platforms than any other operating system.[[13]](https://en.wikipedia.org/?title=Linux&amp;cite_note-14)Thanks to its dominance on [smart phones](https://en.wikipedia.org/wiki/Smartphone), [Android](https://en.wikipedia.org/wiki/Android_%28operating_system%29), which is built on top of the Linux kernel, has the [largest](https://en.wikipedia.org/wiki/Usage_share_of_operating_systems) [installed base](https://en.wikipedia.org/wiki/Installed_base) of all general-purpose operating systems. Linux, in its original form, is also the leading operating system on [servers](https://en.wikipedia.org/wiki/Server_%28computing%29) and other [big iron](https://en.wikipedia.org/wiki/Big_iron) systems such as [mainframe computers](https://en.wikipedia.org/wiki/Mainframe_computer) and [super computers](https://en.wikipedia.org/wiki/Supercomputer), but is used on only around 1.5% of [desktop](https://en.wikipedia.org/wiki/Desktop_computer) [computers.](https://en.wikipedia.org/wiki/Desktop_computer) Linux also runs on [embedded systems](https://en.wikipedia.org/wiki/Embedded_system), which are devices whose operating system is typically built into the [firmware](https://en.wikipedia.org/wiki/Firmware) and is highly tailored to the system; this includes mobile phones, [tablet computers](https://en.wikipedia.org/wiki/Tablet_computer), network[routers,](https://en.wikipedia.org/wiki/Router_%28computing%29) facility automation controls, televisions, [video game](https://en.wikipedia.org/wiki/Video_game_console) [consoles](https://en.wikipedia.org/wiki/Video_game_console)and [smart watches](https://en.wikipedia.org/wiki/Smart_watch).

The development of Linux is one of the most prominent examples of [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source_software) [software](https://en.wikipedia.org/wiki/Free_and_open-source_software) collaboration. The underlying [source code](https://en.wikipedia.org/wiki/Source_code) may be used, modified, and distributed— commercially or non-commercially—by anyone under licenses such as the [GNU General Public](https://en.wikipedia.org/wiki/GNU_General_Public_License) [License.](https://en.wikipedia.org/wiki/GNU_General_Public_License) Typically, Linux is [packaged](https://en.wikipedia.org/wiki/Package_management_system) in a form known as a [*Linux distribution*](https://en.wikipedia.org/wiki/Linux_distribution), for both desktop and server use. Some popular mainstream Linux distributions include [Debian](https://en.wikipedia.org/wiki/Debian_%28operating_system%29), [Ubuntu](https://en.wikipedia.org/wiki/Ubuntu_%28operating_system%29)[,Linux](https://en.wikipedia.org/wiki/Linux_Mint) [Mint](https://en.wikipedia.org/wiki/Linux_Mint), [Fedora,](https://en.wikipedia.org/wiki/Fedora_%28operating_system%29) [openSUSE](https://en.wikipedia.org/wiki/OpenSUSE), [Arch Linux](https://en.wikipedia.org/wiki/Arch_Linux), and the commercial [Red Hat Enterprise Linux](https://en.wikipedia.org/wiki/Red_Hat_Enterprise_Linux) and [SUSE](https://en.wikipedia.org/wiki/SUSE_Linux_Enterprise_Server) [Linux Enterprise Server.](https://en.wikipedia.org/wiki/SUSE_Linux_Enterprise_Server) Linux distributions include the Linux kernel, supporting [utilities](https://en.wikipedia.org/wiki/System_software) and [libraries](https://en.wikipedia.org/wiki/Library_%28computer_science%29) and usually a large amount of application software to fulfill the distribution's intended use.

Distributions [oriented toward desktop use](https://en.wikipedia.org/wiki/Desktop_Linux) typically include [X11](https://en.wikipedia.org/wiki/X11), a [Wayland](https://en.wikipedia.org/wiki/Wayland_%28display_server_protocol%29) implementation or [Mir](https://en.wikipedia.org/wiki/Mir_%28software%29) as the [windowing system,](https://en.wikipedia.org/wiki/Windowing_system) and an accompanying [desktop environment](https://en.wikipedia.org/wiki/Desktop_environment) such as [GNOME](https://en.wikipedia.org/wiki/GNOME) or the [KDE Software Compilation](https://en.wikipedia.org/wiki/KDE_Software_Compilation). Some of such distributions may include a less resource intensive desktop such as [LXDE](https://en.wikipedia.org/wiki/LXDE) or[Xfce,](https://en.wikipedia.org/wiki/Xfce) for use on older or less powerful computers. Distributions intended to run on servers may omit all graphical environments from the standard install, and instead include other software to set up and operate a [solution stack](https://en.wikipedia.org/wiki/Solution_stack) such as[L AMP.](https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29) Because Linux is freely redistributable, anyone may create a distribution for any intended use.

## What is virus? List out the actions and its types. What are the precautions to be taken against virus? (NOV 2014)

A **computer virus** is a [malware](https://en.wikipedia.org/wiki/Malware) [program](https://en.wikipedia.org/wiki/Computer_program) that, when executed, [replicates](https://en.wikipedia.org/wiki/Self-replicating_program) by inserting copies of itself (possibly modified) into other [computer programs](https://en.wikipedia.org/wiki/Computer_programs), data [files](https://en.wikipedia.org/wiki/File_%28computing%29), or the [boot sector](https://en.wikipedia.org/wiki/Boot_sector) of the [hard drive](https://en.wikipedia.org/wiki/Hard_drive); when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing [hard disk](https://en.wikipedia.org/wiki/Hard_disk) space or [CPU](https://en.wikipedia.org/wiki/Central_processing_unit) time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, [logging their keystrokes,](https://en.wikipedia.org/wiki/Keystroke_logger) or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Virus writers use [social engineering](https://en.wikipedia.org/wiki/Social_engineering_%28security%29) and exploit detailed knowledge of [security vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_%28computing%29) to gain access to their hosts' computing resources. The vast majority of viruses target systems running [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade [antivirus software.](https://en.wikipedia.org/wiki/Antivirus_software) Motives for creating viruses can include seeking [profit,](https://en.wikipedia.org/wiki/Income) desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for [sabotage](https://en.wikipedia.org/wiki/Sabotage) and [denial of service,](https://en.wikipedia.org/wiki/Denial_of_service) or simply because they wish to explore [artificial life](https://en.wikipedia.org/wiki/Artificial_life) and [evolutionary algorithms](https://en.wikipedia.org/wiki/Evolutionary_algorithms).

