

This is the Reference copy for the LECTURERS to conduct ONLINE Classes. - Maanyas MGB Publications

Kindly don't send this soft copy to the STUDENTS.

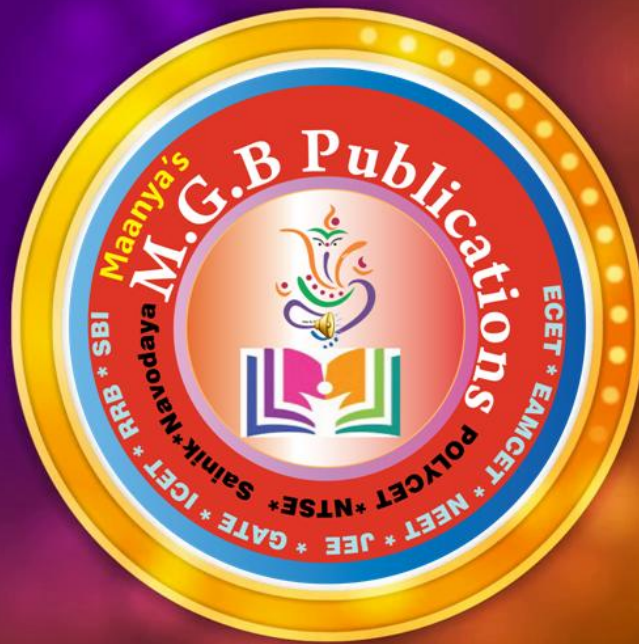
ECET -2021 STUDY MATERIALS & 20+ YEARS PREVIOUS PAPERS WITH SOLUTIONS

MPC	Objective Study Material ECET Objective Study Material MATHEMATICS VOL-1 & VOL-2 4900+ MCQs MAA Publications	Previous Question Papers ECET Previous Question Papers Physics & Chemistry 2018-2020 MAA Publications	Previous Question Papers ECET Previous Question Papers Mathematics Physics & Chemistry 2018-2020 MAA Publications	Previous Question Papers ECET Previous Question Papers Mechanical Engineering 3500 MCQs MAA Publications	MECHANICAL
	₹ 430 ₹ 780	₹ 320 ₹ 540	₹ 270 ₹ 450	₹ 110 ₹ 180	
	Objective Study Material POLY CET Objective Study Material Mathematics Objective Study Material MAA Publications	Objective Study Material POLY CET Objective Study Material Physics & Chemistry Objective Study Material MAA Publications	Previous Question Papers POLY CET Previous Question Papers Mathematics, Physics & Chemistry Previous Question Papers with Solutions MAA Publications	Objective Study Material ECET Objective Study Material Mechanical Engineering Volume 1 & 2 MAA Publications	
	₹ 430 ₹ 780			₹ 430 ₹ 780	
EECE	Previous Question Papers ECET Previous Question Papers Electronics & Communication Engg. 5000 MCQs MAA Publications	Objective Study Material ECET Objective Study Material Electronics & Communications Engg. Volume 1 & 2 MAA Publications	Previous Question Papers ECET Previous Question Papers CIVIL ENGINEERING 1700 MCQs MAA Publications	Objective Study Material ECET Objective Study Material CIVIL ENGINEERING Volume 1 & 2 MAA Publications	CIVIL
	₹ 130 ₹ 285	₹ 430 ₹ 780	₹ 105 ₹ 175	₹ 390 ₹ 680	
	Previous Question Papers ECET Previous Question Papers Electrical & Electronics Engg. 2400 MCQs MAA Publications	Objective Study Material ECET Objective Study Material Electrical & Electronics Engg. Volume 1 & 2 MAA Publications	Previous Question Papers ECET Previous Question Papers COMPUTER SCIENCE ENGG. 2000 MCQs MAA Publications	Objective Study Material ECET Objective Study Material Computer Science ENGINEERING Volume 1 & 2 MAA Publications	
	₹ 135 ₹ 280	₹ 430 ₹ 780	₹ 130 ₹ 285	₹ 390 ₹ 780	
COMBO OFFER					
MPC + Engg (PQP)		45% OFF	₹ 370	₹ 675	
MPC + Engg (OSM)		50% OFF	₹ 990	₹ 1980	
MPC (PQP + OSM)		45% OFF	₹ 940	₹ 1710	
ENGINEERING (PQP + OSM)		45% OFF	₹ 520	₹ 945	

MAANYA'S MGB Publications

All SEMESTER **TEXTBOOKS** are available for the **STUDENTS** at **FREE** of **COST** in our **MOBILE APP**

Hyderabad: 9290429549 & Tirupati: 9000305079



For **FREE**

Study
Materials

Practice
Papers

Recorded Video
Lectures

Online
Exams

Download

Maanyas MGB



Publications

Mobile app



Computer Hardware & & Networking

Fourth Edition: Nov - 2018

© All Rights Reserved

Printing of books passes through many stages—writing, composing, proof reading, printing etc. We try our level best to make the book error-free. If any mistake has inadvertently crept in, we regret it and would be deeply indebted to those who point it out. We do not take any legal responsibility.

No part of this book may be reproduced, stored in any retrieval system or transmitted in any form by any means - electronic, mechanical photocopying, recording or otherwise without the prior written, permission of the author and publishers.

For Copies Please Contact

M.G.B Publications

Cell: 9000305079

Also Available at All Leading Book Shops

Acknowledgements

First of all, I would like to thank God, the almighty of giving me skills to write this book.

I am very thankful to **B.DEEPA** for giving me an opportunity to write this book.

The author wishes to express his deep sense of gratitude to **S. Ramesh, P.V.Subba Reddy, S.V. Subba Reddy, K.Amarnath, B.Srinivas, and G.Sumanasri,** for their keen interest and encouragement in bringing out this book.

I thank **P. Roopa Latha, P.C Pavan Kalyan, Nagraj, Prathusa, Indraja, D. Varaprasad, D.Anitha Kumari, and A.V. Venugopal, and D. Meghajyothi,** for their kind co-operation in preparation of this book.

I specially grateful to the great teacher **T. Sreehari** for his time to time, much needed, valuable guidance.

I wish to express my profound thanks to all those who helped in making this book a reality. Much needed moral support and encouragement is provided on numerous occasions by my whole family.

Finally, I wish to thank **N. Giri Babu** and the entire team of for bringing out this book in a short time with quality printing.

Any suggestions for the improvement of this book and inclusion of new topics will be acknowledged and appreciated.

(Author)

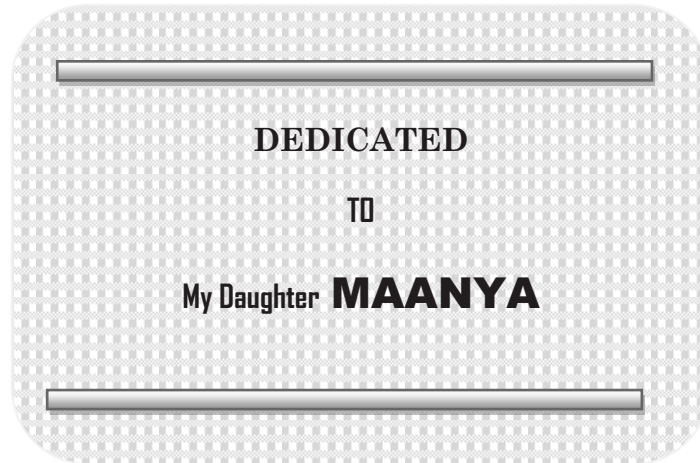


TABLE OF CONTENTS

Chapter Name	Page.No
1. BASIC COMPUTER HARDWARE	1-1 to 1-55
2. PC ASSEMBLY AND SOFTWARE INSTALLATION	2.1. to 2-46
3. BASICS OF DATA COMMUNICATION AND OSI REFERENCE MODEL	3.1. to 3-21
4. PHYSICAL LAYER AND DATA LINK LAYER	4-1 to 4-43
5. NETWORK LAYER, TRANSPORT LAYER AND APPLICATION LAYER	5-1 to 5-29

CHAPTER 1

BASIC COMPUTER HARDWARE

-: Objectives :-

On completion of the study of the chapter a student should be able to comprehend the following:

- 1.1. Draw the component layout of PC-AT motherboard and explain briefly about the function of each component
- 1.2. List different expansion slots available on the motherboard.
- 1.3. List the functions of chipsets.
- 1.4. List the important features of chipsets
- 1.5. Explain the specifications of processor
- 1.6. List the features of DDR2SDRAM and DDR3SDRAM
- 1.7. Explain accelerated graphics port.
- 1.8. List various SMPS power supply connectors used in PC-AT and explain their use
- 1.9. Give the connector details of serial port, mouse, keyboard and USB.
- 1.10. Give four reasons for popularity of USB ports
- 1.11. Explain the working of Hard Disk and data access.
- 1.12. List five specifications of LED monitor.
- 1.13. Explain the working of LED monitor.
- 1.14. Explain the working principle of optical mouse

1.0. UNDERSTAND MOTHERBOARD AND ITS FEATURES

- Motherboard is the most important part of any computer. It can be considered as the backbone of a computer.
- **Definition:** Motherboard is a printed circuit board on which all the electronic components of a PC are mounted.
- A motherboard is known as the main board, system board, logic board, main card, mother card, or mobo.
- A typical computer motherboard is shown in the fig. 1.0(a).

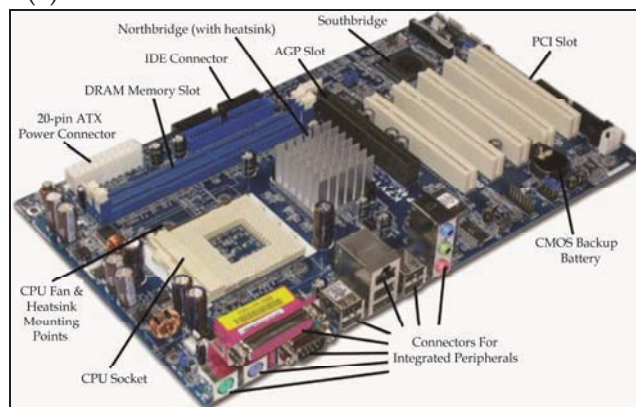


Fig. 1.0(a)

- The motherboard serves as a single platform to connect all of the parts of a computer together. All of the basic circuitry and components required for a computer to function are either contained in or attached to the motherboard.
- A motherboard connects CPU, memory, hard drives, optical drives, video card, sound card, and other ports and expansion cards directly or via cables.

-
- In other words, for all the PC's external devices, the motherboard functions like a central railway station. All traffic originates from or ends up in the motherboard.

1.1. DRAW THE COMPONENT LAYOUT OF PC-AT MOTHERBOARD AND EXPLAIN BRIEFLY ABOUT THE FUNCTION OF EACH COMPONENT

- Positions of various components that make up the motherboard are defined by the layout of the motherboard.
- The layout of components in a motherboard is very significant because this is one of the factors affecting the performance of the computer system.
- There are a large number of varieties in the motherboards. Among all of them, the two most widely used and popular motherboard configurations are **Baby AT** and **ATX**.
- Layout diagrams of a Baby AT motherboard and an ATX motherboard are shown in the figures 1.1(a) and 1.1(b) respectively.

The most important constituent components of both the motherboards shown in the figures 1.1(a) & (b) are listed below:

1. CPU
2. BIOS chip
3. RAM slots
4. CMOS ram
5. CMOS backup battery
6. Bus expansion slots
7. IDE, EIDE and SCSI connectors
8. Chipset
9. Onboard I/O connectors
10. Cache memory

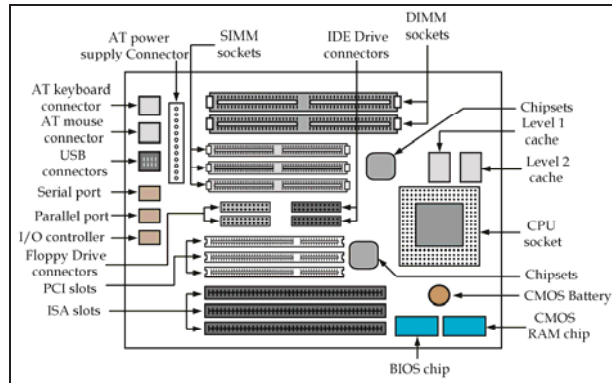


Fig. 1.1(a): Layout diagram of a Baby AT Motherboard

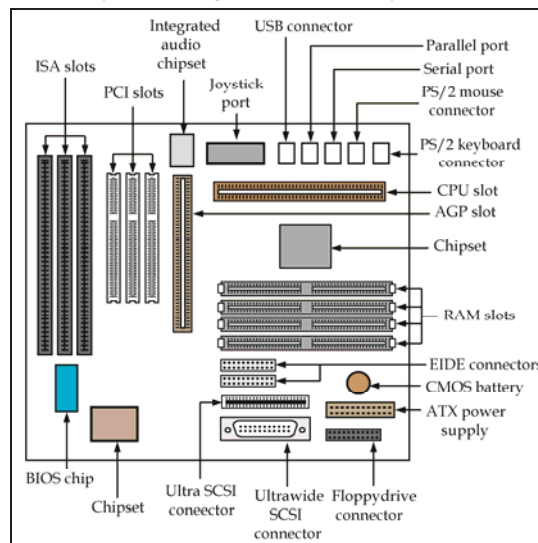


Fig. 1.1(b): Layout diagram of an ATX Motherboard

1. CPU

- The Central Processing Unit, also called the microprocessor performs all the calculations that take place inside a computer.
- It can be called the brain of the computer.