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, source antivirus tools have been developed, and a multi-billion dollar industry of [antivirus software](https://en.wikipedia.org/wiki/Antivirus_software) vendors has cropped up, selling virus protection to users of various operating systems of which Windows is often the most victimized, partially due to its extreme popularity. No currently existing antivirus software is able to catch all computer viruses (especially new ones); computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

## Types of Virus Boot Sector Virus

The term ―boot sector‖ is a generic name that applied generally to the boot information used by any operating system that is on your Hard Drive. In modern computers this is usually called the ―master

boot record,‖ and it is the first sector on a partitioned storage device. Boot sector viruses became popular because of the use of floppy disks to boot a computer. The widespread usage of the Internet and the death of the floppy has made other means of virus transmission more effective. While not as popular as it once was it is still used.

## Browser Hijacker

This type of virus, which can spread itself in numerous ways including voluntary download, effectively hijacks certain browser functions, usually in the form of re-directing the user automatically to particular sites. It’s usually assumed that this tactic is designed to increase revenue from web advertisements. There are a lot of such viruses, and they usually have ―search‖ included somewhere in their description. A program called ―CoolWebSearch‖ may be the most well known example, but others are nearly as common.

## Direct Action Virus

This type of virus, unlike most, only comes into action when the file containing the virus is executed. The payload is delivered and then the virus essentially becomes dormant – it takes no other action unless an infected file is executed again. Most viruses do not use the direct action method of reproduction simply because it is not prolific, but viruses of this type have done damage in the past. The Vienna virus, which briefly threatened computers in 1988, is one such example of a direct action virus.

## File Infector Virus

Perhaps the most common type of virus, the file infector takes root in a host file and then begins its operation when the file is executed. The virus may completely overwrite the file that it infects, or may only replace parts of the file, or may not replace anything but instead re-write the file so that the virus is executed rather than the program the user intended. Although called a ―file virus‖ the definition doesn’t apply to all viruses in all files generally – for example, the macro virus below is not referred to by the file virus. Instead, the definition is usually meant to refer only to viruses which use an executable file format, such as .exe, as their host.

## Macro Virus

A wide variety of programs, including productivity applications like Microsoft Excel, provide support for Macros – special actions programmed into the document using a specific macro programming language. Unfortunately, this makes it possible for a virus to be hidden inside a seemingly harmless document. Macro viruses very widely in terms of payload. The most well known macro virus is probably a Word document supposedly containing the passwords to various websites. The virus also exploited Word’s link to Microsoft Outlook feature in order to automatically email copies of itself to others on your contact list.

## Multipartite Virus

While some viruses are happy to spread via one method or deliver a single payload, Multipartite viruses want it all. A virus of this type may spread in multiple ways, and it may take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files.

## Polymorphic Virus

Another jack-of-all-trades, the Polymorphic virus actually mutates over time or after every execution, changing the code used to deliver its payload. Alternatively, or in addition, a Polymorphic virus may guard itself with an encryption algorithm that automatically alters itself when certain conditions are met.The goal of this trickery is evasion. Antivirus programs often find viruses by the specific code used. Obscuring or changing the code of a virus can help it avoid detection.

## Resident Virus

This broad virus definition applies to any virus that inserts itself into a system’s memory. It then may take any number of actions and run independently of the file that was originally infected. A resident

virus can be compared to a direct payload virus, which does not insert itself into the system’s memory and therefore only takes action when an infected file is executed.

## Web Scripting Virus

Many websites execute complex code in order to provide interesting content. Displaying online video in your browser, for example, requires the execution of a specific code language that provides both the video itself and the player interface. Of course, this code can sometimes be exploited, making it possible for a virus to infect a computer or take actions on a computer through a website. Although malicious sites are sometimes created with purposely infected code, many such cases of virus exist because of code inserted into a site without the webmaster’s knowledge.

## Antivirus software

Many users install [antivirus software](https://en.wikipedia.org/wiki/Antivirus_software) that can detect and eliminate known viruses when the computer attempts to [download](https://en.wikipedia.org/wiki/Downloading) or run the executable (which may be distributed as an email attachment, or on [USB flash drives,](https://en.wikipedia.org/wiki/USB_flash_drive_security#Malware_Infections) for example). Some antivirus software blocks known malicious web sites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to [patch](https://en.wikipedia.org/wiki/Patch_%28computing%29) [security vulnerabilities](https://en.wikipedia.org/wiki/Malware#Vulnerability_to_malware)("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest [threats](https://en.wikipedia.org/wiki/Threat_%28computer%29). The German [AV-TEST](https://en.wikipedia.org/wiki/AV-TEST) Institute publishes evaluations of antivirus software for Windows and Android.

Examples of Microsoft Windows [anti virus](https://en.wikipedia.org/wiki/Antivirus) and anti-malware software include the optional [Microsoft](https://en.wikipedia.org/wiki/Microsoft_Security_Essentials) [Security Essentials](https://en.wikipedia.org/wiki/Microsoft_Security_Essentials)(for Windows XP, Vista and Windows 7) for real-time protection, the [Windows](https://en.wikipedia.org/wiki/Windows_Malicious_Software_Removal_Tool) [Malicious Software Removal Tool](https://en.wikipedia.org/wiki/Windows_Malicious_Software_Removal_Tool) (now included with [Windows (Security) Updates](https://en.wikipedia.org/wiki/Windows_Update) on "[Patch](https://en.wikipedia.org/wiki/Patch_Tuesday) [Tuesday](https://en.wikipedia.org/wiki/Patch_Tuesday)", the second Tuesday of each month), and [Windows Defender](https://en.wikipedia.org/wiki/Windows_Defender) (an optional download in the case of Windows XP).[[49]](https://en.wikipedia.org/wiki/Computer_virus#cite_note-49) Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use). Some such free programs are almost as good as commercial competitors. Common [security vulnerabilities](https://en.wikipedia.org/wiki/Malware#Vulnerability_to_malware) are assigned[CVE](https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) [IDs](https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) and listed in the US [National Vulnerability Database](https://en.wikipedia.org/wiki/National_Vulnerability_Database). [Secunia PSI](https://en.wikipedia.org/w/index.php?title=Secunia&amp;action=edit&amp;redlink=1) is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it. [Ransomware](https://en.wikipedia.org/wiki/Ransomware_%28malware%29) and [phishing](https://en.wikipedia.org/wiki/Phishing) scam alerts appear as press releases on the [Internet Crime Complaint](https://en.wikipedia.org/wiki/Internet_Crime_Complaint_Center#External_links) [Center noticeboard.](https://en.wikipedia.org/wiki/Internet_Crime_Complaint_Center#External_links)

Other commonly used preventative measures include timely operating system updates, software updates, careful Internet browsing, and installation of only trusted software.[[53]](https://en.wikipedia.org/wiki/Computer_virus#cite_note-53) Certain browsers flag sites that have been reported to Google and that have been confirmed as hosting malware by Google.