2. BIOS

- The BIOS is a ROM chip that contains some special programs that helps the computer processor interact and control the other components in the computer.
- These other components include disc drives, video cards, sound cards, network cards, floppy drives, USB ports, hard drives, and others.
- The BIOS chip also contains a program that performs all the basic functions necessary for a PC boot up.

3. RAM slots

- Random-Access Memory (RAM) stores programs and data currently being used by the CPU.
- RAM has been packaged in many different ways. The most current package is called a 168-pin DIMM (Dual Inline Memory module).
- DIMM RAMs are only used in ATX motherboards whereas Baby AT motherboards support both SIMM (Single Inline Memory module) and DIMM sockets.

4. CMOS RAM

- The CMOS (Complementary Metal Oxide Semiconductor)RAM chip is used to store information about the computer components, as well as settings for those components.

5. CMOS backup battery

- Normal RAM chips lose the information stored in them when power is no longer supplied to them.
- Therefore, to retain the information in the CMOS RAM chip, a lithium backup battery on the motherboard supplies constant power to the CMOS RAM chip.

6. Bus expansion slots

- System expansion is possible using the bus expansion slots. If you want to add a new device to computer other

than what is on the motherboard, you need an expansion slot.

- PCI slots, ISA slots and AGP slots shown in the layout diagrams are nothing but bus expansion slots.

7. IDE, EIDE, SCSI and SATA connectors

- These connectors are used to connect hard disk drives to the motherboard.

Note:

1. IDE (Integrated Digital Electronics) standard for hard disk drives is the oldest standard. It is seldom used now. This standard is also known as PATA (Parallel Advanced Technology Attachment) or simply ATA (Advanced Technology Attachment) standard.
2. EIDE (Enhanced IDE) standard is an improved version of IDE standard. This standard includes support for Direct Memory Access (DMA), multiple hard drives and CD-ROM drives.
3. SCSI (Small Computer System Interface) standard is used to connect hard disks to the motherboard in high-end PCs such as network servers or graphical workstations.
4. SATA (Serial Advanced Technology Attachment) is a new standard for connecting mass storage devices such as hard disk drives, optical drives, and solid-state drives to motherboard.

8. Chipset

- The chipset is a group of chips that helps the processor and other components on the PC communicate with and control all of the devices plugged into the motherboard.

9. Onboard I/O connectors

- Various I/O connectors available on the motherboard and their basic usage is given in the table 1.1.1.

I/O connector	Used to connect
Serial ports	Mouse, Modem etc
Parallel	Printers and other computers

ports	
PS/2 ports	Keyboard and mouse
VGA port	Monitor
USB ports	USB versions of many different devices such as mice, keyboards, scanners, cameras, and even printers are available
Table 1.1.1: Motherboard I/O connectors`	

10. Cache memory

- The cache is a fast memory which lies in between the CPU and RAM.
- The frequently used data is placed in cache memory.
- The memory access time of cache memory is very less. So, CPU can access it very fastly. Therefore, cache memory is used to improve the performance of the system.

***Note:**

1. Different motherboard manufactures use different layouts.
2. Motherboards used for different types of computer systems such as desktops, servers or laptops motherboards have different layouts.
3. An improper motherboard layout leads to certain signal integrity problems.

Additional Information

*** Types of Expansion Slots ***

Introduction

- We can boost the functionality and performance of a PC by connecting some more additional devices to the PC than what the PC is actually having now. To do this, we need an expansion slot.
- Expansion slot is the backbone of the computer. Without the expansion slots, computers will not be of much use.

- **Definition:** A socket on a computer motherboard where a [circuit board](#) can be inserted to add new capabilities to the computer is known as the Expansion slot.
- The circuit [boards](#) inserted into the expansion slots are called expansion cards or adapter cards or expansion board or [add-ins](#) or add-ons. A new device can be connected to your basic computer system using these expansion cards.
- Address, data and control buses on the motherboard are connected to different expansion cards through the expansion slots on the motherboard as shown in the fig. 1.1(a).

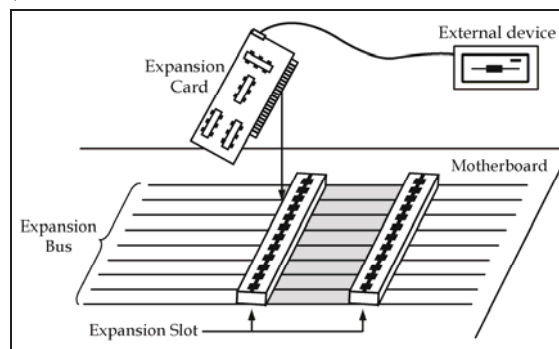


Fig. 1.1(b) : Expansion bus and Expansion slots on the motherboard

1.2. LIST DIFFERENT EXPANSION SLOTS AVAILABLE ON THE MOTHERBOARD.

The expansion slots are categorized according to the number of bits that they can transfer at a time and the bus architecture used. The different types of expansion slots available on the motherboard are listed below.

1. PCI Slots
2. AGP slots

3. PCIe slots
4. ISA slots
5. EISA slots
6. MCA slots
7. PCI-X slots
8. Mini PCI slots

Additional Information

A brief discussion on the above expansion slots is given below.

1. PCI slots

- PCI (Peripheral Component Interconnect) is an older standard which provides less bandwidth for expansion cards.
- These slots are seldom used now. But some new motherboards are still manufactured with PCI slots for compatibility purposes.
- PCI cards are still very common for expansion cards that do not need high bandwidth, such as most sound cards, network cards, USB expansion cards for additional connections, and more.
- Since newer motherboards still tend to come with PCI slots for compatibility, PCI cards will function on most computers.

2. AGP slots

- The AGP stands for Accelerated Graphics Port. As the name suggests, AGP slots are used for video cards.
- This standard was introduced when video cards needed more bandwidth for performance than was provided by PCI.

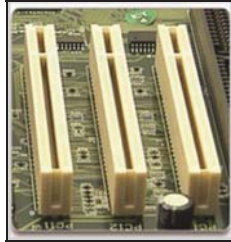


Fig 1.2 (c) :
PCI slots



Fig. 1.2(d) :
AGP slot



Fig. 1.2(e) :
PCIe slots

3. PCIe slots

- PCIe (PCI Express) is the newest standard for expansion cards on personal computers.
- PCI Express is meant to replace older standards like PCI and AGP.
- These slots provide significantly more bandwidth, allowing for higher performance video cards and network cards.
- Video cards, in particular, are the most common consumer use of these slots, since they need high bandwidth for maximum 3D gaming and graphics performance.

4. ISA slots

- ISA (Industry Standard Architecture) is an 8-bit or 16-bit expansion slot.
- It is the first bus architecture for PCs.
- It was the predecessor to PCI and you'll only find it only on much older computers. It is seldom used now.

5. EISA slots

- EISA (Extended Industry Standard Architecture) is a 32-bit expansion slot which is the extension to ISA slots.

- These slots are fully compatible with 8 bit or 16 bit ISA slots.
- These are also older technology and are seldom used.



Fig. 1.2(f) :
ISA slots



Fig. 1.2(g) :
EISA slot



Fig. 1.2(h) :
MCA slots

6. MCA slots

- MCA (Micro Channel Architecture) is a 32-bit expansion slot designed by IBM.
- MCA never became popular because of the two main reasons.
 - It is not compatible with its predecessor, ISA technology.
 - It is proprietary system, so other manufacturers cannot use this architecture.

7. PCIX slots

- PCIX (PCI-Extended) is a 32-bit bus slot with higher bandwidth than the PCI bus.
- PCI-X can run up to four times faster than PCI.
- PCIX slots are different from the PCIe slots in many aspects. The most important one is that the PCIX slots are backward compatible with PCI slots, whereas PCIe slots are not.

8. Mini PCI slots

- Mini PCI is a 32-bit expansion slot used by laptops.
- Mini PCI has three different form factors, Type I, Type II, and Type III.

Additional Information

* Chipsets *

(a) Introduction

- In the initial days, the motherboards used discrete integrated circuits. Therefore, many chips were needed to create all the necessary circuitry.
- After some time, chip manufacturers started to integrate several chips into larger chips. These big integrated chips are known as Chipsets. Instead of requiring dozens of small chips, a motherboard could now be built using only one or two big chips.
- **Definition :** The chipset is a group of chips that helps the processor and other components on the PC communicate with and control all of the devices plugged into the motherboard.
- Chipsets work in conjunction with the processors.
- These chips contain more than one logic like DMA logic, interrupt logic and peripheral interface logic.

(b) Advantages of Chipsets

1. Chipsets reduce chip count in a computer.
2. They reduce power requirements.
3. They shorten the signal paths and allow the circuits to operate at higher speeds.
4. They improve reliability.
5. They reduce construction cost.

1.3. LIST THE FUNCTIONS OF CHIPSETS.

The important functions of chipsets are:

1. The chipset controls the bits that flow between the CPU and devices.
2. It controls system memory.
3. It controls the motherboard's bus.
4. It also manages data transfers between the CPU, memory and peripheral devices.
5. It provides support for the expansion bus and any power management features of the system.

Additional Information

* Chipset Architectures *

- The most widespread chipset architecture consists of two chips, usually called the north and south bridges.
- This division applies to the most popular chipsets from VIA and Intel.
- The north bridge and south bridge are connected by a powerful bus, known as the link channel.
- The north bridge and south bridge share the work of managing the data traffic on the motherboard as shown in the fig. 1.3(a).

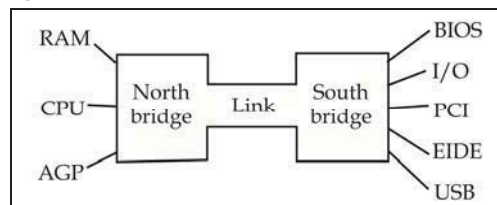


Fig. 1.3(a): North bridge & South bridge

1. **North Bridge:** The north bridge is a controller which controls the flow of data between the CPU and RAM, and to the AGP port.
2. **South Bridge:** The south bridge incorporates a number of different controller functions. It looks after the transfer of data to and from the hard disk and all the other I/O devices, and passes this data into the link channel which connects to the north bridge.

1.4. LIST THE IMPORTANT FEATURES OF CHIPSETS

The details of five Intel chipsets used with the Intel Celeron, Pentium II and Pentium IV processors are discussed in this section. They are

1. Intel 810 chipset
2. Intel 815 chipset
3. Intel 820 chipset
4. Intel 845 chipset
5. Intel 850 chipset

1. Intel 810 Chipset

- This is Intel's first chipset designed with a new hub architecture, called Accelerated hub architecture.
- This chipset is aimed at the Low-End market and has an integrated i740 graphics core, which should allow making low-cost all-in-one motherboards.
- This chipset is a high-integration chipset designed for the basic graphics/multimedia PC platform.
- The complete details of this chipset are given in the table 1.4.1



Fig. 1.4.1 (a) : INTEL 810 chipset

Parameter	Details
Processors supported	Pentium II/III Celeron processor
Multi processor support	No
Funcional blocks	1. 82810 G memory controller hub 2. 82801 I/O controller hub 3. 82802 Firmware hub
Memory support	512 MB memory
Bus support	PCI bus
Video and audio support	AGP 2.0 devices
I/O port support	1. Dual USB port 2. UDMA IDE controller

Table 1.4.1 : Details of INTEL 810 chipset

2. Intel 815 Chipset

- The Intel 815 chipset is an update of the successful 810 chip set.
- It holds an integrated graphics adapter as well as a lot of new functions.
- It is intended to optimize flexibility and stability in INTEL Celeron and INTEL Pentium III processor based PCs.

- It is designed using the same hub-based layout as the former 810 chipset.
- The complete details of this chipset are given in the table 1.4.(b)



Fig. 1.4.(b) : INTEL 815 chipset

Parameter	Details
Processors supported	Pentium III/Celeron processor
Multi processor support	No
Functional blocks	1. 82815 G memory controller Hub 2. 82801 AA I/O controller hub
Memory support	512 MB of SDRAM memory
Bus support	PCI bus
Video and audio support	AP 2.0 devices
I/O port support	1. Two USB ports 2. UDMA IDE controller
Others	1. Integrated LAN support 2. Bus master capabilities

Table 1.4.2 : Details of INTEL 815 chipset

3. Intel 820 Chipset

- It also uses the Accelerated Hub Architecture.
- It supports improved audio and video handling.
- The complete details of this chipset are given in the table 1.4.3.



Fig. 1.4(d) : INTEL 820 chipset

Parameter	Details
Processors supported	Pentium II/ Pentium III processors
Multi processor support	2 processors
Functional blocks	<ol style="list-style-type: none"> 1. 82801 I/O controller hub 2. 82802 firmware hub 3. 82820 memory controller hub
Memory support	1 GB system memory-SDRAM and RDRAM technology
Bus support	PCI, USB and AGP buses
Video and audio support	AGP 4X
I/O port support	Four USB ports

Table 1.4.3 : Details of INTEL 820 chipset

4. Intel 845 chipset

- The Intel 845 chipset is the most versatile chipset that Intel has ever developed.
- This chipset offers performance levels suitable for value, mainstream, and performance PC uses.
- The complete details of this chipset are given in the table 1.4.4.

Parameter	Details
Processors supported	Pentium IV/ Celeron

Multi processor support	2 processors
Functional blocks	1. 82845 - Memory controller hub 2. 82801DB ICH4 - I/O controller hub
Memory support	2 GB of SDRAM
Bus support	400 MHz system bus
Video and audio support	1. AGP 4X devices 2. Onboard audio
I/O port support	1. Four USB ports 2. 2 high speed UART COM ports
Others	Support for the CNR (communications & networking riser) card for integrated modem and 10/100 Ethernet networking

Table 1.4.4 : Details of INTEL 845 chipset

5. Intel 850 chipset

- This chipset provides a balanced performance platform for the Intel pentium IV processor with 400 MHz system bus.
- The complete details of this chipset are given in the table 1.4.5.

Parameter	Details
Processors supported	Pentium IV/ Intel's Net Burst Architecture
Multi processor support	2 processors
Functional blocks	1. 82850 memory controller hub 2. 82801BA I/O controller hub
Memory support	2 GB of RDRAM
Bus support	1. Four 100 MHz system bus 2. 400 MHz data bus
Video and audio support	1. AGP 4X devices 2. Six channels of audio

I/O port support	1. Four USB ports 2. Bus master IDE controller
Others	LAN connect interface facility

Table 1.3.5 : Details of INTEL 850 chipset

Additional Information

* What is an interface *

An interface is a boundary across which two independent systems meet and act on (or) communicate with each other. In computer terminology, there are several types of interfaces.

1. User interface: The user interface allows the user to communicate with the operating system. The keyboard, mouse, menus of a computer system are the general examples of user interfaces.

2. Software interface: Software interfaces are the languages and codes that the applications use to communicate with each other and with the hardware.

3. Hardware interface: Hardware interfaces are usually the wires, plugs and sockets that hardware devices use to communicate with each other.

1.5. EXPLAIN THE SPECIFICATIONS OF PROCESSOR

The specifications of a processor are listed below.

- 1. Clock Speed:** The clock speed (commonly referred to as the frequency) of a CPU is how many instructions per second it can process and is typically reported in MHz or GHz.
- 2. Data Bus Width:** This specifies the number of bits that the data bus of a processor can carry at a time.

***Note:** Processor data bus is also called the front side bus (FSB), processor side bus (PSB), or just CPU bus.

3. Internal Register Size : This is an important specification of a processor. The size of the internal registers of a processor determines the maximum size of the data unit with which the processor can work.

***Note:** Based on the internal register sizes, the processors are generally classified as 16-bit processors, 32-bit processors and 64-bit processors. A 64-bit processor has 64-bit internal registers.

4. Address Bus Width: The width of the address bus of a CPU determines the maximum amount of main memory that the processor can address.

5. Maximum memory: It specifies the maximum total RAM that the processor can address.

6. Number of Cores: This specification of the processor indicates the number of Cores is there in the processor. If there are two cores in the processor, then it is called a Dual core processor and if it has 4 cores in it, it is called Quad core processor.

***Note:**

- A multi-core processor is a single computing component with two or more independent actual processing units.
- These Independent sub-processing units are called Cores.
- The core of a processor reads and executes program instructions individually and thus acts as a independent sub-processor.

7. CPU Socket Type: It specifies the type of the socket (LGA or PGA) for which the CPU is manufactured.

8. Working Voltage: It represents the DC voltage that the CPU requires for its working.

9. Bus Type: The bus type of a CPU is the way in which the CPU cores communicate with the rest of the system.

For the average user, the bus type will not heavily influence the speed of the processor, but newer bus types are generally more efficient than older types.

***Note:** At the moment, QPI (Quick Path Interconnect) is the most common bus for Intel CPUs and Hyper-transport is the most common for AMD CPUs.

- 10. Level 1 (L1) Cache:** The amount of L1 cache is generally given per core and is in the range of 32KB to 64KB per core.
- 11. Level 2 (L2) Cache:** L2 cache can range anywhere from 256KB to 1MB (1024KB) per core.
- 12. Level 3 (L3) Cache:** L3 cache is much larger than L2 or L1 cache. Its size is typically up to 20MB or more on some CPUs.
- 13. Process :** The Process specification of a CPU indicates how tightly the individual microscopic components (such as transistors) within the CPU are packed when it is being manufactured. This is reported in nanometers. Many CPUs on the market today use a 32nm manufacturing process, which is over 30x smaller than the diameter of a human hair.
- 14. No. of Transistors:** It specifies the number of transistors fabricated to manufacture the Processor.
- 15. Thermal Output:** Thermal output (also called TDP or thermal design power) is the maximum amount of power that the processor cooling system needs to dissipate.

Additional Information

*** Computer memory Units ***

The size of a computer memory is the amount of data that can be stored in it. The memory units which are generally used to measure the size of a memory are shown in the table 1.5.1.

Unit	Description
Bit	Logical 0 and 1
Nibble	A group of 4 bits
Byte	A group of 8 bits
Word	A computer word is a group of fixed number of bits processed as a unit. The length of a computer word is called word-size or word length and it may be as small as 8 bits or may be as long as 96 bits. It varies from computer to computer but is fixed for each computer. A computer stores the information in the form of computer words.

Table 1.5.1 : Computer memory units

Generally, the computer memory size is expressed in terms of Bytes. Some higher storage units are given in table 1.5.2.

Unit	Description
Kilobyte (KB)	1 KB = 1024 Bytes
Megabyte (MB)	1 MB = 1024 KB
GigaByte (GB)	1 GB = 1024 MB
TeraByte (TB)	1 TB = 1024 GB
PetaByte (PB)	1 PB = 1024 TB

Table 1.5.2

1.6. LIST THE FEATURES OF DDR2SDRAM AND DDR3SDRAM

Synchronous DRAM (SDRAM) was the first type of memory to run in sync with the processor bus (the connection between the processor, or CPU, and other components on the motherboard).

1.6.1. DDR2 SDRAM

- **Double data rate 2 SDRAM (DDR2 SDRAM)** is the successor to DDR SDRAM. DDR2 SDRAM runs its external data bus at twice the speed of DDR SDRAM and features a four-bit prefetch buffer, enabling faster performance.
- However, DDR2 SDRAM memory has greater latency than DDR SDRAM memory.
- Latency is a measure of how long it takes to receive information from memory; the higher the number, the greater the latency.
- Typical latency values for mainstream DDR2 memory are CL=5 and CL=6, compared to CL=2.5 and CL=3 for DDR memory.
- 240-pin memory modules use DDR2 SDRAM

1.6.1. DDR3 SDRAM

- **Double data rate 3 SDRAM (DDR3 SDRAM)** Compared to DDR2, DDR3 runs at lower voltages, has twice the internal banks, and most versions run at faster speeds than DDR2.
- DDR3 also has an eight-bit prefetch bus.
- As with DDR2 versus DDR, DDR3 has greater latency than DDR2.
- Typical latency values for mainstream DDR3 memory are CL7 or CL9, compared to CL5 or CL6 for DDR2.
- Although DDR3 modules also use 240 pins, their layout and keying are different than DDR2, and they cannot be interchanged.

Memories used in PC

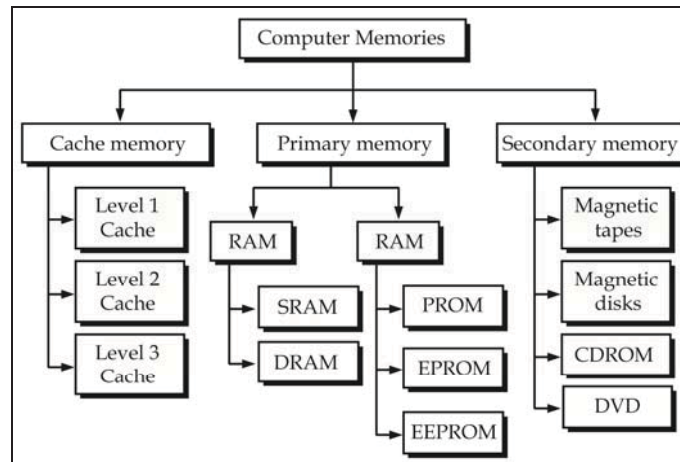


Fig. 1.5 Classification of Computer memories

1.7. EXPLAIN ACCELERATED GRAPHICS PORT

- Accelerated Graphics Port (AGP) is an [interface](#) specification that enables [3-D](#) graphics to display quickly on ordinary personal computers.
- AGP is designed to convey 3D images (for example, from Web sites or CD-ROMs) much more quickly and smoothly than is possible today on any computer other than an expensive graphics workstation.
- AGP is especially useful in conjunction with gaming, 3D video, and sophisticated scientific and engineering graphics programs.
- AGP was designed by Intel in 1996 as an alternative to the PCI standard.
- AGP introduces a dedicated point-to-point channel that allows the graphics controller to directly access the system memory (RAM).

- In other words, AGP interface provides a dedicated bus for graphics data. Therefore, AGP cards are able to render graphics faster than comparable PCI graphics cards.
- Like PCI slots, AGP slots are built into a computer's motherboard. They have a similar form factor to PCI slots, but can only be used for graphics cards. The location of an AGP port on the mother board is shown in the fig. 1.7(a).

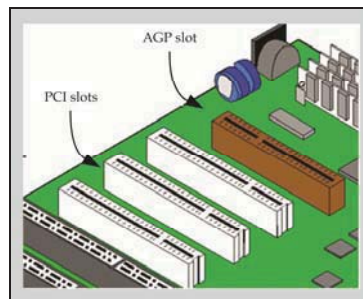


Fig. 1.7(a) : AGP slot on the motherboard

1.8. LIST VARIOUS SMPS POWER SUPPLY CONNECTORS USED IN PC-AT AND EXPLAIN THEIR USE

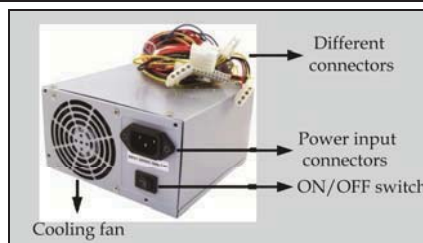


Fig. 1.8(a) : Computer SMPS

The power supply used in the computer systems is a Switch Mode Power Supply (SMPS). Generally, the word "Computer SMPS" is used to refer to a computer power

supply unit. A typical computer SMPS is shown in the fig. 1.8(a).

The various power supply connectors available in different computer power supply units are clearly explained in this section.

Motherboard power connectors

Motherboard power connectors are also known as main power connectors. This connector varies for AT & ATX power supplies as previously explained.

AT Main power connector

- The AT main power connector is a combination of two separate 6-Pin connectors (P8 & P9).

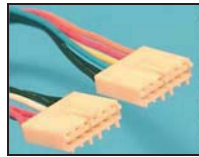


Fig. 1.8(b) : AT main power connector

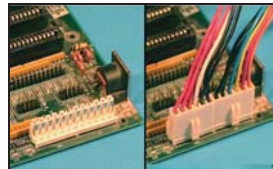


Fig. 1.8 (c) : Connecting a AT main power connector to the motherboard

- Note that you must install these connectors to the motherboard in such a way that the black wires are placed on the centre as shown in the fig. 1.8(c); otherwise the motherboard will be damaged.
- The pin out description for AT main power connector is shown in table 1.8.1.

PIN NUMBER	WIRE COLOR	DESCRIPTION
P8 connector		
1	orange	power good, outputs +5V DC when all voltages has stabilised

2	red	+5 volts or connector key
3	yellow	+12 volts
4	blue	-12 volts
5	black	Ground
6	black	Ground
P9 connector		
1	black	Ground
2	black	Ground
3	white	-5 volts
4	red	+5 volts
5	red	+5 volts
6	red	+5 volts

Table 1.8.1 : Pin out description of AT main power connector

1. ATX Main power connector

- Earlier ATX power supply models used a 20-pin configuration for connecting to the motherboards. But the current standard is a 24-pin configuration.
- The pin out description for ATX 20-pin main power connector is shown in Table 1.8.2.