There are two common methods that an antivirus software application uses to detect viruses, as described in [the antivirus software](https://en.wikipedia.org/wiki/Antivirus_software#Identification_methods) article. The first, and by far the most common method of virus detection is using a list of [virus signature](https://en.wikipedia.org/wiki/Virus_signature) definitions. This works by examining the content of the computer's memory (its [RAM](https://en.wikipedia.org/wiki/Random_Access_Memory), and [boot sectors](https://en.wikipedia.org/wiki/Boot_sector)) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a [database](https://en.wikipedia.org/wiki/Database) of known virus "signatures". Virus signatures are just strings of code that are used to identify individual viruses; for each virus, the antivirus designer tries to choose a unique signature string that will not be found in a legitimate program. Different antivirus programs use different "signatures" to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that

are detected by signatures in their most recent virus definition update, and not protected from new viruses (see "[zero-day attack](https://en.wikipedia.org/wiki/Zero-day_attack)").

A second method to find viruses is to use a [heuristic](https://en.wikipedia.org/wiki/Heuristic_%28computer_science%29) algorithm based on common virus behaviors. This method has the ability to detect new viruses for which antivirus security firms have yet to define a "signature", but it also gives rise to more[false positives](https://en.wikipedia.org/wiki/Antivirus_software#Problems_caused_by_false_positives) than using signatures. False positives can be disruptive, especially in a commercial environment.

## Recovery strategies and methods

One can also reduce the damage done by viruses by making regular [backups](https://en.wikipedia.org/wiki/Backup) of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time), read-only or not accessible for other reasons, such as using different [file systems](https://en.wikipedia.org/wiki/File_system). This way, if data is lost through a virus, one can start again using the backup (which will hopefully be recent).

If a backup session on [optical media](https://en.wikipedia.org/wiki/Optical_disc) like [CD](https://en.wikipedia.org/wiki/CD) and [DVD](https://en.wikipedia.org/wiki/DVD) is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the CD/DVD). Likewise, an operating system on a [bootable](https://en.wikipedia.org/wiki/Bootable) CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable [flash drives](https://en.wikipedia.org/wiki/Flash_drives).

## Virus removal

Many websites run by antivirus software companies provide free online virus scanning, with limited cleaning facilities (the purpose of the sites is to sell antivirus products). Some websites—like Google subsidiary [VirusTotal](https://en.wikipedia.org/wiki/VirusTotal).com—allow users to upload one or more suspicious files to be scanned and checked by one or more antivirus programs in one operation. Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non- commercial use). Microsoft offers an optional free antivirus utility called [Microsoft Security](https://en.wikipedia.org/wiki/Microsoft_Security_Essentials) [Essentials](https://en.wikipedia.org/wiki/Microsoft_Security_Essentials), a[Windows Malicious Software Removal Tool](https://en.wikipedia.org/wiki/Windows_Malicious_Software_Removal_Tool) that is updated as part of the regular Windows update regime, and an older optional anti-malware (malware removal) tool [Windows](https://en.wikipedia.org/wiki/Windows_Defender) [Defender](https://en.wikipedia.org/wiki/Windows_Defender) that has been upgraded to an antivirus product in Windows 8.

Some viruses disable [System Restore](https://en.wikipedia.org/wiki/System_Restore) and other important Windows tools such as [Task](https://en.wikipedia.org/wiki/Task_Manager) [Manager](https://en.wikipedia.org/wiki/Task_Manager) and [CMD.](https://en.wikipedia.org/wiki/CMD_%28Windows%29) An example of a virus that does this is CiaDoor. Many such viruses can be removed by [rebooting](https://en.wikipedia.org/wiki/Booting) the computer, entering Windows [safe mode](https://en.wikipedia.org/wiki/Safe_mode)with networking, and then using system tools or [Microsoft Safety Scanner.](https://en.wikipedia.org/wiki/Microsoft_Safety_Scanner) [System Restore](https://en.wikipedia.org/wiki/System_Restore) on [Windows Me](https://en.wikipedia.org/wiki/Windows_Me), [Windows XP](https://en.wikipedia.org/wiki/Windows_XP)[,Windows](https://en.wikipedia.org/wiki/Windows_Vista) [Vista](https://en.wikipedia.org/wiki/Windows_Vista) and [Windows 7](https://en.wikipedia.org/wiki/Windows_7) can restore the registry and critical system files to a previous checkpoint. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files and does not exist in previous restore points.

## What is the use Multimeter? Explain.

A **multimeter** or a **multitester** is an [electronicmeasuring instrument](http://en.wikipedia.org/wiki/Electronics) that combines several functions in one unit. The most basic instruments include an [ammeter,](http://en.wikipedia.org/wiki/Ammeter) [voltmeter](http://en.wikipedia.org/wiki/Voltmeter), and [ohmmeter](http://en.wikipedia.org/wiki/Ohmmeter).

Analog multimeters are sometimes referred to as "volt-ohm-meters", abbreviated **VOM**. Digital multimeters are usually referred to as "digital-multi-meters", abbreviated **DMM**.

A multimeter can be a handheld device useful for basic fault finding and field service work or a bench instrument which can measure to seven or eight and a half digits of accuracy. Such an instrument will commonly be found in a calibration lab and can be used to characterise resistance and voltage standards or adjust and verify the performance of multi-function calibrators.



*A Digital Multimeter*

Current, voltage, and resistance measurements are considered standard features for multimeter. [AVO](http://en.wikipedia.org/wiki/Avometer) multimeters, a manufacturer of early multimeters, derived their name from amperes, volts, and ohms, the units used for the measurement of [current](http://en.wikipedia.org/wiki/Current_%28electricity%29), [voltage](http://en.wikipedia.org/wiki/Volt), and [resistance](http://en.wikipedia.org/wiki/Electrical_resistance).