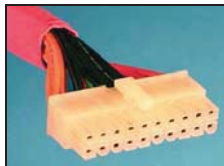


Fig. 1.8(d) : 20-pin ATX main power connector

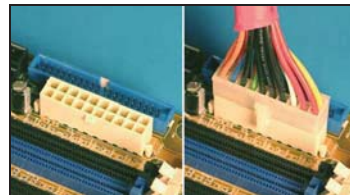


Fig. 1.8(e) : Connecting a 20 pin ATX main power connector to the motherboard

PINS 1 THROUGH 10			PINS 11 THROUGH 20		
Description	Wire color	Pin number	Pin number	Wire color	Description
+3.3 volts	orange	1	11	orange	+3.3 volts
+3.3 volts	orange	2	12	blue	-12 volts
ground	black	3	13	black	ground
+5 volts	red	4	14	green	PS_ON#
ground	black	5	15	black	ground
+5 volts	red	6	16	black	ground
ground	black	7	17	black	ground
PWR_OK	gray	8	18	white	-5 volts (optional)
VSB +5 volts	purple	9	19	red	+5 volts
+12 volts	yellow	10	20	red	+5 volts

Table 1.8.2 : Pin out description of ATX 20-pin main power connector



Fig. 1.8(f) : 24-pin ATX main power connector

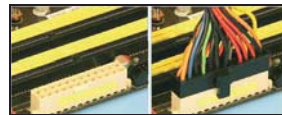


Fig. 1.8(g) : Connecting a 24-pin ATX main power connector to the motherboard

- The pin out description for ATX 24-pin main power connector is shown in Table 1.8.3.

PINS 1 THROUGH 12			PINS 13 THROUGH 24		
Description	Wire color	Pin number	Pin number	Wire color	Description
+3.3 volts	orange	1	13	orange	+3.3 volts
+3.3 volts	orange	2	14	blue	-12 volts
ground	black	3	15	black	ground
+5 volts	red	4	16	green	PS_ON#
ground	black	5	17	black	ground
+5 volts	red	6	18	black	ground
ground	black	7	19	black	ground
PWR_OK	gray	8	20	white	-5 volts (optional)
VSB +5 volts	purple	9	21	red	+5 volts
+12 volts	yellow	10	22	red	+5 volts
+12 volts	yellow	11	23	red	+5 volts
+3.3 volts	orange	12	24	black	Ground

Table 1.8.3 : Pin out description of ATX 24-pin main power connector

***Note:**

- Motherboards can come with either a 20 pin main power connector or a 24 pin main power connector. Many power supplies come with a 20+4 motherboard power connector which is compatible with both 20 and 24 pin motherboards.
- A 20+4 power connector has two pieces: a 20 pin piece, and a 4 pin piece. If you leave the two pieces separate then you can plug the 20 pin piece into a 20 pin motherboard and leave the 4 pin piece unplugged. Be sure to leave the 4 pin piece unplugged even if it fits into another connector. The 4 pin piece is not compatible with any other connectors.
- If you plug the two pieces of a 20+4 power connector together then you have a 24 pin power connector which can be plugged into a 24 pin motherboard.



Fig. 1.8(h) : 20+4 pin ATX motherboard power connector

2. ATX12V Power connector

- It is also called P4 connector. It is a 4-pin connector.
- It was introduced by Intel for Pentium 4 (hence the name P4).
- It plugs into the motherboard and exclusively powers the processor.
- The pin out description for P4 connector is shown in the table 1.8.4.



Fig. 1.8(i) : P4 connector



Fig. 1.8(j) : Connecting a P4 connector to the motherboard

PINS 1, 2			PINS 3, 4		
Description	Wire color	Pin number	Pin number	Wire color	Description
ground	black	1	3	yellow	+12 volts
ground	black	2	4	yellow	+12 volts

Table 1.8.4 : Pin out description of P4 connector

3. EPS +12 volt Power connector

- It is commonly referred to as EPS12V connector. It is a 8-pin connector.
- This connector was originally created for workstations to provide 12 volts to power multiple CPUs.
- But as time has passed many CPUs require more 12 volt power and the [8 pin 12 volt connector](#) is often used instead of a [4 pin 12 volt connector](#).
- EPS12V connector and it's connection details are shown in the fig. 1.8.(k).
- The pin out description for P4 connector is shown in the table 1.8.5.



Fig. 1.8(k) : EPS12V connector

PINS 1 THROUGH 4			PINS 5 THROUGH 8		
Description	Wire color	Pin number	Pin number	Wire color	Description
ground	black	1	5	yellow	+12 volts
ground	black	2	6	yellow	+12 volts
ground	black	3	7	yellow	+12 volts
ground	black	4	8	yellow	+12 volts

Table 1.8.5 : Pin out description of EPS12V connector

***Note:** Motherboards can come with either a 4 pin 12 volt connector or an 8 pin 12 volt connector for powering the processor. Many power supplies come with a 4+4 pin 12 volt connector which is compatible with both 4 and 8 pin motherboards.

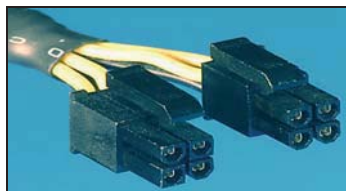


Fig. 1.8(l) : 4+4 pin EPS12V power connector

4. Molex Connector

- It is Also known as peripheral connector.

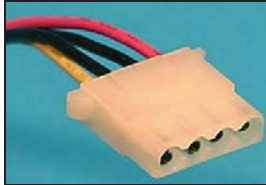


Fig. 1.8.(m) : Molex connector

- It is used for connecting various IDE (Integrated Drive Electronics) devices including floppy drives, hard disks, add-on fans, extra video card power, supplemental motherboard power, case lighting etc. The IDE devices are also known as ATA (AT Attachment) devices.

PIN NUMBER	WIRE COLOR	DESCRIPTION
1	yellow	+12 volts
2	black	ground
3	black	ground
4	red	+5 volts

Table 1.8.6 : Pin out description of Molex connector

5. SATA Connector

- SATA was introduced to upgrade the ATA interface (also called IDE) to a more advanced design. SATA includes both a data connector and a power connector.
- This connector is shaped so it can only be plugged in the correct way.
- Modern power supplies will have at least 4 of these, to power up drives at the SATA standard.

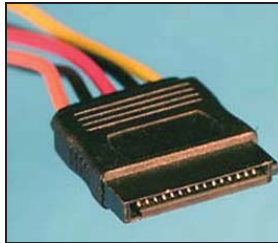


Fig. 1.8(n) : SATA connector

PIN NUMBER	WIRE NUMBER	WIRE COLOR	DESCRIPTION
1	5	orange	+3.3 volts
2	5	orange	+3.3 volts
3	5	orange	+3.3 volts
4	4	black	ground
5	4	black	ground
6	4	black	ground
7	3	red	+5 volts
8	3	red	+5 volts
9	3	red	+5 volts
10	2	black	ground
11	2	black	ground
12	2	black	ground
13	1	yellow	+12 volts
14	1	yellow	+12 volts
15	1	yellow	+12 volts

Table 1.8.7 : Pin out description of SATA connector

6. 6 pin PCI Express power Connector

- This connector is used to provide extra 12 volt power to PCI Express expansion cards.

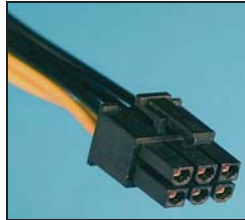


Fig. 1.8. (o) : 6-pin PCIe connector

- PCI Express motherboard slots can provide a maximum of 75 watts. Many video cards draw significantly more than 75 watts so the 6 pin PCI Express power connector was created.
- These connectors are also occasionally called "PEG connectors" where "PEG" stands for PCI Express Graphics.

PINS 1 THROUGH 3			PINS 4 THROUGH 6		
Description	Wire color	Pin number	Pin number	Wire color	Description
+12 volts	yellow	1	4	black	ground
+12 volts or not connected	yellow or not connected	2	5	black	ground
+12 volts	yellow	3	6	black	Ground

Table 1.8.8 : Pin out description of 6-pin PCIe power connector

7. 8 pin PCI Express power Connector

- This connector is just an 8 pin version of the 6 Pin PCI Express power connector.
- Both are primarily used to provide supplemental power to video cards.
- The older 6 pin version officially provides a maximum of 75 watts (although unofficially it can usually provide much more) whereas the new 8 pin version provides a maximum of 150 watts.



Fig. 1.8.(p) : 8-pin PCIe power connector

PINS 1 THROUGH 3			PINS 4 THROUGH 6		
Description	Wire color	Pin number	Pin number	Wire color	Description
+12 volts	yellow	1	5	black	ground
+12 volts	yellow	2	6	black	ground
+12 volts	yellow	3	7	black	Ground
Ground	Black	4	8	Black	Ground

Table 1.8.9 : Pin out description of 8-pin PCIe power connector

***Note:** Some video cards have 6 Pin PCI Express power connectors and others have 8 Pin PCI Express power connectors. Many power supplies come with a 6+2 PCI Express power cable which is compatible with both kinds of

video cards. The 6+2 PCI Express power connector is made up of two pieces: a 6 pin piece, and a 2 pin piece as shown in the fig. 1.8(q).



Fig. 1.8.(q) : 6+2 pin
PCIe power connector

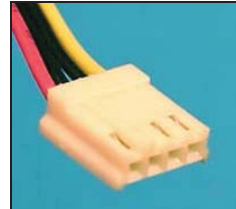


Fig. 1.8.(r) : FDD connector

8. Floppy Drive Connector

- It is also known as FDD connector.

It supplies power to floppy disk drives.

Additional Information

* Introduction to Computer Ports *

- Just having a computer itself is not enough. Imagine a computer without a monitor, printer, mouse, keyboard etc. A computer is completely worthless without all these things. We must have some way to attach these external devices to the computer. For this purpose, computer ports are used.
- **Definition:** In computer hardware, Computer ports (normally just called Ports) are the physical interfaces that connect a computer with the external peripheral devices like monitor, printer, mouse, keyboard etc.
- Do not confuse these computer ports with network ports, which are virtual ports represented by numbers used for communication among networks. Remember

that we are referring to actual physical connections on a computer.

- There are several different types of computer ports; the majority of them are located on the back of a computer case, while there are some on the front of most computer cases.
- Generally, USB ports are the only ports that are present on the front side of the computer cabinet.
- Various ports present on the back side of a computer cabinet are shown in the fig.

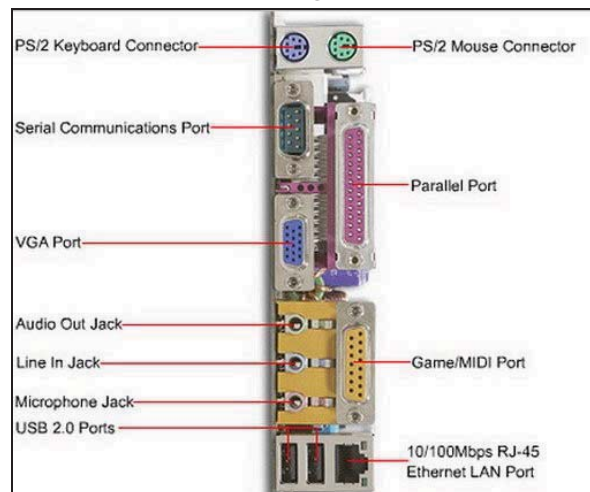


Fig: Various ports on the back of the CPU cabinet

1.9. GIVE THE CONNECTOR DETAILS OF SERIAL PORT, MOUSE, KEYBOARD AND USB.

1.9.1. Serial port connectors

- Serial ports use two types of connectors.
 1. DB-9 pin connector
 2. DB-25 pin connector

- The pinout descriptions of DB25 and DB9 serial connectors are shown in the fig.1.9(a).

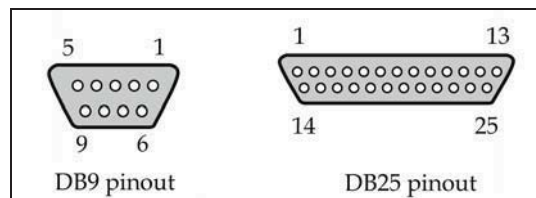


Fig. 1.9(a) : Pin out diagrams of various serial port connectors

1.9.2. Mouse connectors

- A mouse connector is a dedicated socket or interface in the computer for connecting a mouse.
- Since the invention of the first personal computer by IBM back in 1981, different types of mouse connectors have been developed. Different types of mouse connectors used until now are listed below.
 1. Bus mouse
 2. Serial mouse
 3. PS/2 connector
 4. USB connector

1. Bus mouse

- The first type of mouse was connected to the PC by the use of a **bus**, so it was actually being referred to as the bus mouse.
- It was used in the early days of the IBM-compatible personal computers.
- It connected to the PC through a specialized bus interface implemented via an ISA add-in card. It was superseded by the serial mouse.

2. Serial mouse

- The serial mouse was connected to the computer via the serial port.
- Now-a-days, the serial mouse is obsolete.