*A Low Cost Digital Multimeter*



*An Analog Multimeter*

Newer equipment can measure many other quantities. Some common additional measured quantities and the units in which they are measured:

* + [Inductance](http://en.wikipedia.org/wiki/Inductor) in [henrys.](http://en.wikipedia.org/wiki/Henry_%28inductance%29)
	+ [Capacitance](http://en.wikipedia.org/wiki/Capacitor) in [farads.](http://en.wikipedia.org/wiki/Farad)
	+ [Conductance](http://en.wikipedia.org/wiki/Electrical_conductance) in [siemens.](http://en.wikipedia.org/wiki/Siemens_%28unit%29)
	+ [Temperature](http://en.wikipedia.org/wiki/Temperature) in degrees [Celsius](http://en.wikipedia.org/wiki/Celsius) or [Fahrenheit](http://en.wikipedia.org/wiki/Fahrenheit).
	+ [Frequency](http://en.wikipedia.org/wiki/Frequency) in [hertz](http://en.wikipedia.org/wiki/Hertz).
	+ [Duty cycle](http://en.wikipedia.org/wiki/Duty_cycle) as a [percentage.](http://en.wikipedia.org/wiki/Percentage)

A multimeter may be implemented with an analog meter deflected by an electromagnet, as a classic [galvanometer](http://en.wikipedia.org/wiki/Galvanometer); or with a digital display such as an [LCD](http://en.wikipedia.org/wiki/Liquid_crystal_display) or [Vacuum fluorescent display](http://en.wikipedia.org/wiki/Vacuum_fluorescent_display).

Analog multimeters are not hard to find in the used market, but are not very accurate because of errors introduced in zeroing and reading the analog meter face.

Analog meters may be implemented with vacuum tubes to precondition and amplify the input signal. Such meters are known as vacuum tube volt meters (VTVM) or vacuum tube multimeters (VTMM).

The resolution of a multimeter is often specified in "digits" of resolution. The term "digits" dates back to the 1970's when multimeter vendors were very proud of how many digits their products could display (this was important, because readout displays were costly). The vendors started to specify the maximum resolution of the multimeter based on the digital display. For example, the term 5½ digits refers to the number of digits displayed on the readout of a multimeter. A 5½ digit multimeter would have five full digits that display values from 0 to 9 and one half digit that could only display 0 or 1. This digital multimeter could show positive or negative values from 0 to 199,999. For a modern DMM, such as a PC-based multimeter, the term "digits" actual maps to the noise performance of the device.

Modern multimeters are exclusively digital, and identified by the term **DMM** or **digital multimeter**. In such an instrument, the signal under test is converted to a digital voltage and an amplifier with an electronically controlled gain preconditions the signal. Since the digital display directly indicates a quantity as a number, there is no risk of [parallax](http://en.wikipedia.org/wiki/Parallax) causing an error when viewing a reading.

Similarly, better circuitry and electronics have improved meter accuracy. Older analog meters might have basic accuracies of five to ten percent. Modern portable DMMs may have accuracies as good as ±0.025%, and bench-top instruments have accuracies in the single-digit parts per million figures.

The inclusion of solid state electronics, from a control circuit to small embedded computers, has provided a wealth of convenience features in modern digital meters. Commonly available measurement enhancements include:

* + Current-limited tests for voltage drop across [semiconductor junctions](http://en.wikipedia.org/wiki/P-n_junction). While not a replacement for a [transistor tester](http://en.wikipedia.org/wiki/Transistor_tester), this facilitates testing diodes and a variety of transistor types.
	+ A graphic representation of the quantity under test, as a bar graph. This makes go/no-go testing easy.
	+ A continuity tester that beeps when a circuit [conducts](http://en.wikipedia.org/wiki/Electrical_conduction).
	+ A low-bandwidth [oscilloscope.](http://en.wikipedia.org/wiki/Oscilloscope)
	+ A telephone test set.
	+ Automotive circuit testers, including tests for automotive timing and dwell signals.
	+ Simple data acquisition features to record maximum and minimum readings over a given period, or to take a number of samples at fixed intervals.
	+ Sample and hold, which will latch the most recent reading for examination after the instrument is removed from the circuit under test.
	+ Autoranging, which selects the correct range for the quantity under test without any risk of damaging the instrument.

Digital meters often feature circuitry or software to accurately measure AC voltages at any frequency. These meters integrate the input signal using the [root mean square](http://en.wikipedia.org/wiki/Root_mean_square) method, and will correctly read the true voltage of an input signal even if it isn't a perfect sine wave.

Modern meters may be interfaced with a [personal computer](http://en.wikipedia.org/wiki/Personal_computer) by [IrDA](http://en.wikipedia.org/wiki/Infrared_Data_Association) links, [RS-232](http://en.wikipedia.org/wiki/RS-232) connections, [USB,](http://en.wikipedia.org/wiki/USB) or an instrument bus such as [IEEE-488](http://en.wikipedia.org/wiki/IEEE-488). The interface allows the computer to record measurements as they are made or for the instrument to upload a series of results to the computer.

As modern appliances and systems become more complicated, the multimeter is becoming less common in the technician's toolkit. More complicated and specialized equipment replaces it. Where a service man might have used an ohmmeter to measure resistance while testing an antenna, a modern technician may use a hand-held analyzer to test several parameters in order to determine the integrity of a network cable.

## Describe the working principle of CRO with diagram? (NOV 2012), (NOV 2012)

An **oscilloscope** (sometimes abbreviated **CRO**, for [cathode-ray](http://en.wikipedia.org/wiki/Cathode-ray) oscilloscope, or commonly just **scope** or **O-scope**) is a piece of [electronic test equipment](http://en.wikipedia.org/wiki/Electronic_test_equipment) that allows signal voltages to be viewed, usually as a two-dimensional graph of one or more electrical [potential differences](http://en.wikipedia.org/wiki/Potential_difference) (vertical axis) plotted as a function of time or of some other voltage (horizontal axis).



Oscilloscope

## Features and uses Description

**Exterior**

A typical oscilloscope is usually box shaped with a display screen, numerous input connectors, control knobs and buttons on the front panel. To aid measurement, a grid called the *graticule* is drawn on the face of the screen. Each square in the graticule is known as a *division*.

## Inputs

The signal to be measured is fed to one of the input connectors, which is usually a coaxial connector such as a [BNC](http://en.wikipedia.org/wiki/BNC_connector) or [N type.](http://en.wikipedia.org/wiki/N_connector) If the signal source has its own coaxial connector, then a simple [coaxial cable](http://en.wikipedia.org/wiki/Coaxial_cable) is used; otherwise, a specialised cable called a ['scope probe'](http://en.wikipedia.org/wiki/Test_probe), supplied with the oscilloscope, is used. General-purpose oscilloscopes have a standardised input resistance of 1 [megohm](http://en.wikipedia.org/wiki/Ohm) in parallel with a capacitance of around 20 picofarads. This allows the use of standard oscilloscope probes. Scopes for use with very high frequencies may have 50-ohm inputs, which must be either connected directly to a 50-ohm signal source or used with Z0 or active probes. It is used for measuring voltage.