3. PS/2 connector

- A 6-pin mini DIN connector (PS/2 connector) was also used as a mouse connector.
- It has replaced the serial connectors and it was the standard mouse connector for modern PCs until recently.
- This connector is typically colored green to differentiate it from the similar keyboard connector.

4. USB connector

- The PS/2 mice are also now becoming obsolete.
- All the modern computers are now using only the USB mice.
- The physical shape and appearance of the USB mouse is similar to the others. The only difference is the connector that connects to a USB port on the back of your PC.

1.9.3. Keyboard connectors

- The keyboard connector is the device which is at the end of the keyboard cable that is used to attach the keyboard to the system.
- There are three standard types of keyboard connectors, which are the only connector types ever used in the PC world until now. They are
 1. 5-pin DIN connector (AT connector)
 2. 6-pin mini-DIN connector (PS/2 connector)
 3. USB connector

1. 5-pin DIN connector

- 5-pin DIN connector is the oldest of all the keyboard connectors which was used by older computers like XT, AT, Baby AT and LPX computers.
- It is the standard connection through about the mid-1990s. It is seldom used now.
- It is a bit larger than 6-pin DIN connector.
- It had five pins which were oriented asymmetrically (see fig. 1.9(b) to ensure a proper connection.
- It is often referred to as an AT connector, referring to the IBM system that popularized the format.



Fig. 1.9(b) : Female and male
5-pin DIN connectors



Fig. 1.9(c) : Female and male
PS/2 connectors

2. 6-pin mini DIN connector

- It is also called PS/2 connector.
- Its name comes from the [IBM Personal System/2](#) series of [personal computers](#), with which it was introduced in 1987.
- It has 6 pins and it is smaller than the older AT connector.
- It has replaced the larger 5-pin DIN connector and it was the standard keyboard connector for modern PCs until recently.

- This connector is typically colored purple to differentiate it from the similar mouse connector.

3. USB connector

- The USB connectors have almost replaced the former two DIN connectors.
- Now all the modern keyboards are USB keyboards that come with a standard USB plug on it.
- The major advantage of USB connectors over the DIN connectors is that they are hot-swappable.

1.9.4. USB connectors

- USB standards are developed and maintained by an industry body called the USB Implementers Forum (USB-IF).
- In its original specification, USB-IF defined only two connector types for USB ports. They are:
 1. USB type A connector
 2. USB type B connector

1. USB type A connector

- It is the original design for the USB standard with a flat and rectangular shape.
- It is used on devices which provide power (mostly computers).
- This interface holds the connection in place by friction which makes it very easy for users to connect and disconnect.
- Instead of round pins, the connector uses flat contacts which can withstand continuous attachment and removal very well.



Fig. 1.9(f) : USB-A connector

***Note:**

1. The A-type connector provides a "downstream" connection that is intended for use solely on host controllers and hubs.
2. It was not intended for use as an "upstream" connector on a peripheral device.
3. The male USB Type A connector is called the *plug* and the female connector is called the *receptacle* but is commonly referred to as the *port*.

2. USB B-type connector

- The B-style connector is designed for use on USB peripheral devices.

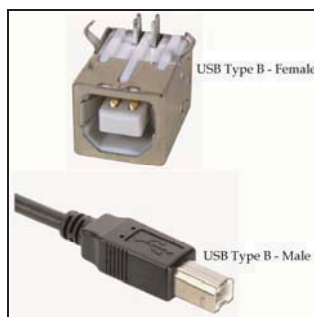


Fig. 1.9(g) : USB-B connector

- The B-style interface is squarish in shape, and has slightly beveled corners on the top ends of the connector.
- Like the A connector, it uses the friction of the connector body to stay in place.

***Note:**

1. The B-socket is an "upstream" connector that is only used on peripheral devices.
2. Because of this, the majority of USB applications require an A-B cable.

1.10. Give four reasons for popularity of USB ports

There are 6 solid reasons for wide spread popularity of USB ports. They are explained below.

1. Higher Speed

- The data transfer speeds supported by various USB versions are shown in the table 1.10.

USB version	Speed
USB 1.0	12 mbps
USB 2.0	480 mbps
USB 3.0	5 Gbps

Table 1.10.

- Traditional serial ports mostly run at a speed up to 115.2 Kbps and parallel ports run at a maximum speed of 500 Kbps to 2 Mbps. Therefore, as you can see, the USB ports are too much faster than serial and parallel ports.

2. Reliability

- Serial ports can subject to data loss due to UART overflows and missed interrupts.
- In parallel ports, if the cable is too long, then the integrity of the data can be lost.
- USB has none of those problems. So the USB ports are more reliable.

3. Multiple Devices

- A USB port can run many devices at once, up to 128 in total.
- To add more devices to a single port, a low cost hub (splitter) can be used. Hubs are often built into monitors.
- The great advantage here is that you no longer have to worry about having enough ports for new peripherals.

4. Self-Powered

- USB itself provides power to the peripheral that we connect to it, so there is no need for external mains Power Supply Unit for many products.

5. Plug & Play

- USB devices can configure themselves. Our PC will automatically detect the new device and install the software for it.

6. Hot-Swappable

- USB devices can be hot-swapped i.e., they can be connected or removed while the PC is switched on.

1.11. Explain the working of Hard Disk and data access.

- The most common internal storage used in the computer systems is **hard disk**.
- Hard disks are magnetic storage devices. They store data on magnet - coated surfaces in the form of magnetic patterns.

1.11.1. Working

- Fig. 1.11 shows all the internal parts of a hard disk drive.

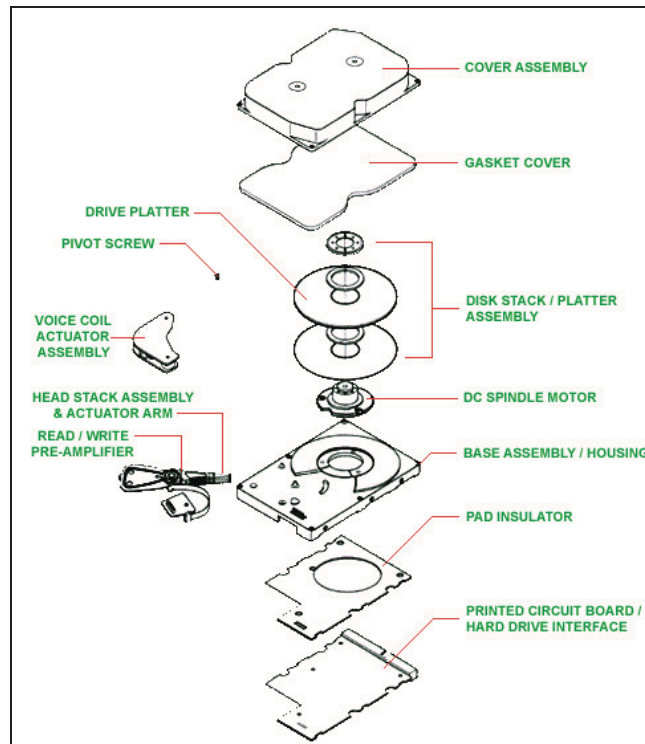


Fig. 1.11: Internal parts of a hard drive

- The hard disk drive controller controls the communication between the CPU and the disk drive. The following three are the most commonly used disk drive controllers.
 1. IDE or ATA standard
 2. SCSI standard
 3. SATA standard

1. Disk Writing

- The process of writing data onto a disk involves magnetizing the surface of the spinning disk with a set

of signals corresponding to the data that is to be recorded.

- When the computer wants to write something on the disk, then it sends signal to the hard disk controller to accept data from the computer. Along with this the CPU also sends the location where it wants to write data.
- After receiving the write signal from the computer, the drive controller places the read/write head over the desired location.
- Here buffers come into the picture to handle the communication between CPU and drive. This is because the operating speeds of the CPU and disk drive mismatch (disk drive works at a very slow rate when compared with CPU). The received data is stored in buffers.
- The disk controller then sends the data stored in the buffers to the hard disk.
- Electronic circuits in the logic board of the hard disk receive this data and convert it into magnetic pulses for recording on the surface of the disk.
- After writing the data is over, disk controller generates an interrupt to indicate the CPU that the write operation is over.

2. Disk Reading

- Reading is done using the reverse process.
- The recorded magnetic pulses are converted to electrical signals and these electrical signals are then converted to meaningful data.

***Note:** The hard disks use different methods for coding electrical signals to magnetic patterns. Some common ones among them are

1. Frequency Modulation (FM)
2. Modified Frequency Modulation (MFM)
3. Run Length Limited (RLL) coding scheme

1.11.2. Data Access

- The circular platter is divided into concentric circles known as tracks.
- Each track is divided into several partitions known as sectors.
- Each sector holds 512 bytes of data.
- Sector is the smallest accessible unit of a platter.
- A group of sectors is termed as a cluster.
- The number of sectors available on the inner track is less than that of the outer tracks.
- A combination of sectors and tracks of all vertical platters is known as a cylinder.
- Data is stored in sectors, tracks and cylinders and in both sides of the platters.
- The process of reading from or writing to the sectors involves two steps.
 1. First the read/write head is moved to the desired track. The position of the head is controlled by the head actuator. The head waits until the required sector comes under it.
 2. In second step, the spindle is rotated by the electric motor (stepper motor) that makes the sector to take position below the head correctly. When the desired sector comes under the head, the reading or writing takes place.

***Note:**

1. The number of sectors forming a cluster is the minimum space allotted by the operating system for storing a file on the disk and this size varies with the capacity of the operating system.
2. The total capacity of disk can be calculated when the details of tracks and sectors are known. The storage capacity is calculated using the following equation:

$$\text{Storage Capacity} = \text{Number of sides} \times \text{Heads} \times \text{Surface} \\ \times \text{Number of tracks} \times \text{Number of sectors} \times 512 \text{ bytes.}$$

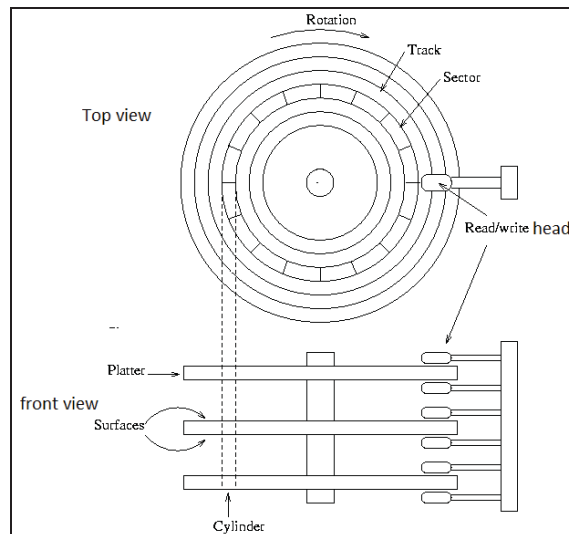


Fig. 1.11: Top view and front view of a hard disk platter assembly showing Tracks, sectors and cylinders

1.12. List five specifications of LED monitor.

HP 23vx IPS LED Backlit Monitor - Product Specifications

LED feature	Specification
Display size	58.4cm(23 in)diagonal

Display type	IPS with LED Backlight
Aspect ratio	16:9
Brightness	250cd/m ²
Inputs	1VGA 1HDMI 1DVI-D
scanning frequency	horizontal:24 to 94KHz Vertical : 50 to 76 Hz
Viewing angle	Horizontal viewing angle (typical):178 degrees Vertical viewing angle (typical):178 degrees
Recommended resolution (HxV)	1920 x180@60Hz
Power consumption	30 Watts max power consumption (28 Watts typical power consumption)
Operating temperature	5 degrees C to 35 degrees C (41 degrees F to 95 degrees F)
Storage temperature	-20 degrees C to 60 degrees C (-4 degrees F to 140 degrees F)
Tilt	-2 to +25 degrees
Dimensions	W x D x H(unpacked):
Weight	Unpacked :3.5kg (7.7 lbs)

Additional Information

- LED monitors are the latest types of monitors on the market today. These are flat panel, or slightly curved displays which make use of light-emitting diodes for back-lighting, instead of cold cathode fluorescent

(CCFL) back-lighting used in LCDs. LED monitors are said to use much lesser power than CRT and LCD and are considered far more environmentally friendly.

- The advantages of LED monitors are that they produce images with higher contrast, have less negative environmental impact when disposed, are more durable than CRT or LCD monitors, and features a very thin design. They also don't produce much heat while running. The only downside is that they can be more expensive, especially for the high-end monitors like the new curved displays that are being released.

1.13. Explain the working of LED monitor.

- LED, which stands for "light emitting diodes," differs from general LCD monitors in that LCDs use fluorescent lights while LEDs use those light emitting diodes. Also, the placement of the lights on an LED monitor can differ. The fluorescent lights in an LCD monitor are always behind the screen. On an LED monitor, the light emitting diodes can be placed either behind the screen or around its edges. The viewing angle of LED is greater than LCD. The LED monitors run with greater energy efficiency and can provide a clearer, better picture than the general LCD monitors.

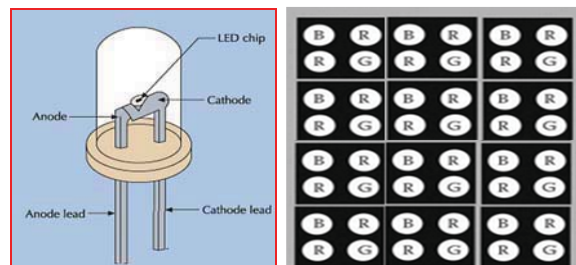


Fig. 4.19:

Working principle:

- In an ordinary diode, the semiconductor material itself ends up absorbing a lot of the light energy. LEDs are specially constructed to release a large number of photons outward.
- LED display refers to the light emitting elements who is composed by the LED (light emitting diodes) array, which is directly used as a pixel to emits red, green, and blue light, thereby forming color picture on screen.
- Fig. 4.19 shows Pixel arrangement on a portion of a monitor screen with each pixel formed from four LED's(2-red LED's, 1-Green LED, 1- Blue LED).
- LED monitors provide a better picture for two basic reasons. First, LED monitors work with a color wheel or distinct RGB-colored lights (red, green, blue) to produce more realistic and sharper colors. Second, light emitting diodes can be dimmed. The dimming capability on the back lighting in an LED monitor allows the picture to display with a truer black by darkening the lights and blocking more light from passing through the panel.

Additional Information

1. A mouse is basically a pointing device about the size of palm. It rolls on a small ball and has one or more buttons on the top. When the user rolls the mouse across a flat surface, the screen "cursor" (a blinking underline) or mouse pointer moves in the direction of the mouse's movement.
2. The "Mouse" is basically made for Graphical User Interface applications, but, compared to choosing an option using the cursor control keys, using a mouse is more natural, even in the text based environment.

3. The mouse can never replace the keyboard, but it can supplement the keyboard by doing tasks such as moving the cursor and pointing to on screen objects, tasks for which the cursor movement arrow keys are ill – suited.
4. With advances in mouse technology, now preferred device for pointing and clicking is the **Optical Mouse**. It was developed by Microsoft and introduced to the world in late 1999.
5. Optical mice have several benefits over wheeled mice or scroll mice:
 - a. Able to work on almost any surface.
 - b. No moving parts means less wear and a lower chance of failure.
 - c. There’s no way for dirt to get inside the mouse and interfere with the tracking sensors.
 - d. Increased tracking resolution means smoother response.
 - e. They don’t require a special surface, such as a mouse pad.

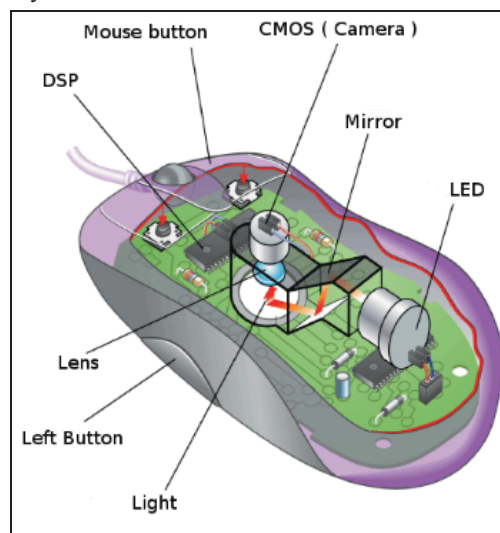
1.14. Explain the working principle of optical mouse

1. The different components that make up an optical mouse are given fig. 2.7 (a).
 2. The main components of an optical moue are
 - a. Optical eye
 - b. Micro camera
 - c. Digital signal processor (DSP)
- a) **Optical Eye:**
1. It is nothing but an LED placed beneath the mouse.
 2. It is used to scan the surface.

3. It scans the surface by projecting light onto the surface.

b) Micro Camera:

1. A CMOS (Complimentary Metal - Oxide Semiconductor) sensor serves as the micro camera. It takes the pictures of the surfaces that are scanned by the optical eye.



c) DSP:

1. The CMOS sensor sends each image to a **digital signal processor (DSP)** for analysis.
2. The DSP is able to detect patterns in the images and see how those patterns have moved or changed since the previous image.
3. Based on the change in patterns over a sequence of images, the DSP determines how far the mouse has moved and sends the corresponding coordinates to the computer.
4. The computer moves the cursor on the screen based on the coordinates received from the mouse. This happens

hundreds of times each second, making the cursor appear to move very smoothly.

C) Data sent to Computer by the Mouse:

1. When the mouse moves or the user clicks a button, it sends 4 bytes (32 bits) of data to the computer. The first 8 bits contain:
 - a. Left button state (0 = off, 1 = on)
 - b. Right button state (0 = off, 1 = on)
 - c. 0
 - d. 1
 - e. X direction (positive or negative)
 - f. Y direction
 - g. X overflow (the mouse moved more than 255 pulses in $\frac{1}{40}$ th of a second)
 - h. Y overflow
2. The next 3 bytes contain the X and Y movement values, respectively.

D) Note:

1. The digital signal processor which was placed in the first optical mouse created by Microsoft could take in 18 million instructions per second.
2. The first optical mouse could scan the surface around 1500 times per second.
3. Gaming optical mouse has advanced cameras embedded for the better mouse reaction.
4. Most of the optical mice use red LED. The reasons for this are:
 - a. Red LED's are cheaper when compared to other LED's.
 - b. Photo detectors are more sensitive to red light.

CHAPTER 2

PC ASSEMBLY AND SOFTWARE INSTALLATION

-: Objectives :-

On completion of the study of the chapter a student should be able to comprehend the following:

- 2.1. Explain the steps in assembling a PC.
- 2.2. Explain the editing of CMOS set up and its details.
- 2.3. Describe the process of formatting.
- 2.4. State the need for disk partitioning
- 2.5. Define the Power On Self Test (POST).
- 2.6. Explain about the booting procedure.
- 2.7. Compare File Allocation Table (FAT) and NTFS.
- 2.8. Describe the structure and uses of Windows registry
- 2.9. Explain general steps involved in the installation of WINDOWS OS
- 2.10. State the need for installation of device drivers.
- 2.11. List different types of viruses and ways of removing viruses.
- 2.12. List popular Anti-Virus Software available in market

2.1. EXPLAIN THE STEPS IN ASSEMBLING A PC.

A desktop computer is easy to assemble. The step – by – step procedure for assembling a PC is explained below:

Step 1: Procuring Parts

First you will need to buy the parts necessary to build the computer. The essential components for building a computer include the following:

1. Computer Cabinet (Also known as Computer Chassis or Computer Case)
2. Power Supply
3. Motherboard
4. Processor
5. Thermal Grease
6. Processor heat sink and cooling fan
7. Hard Disk
8. Memory
9. Optical Drive
10. Data and power cables for hard disk and optical drive
11. Case fan
12. Keyboard, Mouse, Monitor and
13. Other peripherals (if required)

Step 2: Gather Tools and Supplies

The following tools are required for making the assembling process easier:

1. Screwdriver (for slotted and Phillips head screws)
2. Wire cutters and strippers

3. Needle - nosed pliers
4. Utility Knife
5. Small flashlight
6. Adjustable wrench
7. Small container to hold screws
8. Heat sink compound
9. Grounding Strap



Fig. 2.1(a) : Various tools required for assembling a PC

Step 3: Setting up the Cabinet

The process of preparing a cabinet (case) for assembling involves the following sub - steps.

Step 3.1: Opening the Case

1. Open the computer case by removing the side panels.
2. Find the screws that hold the side panels in place and remove them.
3. The panel is removed by first sliding it back then lifting it away from the case as shown in the fig.2.1(b).



Fig. 2.1. (b) : Removing the side panel of a cabinet

Step 3.2: Preparing the Case for Assembly

1. Remove any parts or packing materials that may have been shipped inside the case (fig. 2.1 (c)).
2. Make note of the cables pre - installed in the case. These should be front panel connections for features such as the power switch, audio jacks and USB ports.



Fig. 2.1(c): Removing parts and packing materials inside the case

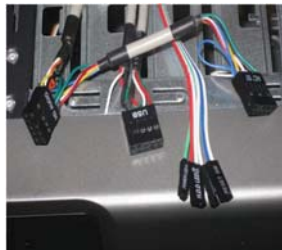


Fig. 2.1 (d) : Cables pre-installed in the cabinet

Step 3.3: Fixing the I/O Shield

1. The desktop motherboard package comes with an I/O shield or a back plate.
2. The I/O shield is to be installed on the chassis before installing the motherboard. It is installed in the window provided on the rear side of the computer chassis. The location of the window for installing the I/O shield is clear from fig. 2.1 (e).

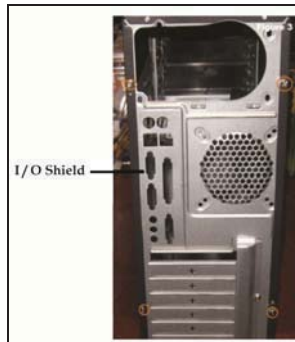


Fig. 2.1 (e) : I/O shield on a cabinet

3. To install the shield, it must be placed inside the cabinet correctly in the window and it is firmly pressed into the right place so that the shield fits tightly and securely on the I/O shield window of the chassis.

***Note:**

- If an I/O shield is already present in the cabinet, this must be removed.
- The shield available with the motherboard alone must be used for assembling the computer, since the I/O shield coming with the motherboard is designed to match the exact orientation of different ports on the motherboard.

Step 4: Ground Yourself

1. Put the grounding strap on your wrist and connect the other end to the computer case (see fig. 2.1 (f)).
2. This will prevent any buildup of static electricity on your body which will damage the computer components.



Fig. 2.1 (f) : Grounding yourself

Step 5: Installing Power Supply Unit

Power supply unit has to be fixed on the top rear corner window of the cabinet. To install the power supply unit, following steps are to be done:

1. First of all, the power supply unit is inserted inside the cabinet and then the screw holes of the chassis are aligned with the screw holes of the power supply unit. The insertion of the power supply unit should be done in a manner so that its socket for connecting to the mains power supply is facing outwards.
2. After placing the power supply unit in its place, the screws are inserted in the holes from outside (one by one) and each one is tightened gently. The arrangement is shown in the figure 2.1 (g).



Fig. 2.1(g) : Installing the power supply unit

Step 6: Installing the CPU

To install the CPU, following steps are to be done:

1. Locate the CPU socket on the motherboard.

2. Release the load lever from the retention tab by pressing it down and then moving it away from the socket.

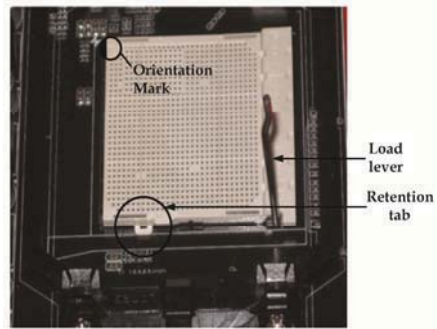


Fig. 2.1(h) : Load lever and retention tab on a CPU socket

3. Now remove the processor from the protective processor cover. The processor must be handled only through its edges. Touching the bottom of the processor or holding the processor at its bottom must be avoided.
4. Align the orientation mark present on the processor with the orientation mark on the CPU socket.
5. Lower the processor straight down to the socket without tilting or sliding (see fig. 2.1(j)).



Fig. 2.1(i) : Orientation mark on a processor



Fig. 2.1(j) : Inserting the processor into the socket

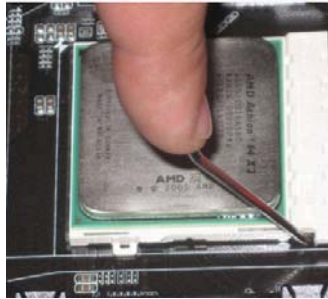


Fig. 2.1(k) : Closing the load lever

6. After correctly placing the CPU chip in its position, close the socket lever and lock it as shown in the fig. 2.1(k).

Step 7: Installing Heat Sink and Cooling Fan

Fitting of the heat sink and processor fan is essential to prevent the overheating of the processor. Perform the following steps to install the CPU heat sink and cooling fan.

1. Apply a small amount of thermal paste on the above surface of the processor.
2. After applying the thermal paste, press down the mounting screws provided with the cooling fan into the mounting holes present on the motherboard.
3. Now lock them in their positions.

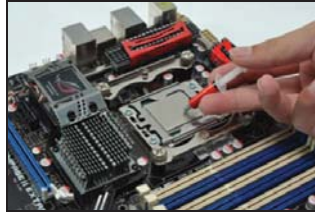


Fig. 2.1 (l) : Applying thermal paste over the CPU



Fig. 2.1 (m) : Processor cooling fan

4. Finally connect the fan power cable to the fan power connector on the motherboard.

***Note:**

- The fan is powered from the connector in the motherboard.
- The fan power connector is marked on the motherboard and is usually located near the memory slots.