## The trace

In its simplest mode, the oscilloscope repeatedly draws a horizontal line called the *trace* across the middle of the screen from left to right. One of the controls, the *timebase control*, sets the speed at which the line is drawn, and is calibrated in [seconds](http://en.wikipedia.org/wiki/Second) per division. If the input voltage departs from zero, the trace is deflected either upwards or downwards. Another control, the *vertical control*, sets the scale of the vertical deflection, and is calibrated in [volts](http://en.wikipedia.org/wiki/Volt) per division. The resulting trace is a graph of voltage against time (the present plotted at a varying position, the less recent past to the left, the most recent past to the right).

If the input signal is periodic, then a nearly stable trace can be obtained just by setting the timebase to match the [frequency](http://en.wikipedia.org/wiki/Frequency) of the input signal. For example, if the input signal is a 50 [Hzsine](http://en.wikipedia.org/wiki/Hertz) wave, then its period is 20 ms, so the timebase should be adjusted so that the time between successive horizontal sweeps is 20 ms. This mode is called *continual sweep*. Unfortunately, an oscilloscope's timebase is not perfectly accurate, and the frequency of the input signal is not perfectly stable, so the trace will drift across the screen making measurements difficult.

## Trigger

To provide a more stable trace, modern oscilloscopes have a function called the *trigger*. When using *triggering*, the scope will pause each time the sweep reaches the extreme right side of the screen. The scope then waits for a specified event before drawing the next trace. The trigger event is usually the input waveform reaching some user-specified threshold voltage in the specified direction (going positive or going negative). The effect is to resynchronise the timebase to the input signal, preventing horizontal drift of the trace. In this way, triggering allows the display of periodic signals such as sine waves and square waves. Trigger circuits also allow the display of nonperiodic signals such as single pulses or pulses that don't recur at a fixed rate.

Types of trigger include:

* + *external trigger*, a pulse from an external source connected to a dedicated input on the scope.
	+ *edge trigger*, an edge-detector that generates a pulse when the input signal crosses a specified threshold voltage in a specified direction.
	+ *video trigger*, a circuit that extracts synchronising pulses from [video](http://en.wikipedia.org/wiki/Video) formats such as [PAL](http://en.wikipedia.org/wiki/PAL) and [NTSC](http://en.wikipedia.org/wiki/NTSC) and triggers the timebase on every line, a specified line, every field, or every frame. This circuit is typically found in a [waveform monitor](http://en.wikipedia.org/wiki/Waveform_monitor) device.
	+ *delayed trigger*, which waits a specified time after an edge trigger before starting the sweep. No trigger circuit acts instantaneously, so there is always a certain delay, but a trigger delay circuit extends this delay to a known and adjustable interval. In this way, the operator can examine a particular pulse in a long train of pulses.

## X-Y mode Other features

Some oscilloscopes have *cursors*, which are lines that can be moved about the screen to measure the time interval between two points, or the difference between two voltages. Oscilloscopes may have two or more input *channels*, allowing them to display more than one input signal on the screen. Usually the oscilloscope has a separate set of vertical controls for each channel, but only one triggering system and timebase.

Sometimes the event that the user wants to see may only happen occasionally. To catch these events, some oscilloscopes, known as "storage scopes", preserve the most recent sweep on the screen. This was originally achieved by using a special CRT, a "storage tube", which would retain the image of even a very brief event for a long time.

Some digital oscilloscopes can sweep at speeds as slow as once per hour, emulating a strip chart recorder. That is, the signal scrolls across the screen from right to left. Most oscilloscopes with this facility switch from a sweep to a strip-chart mode right around one sweep per ten seconds. This is because otherwise, the scope looks broken: it's collecting data, but the dot cannot be seen.

Oscilloscopes were originally analog devices. In more recent times digital signal sampling is more often used for all but the simplest models. Many oscilloscopes have different plug-in modules for different purposes, e.g., high-sensitivity amplifiers of relatively narrow bandwidth, differential amplifiers, amplifiers with 4 or more channels, sampling plugins for repetitive signals of very high frequency, and special-purpose plugins.

## What is the use Logic Analyzer? Explain.

A **logic analyzer** displays signals in a [digital circuit](http://en.wikipedia.org/wiki/Digital_circuit) that are too fast to be observed by a human being and presents it to a user so that the user can more easily check correct operation of the digital system. Logic analyzers are typically used for capturing data in systems that have too many channels to be examined with an [oscilloscope.](http://en.wikipedia.org/wiki/Oscilloscope) Software running on the logic analyzer can convert the captured data into timing diagrams, protocol decodes, state machine traces, assembly, or correlate assembly with source-level software.



*A* [*HP*](http://en.wikipedia.org/wiki/HP) *1615A Logic Analyzer (from 1980)showing a timing diagram.*



[*A Agilent*](http://en.wikipedia.org/wiki/Agilent) *16801A Logic Analyzer (from 2006)showing a timing diagram with imported scope signals.*

Current analyzers are either mainframes, which consist of a chassis containing the display, controls, control computer, and multiple slots into which the actual data capturing hardware is installed, or standalone units which integrate everything into a single package, with options installed at the factory. Recent mainframe models include the Agilent 16900 and Tek TLA7000, and recent standalone models include the Agilent 16800-series and Tek TLA5000.

Agilent and Tektronix make up over 95% of the industry's revenue.

## Operation

A logic analyzer can trigger on a complicated sequence of digital events, and then capture a large amount of digital data from the system under test (SUT). The best logic analyzers behave like software [debuggers](http://en.wikipedia.org/wiki/Debugger) by showing the flow of the [computer program](http://en.wikipedia.org/wiki/Computer_program) and decoding protocols to show messages and violations.

When logic analyzers first came into use, it was common to attach several hundred "clips" to a digital system. Later, specialized connectors came into use. The evolution of logic analyzer probes has led to a common footprint that multiple vendors support, which provides added freedom to end users. Since 2004, connectorless technology, known as Soft Touch, has become popular. These

probes provide a durable, reliable mechanical and electrical connection between the probe and the circuit board with less than 0.7 pF loading per signal.

Once the probes are connected, the user programs the analyzer with the names of each signal, and can group several signals into groups for easier manipulation. Next, a capture mode is chosen, either *timing* mode, where the input signals are sampled at regular intervals based on an internal or external clock source, or *state* mode, where one or more of the signals are defined as "clocks," and data is taken on the rising or falling edges of these clocks, optionally using other signals to qualify these clocks.

After the mode is chosen, a *trigger condition* must be set. A trigger condition can range from simple (such as triggering on a rising or falling edge of a single signal), to the very complex (such as configuring the analyzer to decode the higher levels of the TCP/IP stack and triggering on a certain HTTP packet).

At this point, the user sets the analyzer to "run" mode, either triggering once, or repeatedly triggering. Once the data is captured, it can be displayed several ways, from the simple (showing waveforms or state listings) to the complex (showing decoded Ethernet protocol traffic). The analyzer can also operate in a "compare" mode, where it compares each captured data set to a previously recorded data set, and stopping triggering when this data set is either matched or not. This is useful for long-term empirical testing. Recent analyzers can even be set to email a copy of the test data to

the engineer on a successful trigger.

## Uses

Many digital designs, including those of [ICs,](http://en.wikipedia.org/wiki/Integrated_circuit) are simulated to detect defects before the unit is constructed. The simulation usually provides logic analysis displays. Often, complex discrete logic is verified by simulating inputs and testing outputs using [boundary scan.](http://en.wikipedia.org/wiki/Boundary_Scan) Logic analyzers can uncover hardware defects that are not found in simulation. These problems are typically too difficult to model in simulation, or too time consuming to simulate and often cross multiple clock domains.

[Field-programmable gate arrays](http://en.wikipedia.org/wiki/Field-programmable_gate_array) have become a common measurement point for logic analyzers.

## What is the use In-Circuit Emulator? Explain.

An **in-circuit emulator** (ICE) also called **on-circuit debugger** (OCD) or **background debug module** (BDM) is a hardware device used to [debug](http://en.wikipedia.org/wiki/Debugger) the [software](http://en.wikipedia.org/wiki/Software) of an [embedded system](http://en.wikipedia.org/wiki/Embedded_system). Embedded systems present special problems for a programmer, because they usually lack keyboards, screens, disk-drives and other helpful user interfaces and storage devices that are present on business computers.

**In-circuit emulation** can also refer to the use of [hardware emulation](http://en.wikipedia.org/wiki/Hardware_emulation), when the emulator is plugged into a system (not always embedded) in place of a yet-to-be-built chip (not always a processor). These in-circuit emulators provide a way to run the system with "live" data while still allowing relatively good debugging capabilities.

## Function

The basic idea of an "in-circuit emulator" is that it provides a window into the embedded system. The programmer uses the emulator to load programs into the embedded system, run them, step through them slowly, and see and change the data used by the system's software.

An "emulator" gets its name because it often "emulates" the [central processing unit](http://en.wikipedia.org/wiki/Central_processing_unit) of the embedded system's computer. Often, it literally has a plug that plugs into the same socket as the CPU [chip](http://en.wikipedia.org/wiki/Integrated_circuit). Emulating the main computer lets it do anything that the main computer can do, but under the control of a programmer.

ICEs are always tools that attach a [terminal](http://en.wikipedia.org/wiki/Computer_terminal) or [PC](http://en.wikipedia.org/wiki/IBM_PC_clone) to the embedded system. The terminal or PC provides an interactive user interface for the programmer to investigate and control the embedded system.

Notably, when their program fails, most embedded systems simply become inert lumps of nonfunctioning electronics. Embedded systems often lack basic functions to detect signs of software failure, such as an [MMU](http://en.wikipedia.org/wiki/Memory_Management_Unit) to catch memory access errors. Without an ICE, the development of embedded systems can be extremely difficult, because there is usually no way to tell what went wrong. With an ICE, the programmer can usually test pieces of code, then isolate the fault to a particular failing piece of code, and then inspect the failing code and rewrite it to solve the problem.

In usage, an ICE provides the programmer with execution breakpoints, memory display & monitoring, and input/output control. Beyond this, the ICE can be programmed to look for any range of matching criteria to pause at, hopefully catching the failure's origin.

## Advantages

Virtually all embedded systems have a hardware element and a software element, which are separate but tightly interdependent. The ICE allows the software element to be run and tested on the actual hardware on which it is to run, but still allows programmer conveniences to help isolate faulty code, such as "source-level debugging" (which shows the program the way the programmer wrote it) and single-stepping (which lets the programmer run the program step-by-step to find errors).

Most ICEs consist of an adaptor unit that sits between the ICE host computer and the system to be tested. A header and cable assembly connects the adaptor to a socket where the actual [CPU](http://en.wikipedia.org/wiki/Central_processing_unit) or [microcontroller](http://en.wikipedia.org/wiki/Microcontroller) mounts within the embedded system. Recent ICEs enable a programmer to access the on-chip debug circuit that is integrated into the CPU via [JTAG](http://en.wikipedia.org/wiki/JTAG) in order to debug the software of an embedded system.

The ICE emulates the CPU. From the system's point of view, it has a real processor fitted, but from the programmer's point of view the system under test is under full control, allowing the developer to load, debug and test code directly.

Most host systems are ordinary commercial computers unrelated to the CPU used for development - for example, a [WindowsPC](http://en.wikipedia.org/wiki/Microsoft_Windows) might be used to develop software for a system using a [Freescale 68HC11](http://en.wikipedia.org/wiki/Freescale_68HC11) chip, which itself could not run Windows.

The programmer usually edits and compiles the embedded system's code on the host system, as well. The host system will have special compilers that produce executable code for the embedded system. These are called [cross compilers](http://en.wikipedia.org/wiki/Cross_compiler) or [cross assemblers.](http://en.wikipedia.org/wiki/Cross_assembler)

## Explain the diagnostic programs and troubleshooting tools in detail. (NOV 2010), (APR 2011)

1. **Describe the tools available for troubleshooting. (NOV 2014) Diagnostic Program**

A diagnostic program is a program written for the express purpose of locating problems with the software, hardware, or any combination there of in a system, or a network of systems. Preferably, diagnostic programs provide solutions to the user to solve issues.

* + Diagnostics that are run on-demand when a user needs assistance, typically within the primary operating system of the computer (e.g.Windows)
	+ "Off-line diagnostics" that are run outside the primary operating system, typically to reduce the masking influence of software on hardware issues
	+ Background diagnostics that monitor the system for failures and marginal events, and provide statistical data for failure prediction, and root cause analysis of actual failure conditions
	+ Solutions-oriented diagnostics, that diagnose and resolve user-perceived issues with a computer

system.

## Multimeter

A multimeter can be a handheld device useful for basic fault finding and field service work or a bench instrument which can measure to seven or eight and a half digits of accuracy. Such an instrument will commonly be found in a calibration lab and can be used to characterise resistance and voltage standards or adjust and verify the performance of multi-function calibrators.