Step 8: Installing RAM

To install a RAM in the DIMM slot, following steps are to be done:

1. Open the latches on both sides of the slot and then move those latches completely outwards.

2. The DIMM slot is divided into two parts by a small notch. A similar notch can be seen in the connecting edge of the memory module also.
3. Align the notch on the module with the notch in the memory slot as shown in the fig. 2.1(n).
4. After aligning, push down the memory module to the slot gently and then press down the module firmly by applying pressure on both the edges of the module. The retaining clips snaps into the locked position when the module is firmly seated in the connector.
5. Finally, lock the latches on the both sides as shown in the fig. 2.1(o).

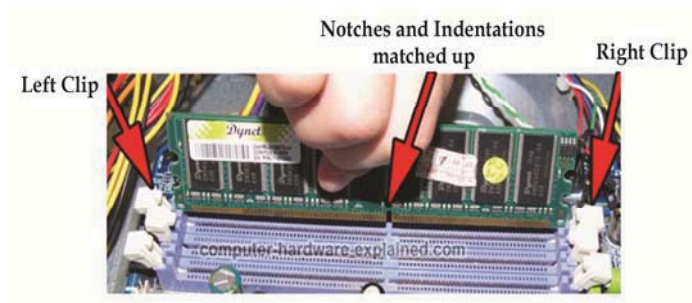


Fig. 2.1 (n) : Aligning the RAM

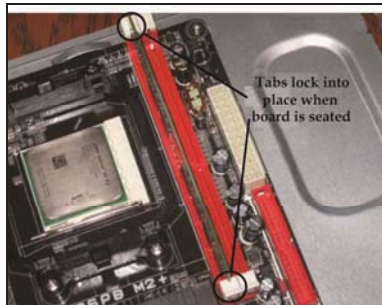


Fig. 2.1(o) : Fixing the RAM in its position

***Note:** Depending on the requirements on the memory and the availability of slots, more than one memory module can be installed in the free memory slots of the motherboard.

Step 9: Installing Motherboard

Installing motherboard in the computer cabinet can be done by following the below steps:

1. Fix the standoffs to the matching screw holes on the surface of the cabinet with the help of pliers as shown in the fig. 2.1(p).



Fig. 2.1(p) : Fixing standoffs on the cabinet

2. Lower the motherboard into the case and align with the I/O shield.
3. Install the screws.

***Note:**

- It is necessary to ensure that the motherboard, when fixed, is not in contact with the metallic parts of the computer chassis, as this type of contact can damage the motherboard components.
- So in order to ensure this the motherboard is usually seated on two or more standoffs fixed on the chassis metal surface.

Step 10: Installing Hard Disk

The following steps are to be done to install the hard disk.

1. Normally, hard disks are fitted at the lowest drive bay of the chassis. Mount the hard disk drive in the bay and

- adjust its position slowly so as to make the position of the screws match with the slots in the mounting plate.
2. Fit the hard disk to the bay using the screws as shown in the fig. 2.1(q).
 3. After firmly fixing the hard disk, connect the data cable to the hard disk and to the motherboard and then connect the power cable from the power supply unit to the hard disk.

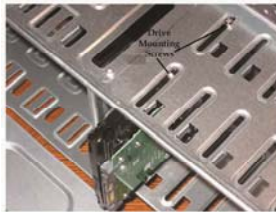


Fig. 2.1 (q) : Installing hard disk

Step 11: Installing Optical Drive

The steps that must be followed to install an optical drive are given below:

1. First of all, remove the blanking panel from the front side of the computer chassis.
2. Now, insert the drive slowly in the drive bay with the tray opening gate facing outwards.
3. After that, fix the drive in the bay using mounting screws.
4. Now connect the data cable to the drive and the motherboard.
5. Connect a free power cable from the computer power supply to the power connector of the drive.
6. Finally, connect the audio cable of the drive to the audio connector in the motherboard.



Fig. 2.1(r) : Cabinet with blanking panel removed

Step 12: Installing Cabinet Fan

The cabinet fan is usually installed on the back panel of the cabinet. To mount the fan follow the below steps:

1. Align the mounting holes by holding the fan to the mounting pad on the inside of the case as shown in fig. 2.1(s).
2. Insert the screws from the outside of the case and tighten.

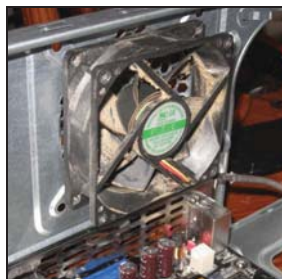


Fig. 2.1(s) : Installing cabinet fan

Step 13: Connecting Motherboard Power Supply Cables

1. Connect an AT or ATX power connector from the power supply unit to the motherboard.
2. After that, connect the 4-pin processor connector from the power supply to the processor connector on the motherboard.

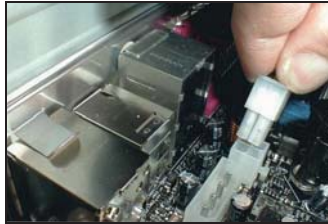


Fig. 2.1 (t) : Processor power connector

Step 14: Connecting to Front Panel

1. The front panel usually consists of a power switch, power LED indicator, reset switch, a USB connector and a hard disk active indicator.
2. All these items are to be connected to the respective connectors in the motherboard.
3. Position of the different connecting points in the motherboards can vary with the different motherboards.
4. Hence, by using the manual, different connections are made in the motherboards.
5. Generally, the connection points are clearly marked in the motherboards and the cable end connectors, as shown in figures 2.1(u) and 2.1(v).



Fig. 2.1(u) : Front panel connectors

Step 15: Closing the Cabinet

1. Now all the components in the cabinet are completely installed, the last thing to do is to reinstall the side panels on the cabinet.
2. Before closing the cover,

- Check all the connections again.
 - Tie up all the loose hanging wires inside the cabinet as a bunch.
 - Ensure that no screws or other components are left free inside the cabinet.
3. After doing all these activities, close the cabinet by reinstalling the side panels.

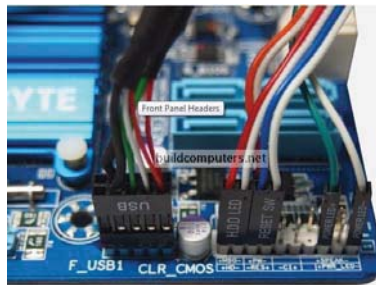


Fig. 2.1(v) : Front panel connections on the motherboard

Step 16: Connecting external peripherals

1. Connect the mouse and the keyboard to the mouse port and the keyboard port respectively, present on the rear panel.
2. Connect the signal cable of the monitor to the video port on the rear panel.
3. Connect different audio devices such as speaker, head phone and microphone to the respective audio jacks, if required.

Step 17: Switching on the Computer

1. Once all the connections are made, the assembling of the computer is completed.
2. Now, the system is to be switched on. For this, the computer chassis and the monitor are connected to the mains power supply and then the power is switched on.



Fig. 2.1(w) : Assembled PC

2.2. EXPLAIN THE editing OF CMOS SET UP AND ITS DETAILS.

- BIOS code includes a program called configuration/ setup utility program that allows the user to view and change the settings of various system parameters.
- There are two types of BIOS set-up programs. One is Text based menu set-up and the other is WinBIOS set-up in which the menu will be in graphics. Generally, it is necessary to set up- the BIOS when a system it is installed. Once the set-up is done and saved, a better powered CMOS will memorize it. The system will use this configuration every time it is powered-up.
- The table 2.1 shows different categories of BIOS set-up and the various settings available.

Category	Settings
Standard set-up	Date/Time Settings for floppy drive A and floppy drive B Settings for master hard disk and slave hard disk.
Advanced set-up	Keyboard settings (chars/sec) Settings for display

	Mouse support System boot-up NUM LOCK Floppy drive seek at boot Floppy drive swapping System boot-up sequence
Chipset set-up	Cache memory settings
Power management	Enable/Disable APM (Automatic power Management) mode Sleep mode timeout Suspend mode timeout VGA power down HDD power down.

Table 2.1. : Different categories of BIOS CMOS set-up

2.3. DESCRIBE THE PROCESS OF FORMATTING.

Disk formatting is the process of preparing a data storage device such as a hard disk drive, solid – state drive, floppy disk or USB flash drive for initial use.

Formatting a hard disk involves three steps:

1. Low – Level Formatting (LLF)
2. Partitioning
3. High – Level Formatting (HLF)

Each of the above processes is briefly explained below:

1. Low – Level Formatting

- Low – level formatting is the process of marking out cylinders and tracks for a blank hard disk, and then dividing tracks into multiple sectors.
- After that, each sector's data area is filled with a dummy byte value or test pattern of values.

***Note:**

1. Low - level formatting is often called the “real” formatting since it creates physical format which defines where the data is saved.
2. If users perform low - level formatting when data have been installed, all existing files will be erased, and it is almost impossible to recover them.
3. Nevertheless, performing low - level formatting will bring great influence on hard disk, thus shortening hard disk service time. Therefore, it is not suggested.
4. To low level format a hard disk, users can make use of specific tools as well as Debug assembler languages.

2. Partitioning

- Partitioning is the process of dividing a hard disk into a number of logical portions.
- Dividing a large hard disk into a number of parts helps in the easy management of the storage space.

***Note:**

1. Partitioning is required because a hard disk is designed to be used with more than one operating system.
2. Separating the physical format in a way that is always the same, regardless of the operating system being used and regardless of the high - level format (which would be different for each operating system), makes possible the use of multiple operating systems on one hard drives.
3. This step of formatting often includes checking for defective tracks or defective sectors.
4. Each partition of a hard disk is also known as a Logical Volume. The process of disk partitioning is explained in more detail in the section 5.5.

3. High – Level Formatting

- After partitioning the hard disk into logical volumes, users need to make high – level formatting to each volume which makes it possible to save data.
- High – level formatting is the process of writing a file system, cluster size, partition label, and so on for a newly created partition or volume.

***Note:**

1. This process does no harm to hard disk in general situations, so we suggest taking such a format to fix a logically damaged partition or device, for example, Windows asks to format a SD card.
2. It can be very easy to high level format a drive, and users can complete this operation in Windows snap – in Disk Management tool, diskpart, cmd, etc. Nevertheless, if users perform such a format on partitions with data saved, all these data will be lost.

2.4. STATE THE NEED FOR DISK PARTITIONING

- Disk Partitioning is the process of dividing a hard disk into a number of logical portions.
- Each partition is known as a logical volume.
- Most operating systems allow users to divide a hard disk into multiple partitions, making one physical hard disk into several smaller logical hard disks.
- We must partition a disk before using it because of the following advantages with the disk partitioning.
 - On Microsoft Windows machines, it is common to store the OS and applications on one hard disk partition and user data on another hard disk partition. When a problem occurs with the OS, the

OS partition can be completely formatted and reinstalled without affecting the data partition.

- Partitioning the disk allows us to organize the data more effectively.
 - Small partitions often have smaller cluster sizes. So the wastage of disk space can be reduced by partitioning it (refer additional information at the end of this section for more information on this).
 - Partitioning a hard disk also allows us to store more than one operating system in the same hard drive.
 - A user may have to split a large hard disk into multiple partitions if the hard disk is larger than the partition size supported by the operating system.
- Disk partitions are of two types.
 1. Primary partition
 2. Extended partition

1. Primary partition

- Primary partition is the hard disk partition where both Windows OS and user data can be stored.
- It is the only partition that can be set active. A primary partition in which the OS is installed is known as the active partition. Any primary partition can be set as an active partition.
- The basic information about the division of the hard disk drive into primary partitions is stored in a data structure called Partition table.

2. Extended partition

- A standard partition table is only able to store information about four primary partitions at a time. This means that a hard disk could have a maximum of four primary partitions at a time.

- To work around this limitation, extended partitions were created. An extended partition stores information about other partitions. By using an extended partition, you can create many more than four partitions on your hard disk.

Partitions configured into an extended partition are often referred to as logical partitions.

2.5. DEFINE THE POWER ON SELF TEST (POST).

- **Definition:** Post stands for power-on self-test. It is the diagnostic testing sequence that a computer's BIOS (Basic Input/Output System) runs to determine if the computer keyboard, RAM, disk drives, and other hardware are working correctly, when the computer is turned on.
- If the necessary hardware is detected and found to be operating properly, the computer begins to 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. So, invariably the error message is communicated as a series of beeps.
- 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 message 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.


A screenshot of a BIOS POST screen. The background is black with white text. At the top left, it says 'Phoenix - AwardBIOS v6.00PG, An Energy Star Ally' and 'Copyright (C) 1984-2002, Phoenix Technologies, LTD'. In the top right corner, there is a yellow 'Energy Star' logo. The main text displays system information: 'ASUS A7N8X2.0 Deluxe ACPI BIOS Rev 1008', 'Main Processor : AMD Athlon(tm) XP 2400+', 'Memory Testing : 1048576K OK', 'Memory Frequency is at 200 MHz , Dual Channel mode', 'Primary Master : SAMSUNG SU4004H PM100-21', 'Primary Slave : SAMSUNG SP4002H QU100-60', 'Secondary Master : Pioneer DVD-ROM ATAPI Model DVD-105S 0133 E1.33', and 'Secondary Slave : SAMSUNG CF/ATA 04/05/06'. At the bottom, it says 'Press DEL to enter SETUP ; press Alt+F2 to enter AWDFLASH utility' and '08/04/2004-nVidia-nForce-A7N8X2.0'.