## Oscilloscope

An **oscilloscope** (sometimes abbreviated **CRO**, for [cathode-ray](http://en.wikipedia.org/wiki/Cathode-ray) oscilloscope, or commonly just **scope** or **O-scope**) is a piece of [electronic test equipment](http://en.wikipedia.org/wiki/Electronic_test_equipment) that allows signal voltages to be viewed, usually as a two-dimensional graph of one or more electrical [potential differences](http://en.wikipedia.org/wiki/Potential_difference) (vertical axis) plotted as a function of time or of some other voltage (horizontal axis).

## Logic analyzer

A **logic analyzer** displays signals in a [digital circuit](http://en.wikipedia.org/wiki/Digital_circuit) that are too fast to be observed by a human being and presents it to a user so that the user can more easily check correct operation of the digital system. Logic analyzers are typically used for capturing data in systems that have too many channels to be examined with an [oscilloscope](http://en.wikipedia.org/wiki/Oscilloscope). Software running on the logic analyzer can convert the captured data into timing diagrams, protocol decodes, state machine traces, assembly, or correlate assembly with source-level software.

## In-Circuit Emulator (ICE)

An **in-circuit emulator** (ICE) also called **on-circuit debugger** (OCD) or **background debug module** (BDM) is a hardware device used to [debug](http://en.wikipedia.org/wiki/Debugger) the [software](http://en.wikipedia.org/wiki/Software) of an [embedded system](http://en.wikipedia.org/wiki/Embedded_system). Embedded systems present special problems for a programmer, because they usually lack keyboards, screens, disk-drives and other helpful user interfaces and storage devices that are present on business computers.

## Explain the various problems associated with the mother board. (APR 2011), (APR 2012), (NOV 2012)

1. **How to Trouble ShootPC problems? Justify. Troubleshooting Motherboard**

More than 70% of all computer problems are related to cabling and connections. Ensure all cables are connected and connected firmly. IDE and floppy ribbon cables and power cables can often go loose. Ensure microprocessor, memory modules, and adapters such as video card are inserted correctly and didn't "pop-up" due to vibration.

## System has no power at all. Power light does not illuminate, fan inside the power supply does not turn on, and indicator light on keyboard does not turn on.

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Power cable is unplugged. | Visually inspect power cable. | Make sure power cable is securely plugged in. |
| Defective power cable. | Visual inspection, try another cable. | Replace cable. |
| Power supply failure. | Power cable and wall socket are OK, but system is still dead. | Contact technical support |
| Faulty wall outlet;circuit breaker or fuse blown. | Plug device into socket know to work and test. | Use different socket, repair outlet, reset circuit breaker or replace fuse. |

**System inoperative. Keyboard lights are on, power indicator lights are lit, and hard drive is spinning.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Expansion card is partially dislodged from expansion slot on the motherboard. | Turn off computer. Take cover off system unit. Check all expansion cards to ensure they are securely seated in slots. | Using even pressure on both ends of the expansion card, press down firmly on expansion card. |
| Defective floppy disk drive or tape drive. | Turn system off. Disconnect the cables from one of the floppy drives. Turn on the system, check to see if the keyboard operates normally. Repeat until you have located defective unit. | Contact Technical Support. |
| Defective expansion card. | Turn computer off. Remove an expansion card. | Make sure expansion card is secure in expansion socket. |

**System does not boot from hard disk drive, can be booted from floppy disk drive.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Connector between hard drive and system board unplugged. | When attempting to run the FDISK utility described in the | Check cable running form disk to disk controller on the board. |

|  |  |  |
| --- | --- | --- |
|  | HARD DISK section of the manual you get a message, INVALID DRIVE SPECIFICATION. | Make sure both ends are securely plugged in; check the drive type in the Standard CMOS Setup (in your motherboard manual). |
| Damaged Hard Disk or Disk Controller. | Format hard disk; if unable to do so, the hard disk may be defective. | Contact Technical Support. |
| Hard Disk directory or FAT is scrambled. | Run the FDISK program, format the hard drive(See HARD DRIVE section of manual). Copy your backup data back onto hard drive. | Backing up the hard drive is extremely important. All Hard Disks are capable of breaking down at any time. |

**System only boots from Floppy Disk. Hard Disk can be read and applications can be used, but booting from Hard Disk is impossible.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Hard Disk boot program has been destroyed. | A number of causes could be behind this. | Back up data and applications files.Reformat the Hard Drive as described in the Hard Drive section of the manual. Re-install applications and data using backup disks. |

**Error message reading "SECTOR NOT FOUND" or other error messages indication certain data is not allowed to be retrieved.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| A number of causes could be behind this. | Use a file by file backup instead of an image backup to backup the Hard Disk. | Back up any salvageable data. Then do a low level format, partition, and high level format of the hard drive( see Hard Disk section of your manual for instructions). Re-install all saved data when completed. |

**Disk formatted on IBM PS/2 will not operate with this system.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| The IBM PS/2 uses a different format than other computers. | IBM PS/2 disk format will not work in an AT type computer. | Format disk in the AT type computer insert disk into the IBM PS/2 and copy the files you wish. |

**After install an expansion card (network card, tape drive card, etc.) the system no longer works properly.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| No power to monitor. | All or part of the system may be inoperable. The new card may work but a mouse or COM port may not work. | Change the interrupt or RAM address on the new expansion card. See the documentation that came with the new card in order to change pin settings. many expansion devices come with proprietary software that will assist you in doing this. |

**Screen message says "Invalid Configuration" or "CMOS Failure."**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |

|  |  |  |
| --- | --- | --- |
| Incorrect information entered into the configuration (setup) program. | Check the configuration program. Replace any incorrect information. | Review system's equipment. Make sure correct information is in setup. |

**Screen is blank.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| No power to monitor. | Power connectors may be loose or not plugged in. | Check the power connectors to monitor and to system. Make sure monitor is connected to display card, change I/O address on network card if applicable. |
| Monitor computer. | not | connected to |  | See instructions above. |
| Network conflict. | card | I/O address |  | See instructions above. |

**System does not boot from hard disk drive, can be booted from floppy disk drive.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Connector between hard drive and system board unplugged. | When attempting to run the FDISK utility described in the HARD DISK section of the manual you get a message, INVALID DRIVE SPECIFICATION. | Check cable running form disk to disk controller on the board. Make sure both ends are securely plugged in; check the drive type in the Standard CMOS Setup (in your |

**Problem**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Memory problem, display card jumpers not set correctly. |  | Reboot computer. Re-install memory, make sure that all memory modules are installed in correct sockets. Check jumper and switch settings on display card. See display card section for information of settings. |
| Computer virus. |  | Use anti-virus programs (McAfee/PC-cillin, E-port, etc) to detect and clean viruses. |

**Screen goes blank periodically.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Screen saver is enabled. |  | Disable screen saver. |

**Keyboard failure.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Keyboard is disconnected. |  | Reconnect keyboard. Check keys again, if no improvement, replace keyboard. |

**No color on screen.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Faulty Monitor. |  | If possible, connect monitor to another system. If no color, replace monitor. |
| CMOS incorrectly set up. |  | Call technical support. |

**Floppy drive lights stays on.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
|  |  |  |  | Reconnect floppy cable making |
| Floppy Drive | cable | not | sure PIN1 on the Floppy Drive |
| connected correctly. |  |  | corresponds with PIN1 on floppy |
|  |  |  | cable connector. |

**Error reading drive A:**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Bad floppy disk. |  | Try new floppy disk. |
| Floppy disk not formatted |  | Format floppy disk(type ENTER) |

**C: drive failure.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| SETUP program does not have correct information. |  | Boot from drive A: using DOS system disk. Input correct information to SETUP program. |
| Hard Drive cable not connected properly. |  | Check Hard drive cable. |

**Cannot boot system after installing second hard drive.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Master/Slave jumpers not set correctly. |  | Set master /Slave jumpers correctly. |
|  |  | Run SETUP program and select |
| Hard Drives not compatible / | correct drive types. Call drive |
| different manufacturers. | manufactures for compatibility |
|  | with other drives. |

**Missing operating system on hard drive.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| CMOS setup has been changed. |  | Run setup and select correct drive type. |

**Certain keys do not function.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Keys jammed or defective. |  | Replace keyboard. |

**Keyboard is locked, no keys function.**

|  |  |  |
| --- | --- | --- |
| **PROBABLE CAUSE** | **DIAGNOSIS** | **SOLUTION** |
| Keyboard is locked. |  | Unlock keyboard |

**Pondicherry University Questions Unit – V**

1. What are the two types of computer for faults based on the frequency occurrence of the problem? **(NOV 2010)**
2. Categorize the type of trouble shooting tools? **(NOV 2010), (APR 2012), (NOV 2012)**
3. List some of the symptoms of computer faults? **(APR 2011)**
4. What are the four levels of troubleshooting approaches? **(APR 2011)**
5. What are the troubleshooting problems of CD-ROM drive? **(APR 2012)**
6. List out the different types of Hardware Interrupts? **(NOV 2012)**
7. Define Operating System? **(NOV 2012)**
8. What do you mean by spyware? **(NOV 2012)**
9. What are the major functions OS? **(NOV 2013)**
10. What is mean by network? **(NOV 2013)**
11. What is the use of logic probe? **(NOV 2014)**
12. What do you mean by Boot virus? **(NOV 2014)**

## PART B

1. Compare Serial Port Vs. Parallel Port (Ref.Pg.No.5,Qn.No.1)
2. Explain briefly about USB. (Ref.Pg.No.5,Qn.No.2)
3. Explain about RS232C. (Ref.Pg.No.12,Qn.No.3)
4. Explain briefly about Parallel Port. (Ref.Pg.No.13,Qn.No.4)
5. Describe the structure, operating modes and features of enhanced capabilities port. (NOV 2014) (Ref.Pg.No.13,Qn.No.5)
6. Explain parallel and serial interface with block diagram? (NOV 2010) (Ref.Pg.No.13,Qn.No.6)
7. What are the required components to build LAN (Ref.Pg.No.14,Qn.No.7)
8. Explain briefly about Wired and Wireless Networks. (Ref.Pg.No.15,Qn.No.8)
9. What is Bluetooth? (Ref.Pg.No.17,Qn.No.9)
10. Explain the detail about network interface card (NIC) with neat diagram. **(APR 2012)**

(Ref.Pg.No.17,Qn.No.10)

1. Explain briefly about network topology. (Ref.Pg.No.18,Qn.No.11)
2. What are the hardware requirements needs to form wireless Ethernet. (Ref.Pg.No.20,Qn.No.12)
3. What is access point and switch or Hub? (Ref.Pg.No.21,Qn.No.13)
4. Explain briefly about network Protocols. (Ref.Pg.No.22,Qn.No.14)
5. Discuss about various types of cables and connectors. **(NOV 2012)** (Ref.Pg.No.23,Qn.No.15)
6. How to troubleshoot network problems? (Ref.Pg.No.27,Qn.No.16)
7. List and explain the various test performed by POST sequence? **(APR 2011), (NOV 2012)**

(Ref.Pg.No.30,Qn.No.17)

1. Explain about BIOS Services. (Ref.Pg.No.31,Qn.No.18)
2. What are the service routines provided by BIOS to handle mouse and printers? Explain. **(NOV 2014)** (Ref.Pg.No.32,Qn.No.19)
3. Write short notes on the following the network interfaces: i) Ethernet ii) Token Ring. **(NOV 2010)** (Ref.Pg.No.35,Qn.No.20)
4. Explain parallel and serial interface with block diagram? **(NOV 2010)**

(Ref.Pg.No.35,Qn.No.21)

1. Write short notes on: i) windows, ii) Unix, iii) Linux **(NOV 2012)** (Ref.Pg.No.37,Qn.No.22)
2. What is virus? List out the actions and its types. What are the precautions to be taken against virus? **(NOV 2014)** (Ref.Pg.No.39,Qn.No.23)
3. What is the use Multimeter? Explain. (Ref.Pg.No.42,Qn.No.24)
4. Describe the working principle of CRO with diagram? **(NOV 2012), (NOV 2012)**

(Ref.Pg.No.45,Qn.No.25)

1. What is the use Logic Analyzer? Explain. (Ref.Pg.No.47,Qn.No.26)
2. What is the use In-Circuit Emulator? Explain. (Ref.Pg.No.49,Qn.No.27)
3. Explain the diagnostic programs and troubleshooting tools in detail. **(NOV 2010), (APR 2011)** (Ref.Pg.No.51,Qn.No.28)
4. Describe the tools available for troubleshooting. **(NOV 2014)** (Ref.Pg.No.51,Qn.No.29)
5. Explain the various problems associated with the mother board. **(APR 2011), (APR 2012), (NOV 2012)** (Ref.Pg.No.52,Qn.No.30)
6. How to Trouble ShootPC problems? Justify. (Ref.Pg.No.52,Qn.No.31)