Fig. 2.5(a) : POST screen

***Note:** During POST, BIOS performs various activities. The principle duties performed by the main BIOS during POST are listed below:

- Verify CPU registers
- Verify the integrity of the BIOS code itself
- Verify some basic components like DMA, timer, interrupt controller
- Find, size, and verify system main memory
- Initialize BIOS
- Pass control to other specialized extension BIOSes (if installed)

- Identify, organize, and select which devices are available for booting
- Discover, initialize, and catalog all systems buses and devices
- Provide a user interface for systems configuration
- Construct whatever system environment is required by the target operating system.

2.6. EXPLAIN ABOUT THE BOOTING PROCEDURE.

Booting is the process of starting up a computer from a halted or powered down condition. It is a bootstrapping process that starts the operating system when the user turns on a computer system.

The way a computer boots up is given below.

1. As soon as we turn on the power button, the CPU initializes itself. The CPU registers are initialized such that they direct the CPU to the starting address of the system BIOS (0xFFFF0).
2. BIOS first runs POST (power-on-self-test) to determine if the basic hardware is working correctly.
3. If POST is successful, then BIOS initializes the various hardware devices connected to the PC.
4. After this, the BIOS checks the disk drives (in the order specified in the boot sequence) for a MBR (Master Boot Record) or boot sector.
5. Once the BIOS finds the MBR, it copies the MBR to RAM and switches the control to it. MBR contains the code to locate the active partition and to invoke its Volume Boot Record (VBR).
6. As soon as MBR finds the active partition, it invokes VBR. VBR contains code to load and invoke the

operating system installed on that device or within that partition.

7. The VBR loads the OS files into the main memory. Now, the OS takes control of the boot process.
8. The OS loads the device drivers that it needs to control the peripheral devices, such as a printer, scanner, optical drive, mouse and keyboard. This is the final step in the boot process, after which the user can access the systems applications to perform tasks.

Additional Information

Detailed Booting Procedure

The booting procedure involves a sequence of 7 steps. These steps are explained below.

Step 1:

- As soon as we turn on the power button, a reset signal is sent to the CPU.
- This reset signal initializes the CPU by resetting the CPU pins and setting CPU registers to their predefined value.
- The CPU registers are initialized such that they direct the CPU to the starting address of the system BIOS (0xFFFF0).
- Now, the BIOS take up the further process of powering up the system.

Step 2:

- BIOS first runs POST (power-on-self-test) to determine if the basic hardware is working correctly.
- If the necessary hardware is detected and found to be operating properly, then the BIOS moves ahead.

- Otherwise, the BIOS stops the booting process and issues an error message.

Step 3:

- Now, the BIOS initialize the hardware devices by letting them run their individual BIOS (for example, video card have their own inbuilt BIOS code).

Step 4:

- Now, the BIOS looks for a master boot record (MBR) or boot sector in a set of bootable devices, in a predetermined order.

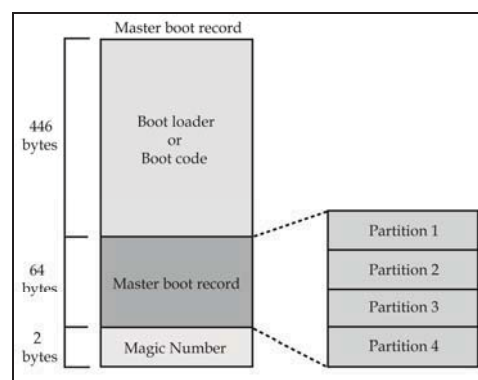


Fig.2.6 (a) : Master Boot Record (MBR)

- The priority of boot devices is set by the user in BIOS settings. The normal priority is floppy disk first, then hard disk.
- Once the BIOS finds the MBR, it copies the MBR to RAM and switches the execution authority to it.
- If a valid boot sector is not found, BIOS check for next drive in boot sequence until it finds a valid boot sector. If BIOS fails to get a valid boot sector, generally it stops

execution and gives an error message “**disk boot failure**”.

***Note:**

1. The master boot record is generally stored in the first 512 bytes i.e., the first sector of a data storage device.
2. MBR contains the boot loader or boot code and the partition table.
3. The boot loader (or boot code) is stored in the first 446 bytes and the partition table is stored in the next 64 bytes.
4. As shown in the fig.2.6.(a), the MBR ends with two layer bytes that should be 0xAA55. These numbers act as validation that this sector is the MBR.
5. The boot loader or boot code contains the code to locate the active partition and to invoke its Volume Boot Record (VBR).
6. The partition table identifies the file system on the partitions on the disk.

Step 5:

- The boot loader or boot code processes the partition table to identify which partition is bootable. The bootable partition is also known as active partition.
- Once, an active partition is located, the boot loader transfers the control to the first sector of the active partition.
- The first sector of active partition is called the OS boot sector, or volume boot record (VBR).

Step 6:

- VBR contains code to load and invoke the operating system installed on that device or within that partition.

- The VBR loads the OS files into the main memory. Now, the OS takes control of the boot process.

Step 7:

- Now in control, the OS performs another inventory of the systems memory and memory availability (which the BIOS already checked) and loads the device drivers that it needs to control the peripheral devices, such as a printer, scanner, optical drive, mouse and keyboard.
- This is the final stage in the boot process, after which the user can access the systems applications to perform tasks.

***Note:**

1. In the case of a network boot, where a machine may be diskless, the boot sequence is essentially same as the above, but the BIOS is in the ROM of a network card which fetches the boot loader program from the network.
2. The boot process is considered complete when the computer is ready to interact with the user or the operating system is capable of running ordinary applications.
3. Typical modern PCs boot in about a minute, while large servers may take several minutes to boot and to start all services.
4. Most embedded systems must boot almost instantly- for instance, waiting a minute for the television to come up is not acceptable. Therefore they have their whole operating system in ROM of flash memory, so it can be executed directly.

Additional Information

File Systems

Definition: A file system is an index or a database containing the physical location of every piece of data on a data storage device.

- In [computing](#), a file system is used to control how data is stored and retrieved from a data storage media such as a hard drive, CD, DVD, Floppy disk etc.
- Without a file system, information placed in a storage area would be one large body of data with no way to tell where one piece of information stops and the next begins.
- By separating the data into pieces and giving each piece a name, the information is easily isolated and identified.
- Each group of data is called a "file".
- The structure and logic rules used to manage the groups of information and their names is called a "file system".
- The windows operating systems use two file systems for data storage. They are
 1. FAT
 2. NTFS

2.7. COMPARE FILE ALLOCATION TABLE (FAT) AND NTFS.

2.7.1. Usage of FAT file system

- File Allocation Table (FAT) is a table that the older windows operating systems use to locate files on a disk.
- When you write a new file to a hard disk, the file is stored in one or more clusters that are not necessarily

next to each other; they may be rather widely scattered over the disk.

- For each file that is stored on the disk, the operating system creates a FAT entry for the file.
- The FAT entry for a file is nothing but a pointer that points to the first cluster used by the file.
- Each cluster contains a pointer to the next cluster in the file, or an indication (0xFFFF) that this cluster is the end of the file. These links and end of file indicators are shown in fig.2.7 (a).
- When you read a file, the operating system reassembles the file from clusters and places it as an entire file where you want to read it.

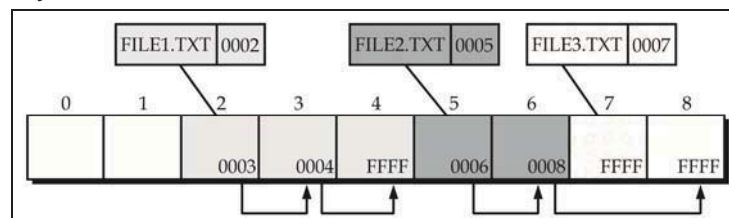


Fig 2.7 (a) : Storing files using FAT file system

- Fig 2.7 (a) shows three files. The file file1.txt is a file that is large enough to use three clusters. The FAT entry for FILE1.txt points to the starting cluster. Cluster-2 contains the address of the next cluster in which the remaining part of the File1 is stored. Similarly, cluster-3 points to cluster-4. Cluster-4 is the last cluster, so it contains the cluster address FFFF. The second file, File2.txt, is a fragmented file that also requires three clusters. A small file, File3.txt, fits completely in one cluster.

***Note:**

1. The FAT file system is relatively uncomplicated, and is supported by virtually all existing operating systems for personal computers.
2. The drawback of FAT is that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire disk, making reading and writing a slow process.
3. FAT file system now has three different versions: FAT12, FAT16, and FAT32. The numbers used in these versions designate the number of bits used to identify a cluster.
4. The table 2.7.1 shows the comparison between various FAT versions.

Attribute	FAT12	FAT16	FAT32
Used for	Floppies, small hard disk drives	Small to large hard disk drives	Large to very large hard disk drives
Size of each FAT entry	12 bits	16 bits	28 bits
Maximum Number of Clusters	4,086	65,526	~268,435,456
Cluster Size Used	512 B to 4 KB	2 KB to 32 KB	4 KB to 32 KB
Maximum Volume Size	16,736,256	2,147,123,200	about 2^{41} bytes
Table 2.7.1. : Comparison between FAT versions			

2.7.2. Usage of NTFS

- NTFS (New Technology File System) is a proprietary file system developed by Microsoft. Starting with Windows

NT 3.1, it is the default file system of Windows NT family.

- NTFS has several technical improvements over FAT such as improved support for metadata, and the use of advanced data structures to improve performance, reliability, and disk space utilization, plus additional extensions, such as security access control lists (ACL) and file system journaling.
- When a file is created using NTFS, a record about the file is created in a special file called the Master File Table (MFT). The MFT is used to locate a file's possibly scattered clusters. NTFS tries to find contiguous storage space that will hold the entire file (all of its clusters).
- Each file contains, along with its data content, a description of its attributes (its metadata).

Additional Information

Windows Registry

- The windows registry is a hierarchical database that stores low-level settings for the Microsoft windows operating system and for applications that opt to use the registry.
- It contains data that is critical for the operation of windows and the applications and services that run on windows.

2.8. DESCRIBE THE STRUCTURE AND USES OF WINDOWS REGISTRY

- The windows registry has a structure similar to Windows folders and files.
- Each main folder is named as a **Hive**.
- Each hive contains sub folders called keys.

- Each key can contain both sub-keys and data entries called values.
- The structural details of a windows registry are illustrated in the fig.2.8 (a).

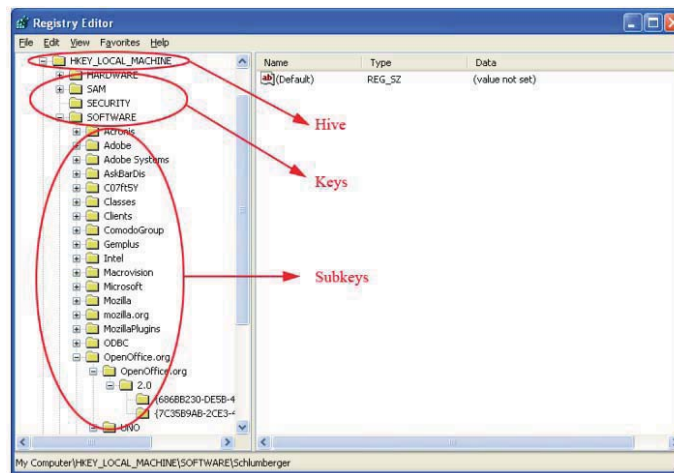


Fig. 2.8 a) : Structural details of Windows registry

2.8.1.Hives

There are six main Hives in windows registry whose descriptions are given below:

1. Hkey- Classes-Root

This hive is used to store the following information.

- ❖ Software settings about the file system.
- ❖ Windows shortcuts information.
- ❖ Information on file associations.
- ❖ Core aspects of the windows user interface.
- ❖ OLE information.

***Note:** The file association information is essentially used by windows to do the following two things.

- (a) To support the drag-and-drop feature.

- (b) To invoke the correct program when a file is opened using windows explorer.

2. HKEY-USERS

- The configuration settings for each hardware and software item in the computer systems, corresponding to each of the users of the computer system are stored in this hive.
- The information on the user's folders, user's choices of themes, colors, control panel settings and so on are stored here as users profile.
- This hive has a sub-key for each user.

3. HKEY- CURRENT- USER

- The configuration settings for each hardware and software item in the computer system, corresponding to the currently logged-on user are stored in this hive.
- This hive is dynamic, i.e. whenever a user logs-on into the system, the settings corresponding to the user are retrieved from the respective sub-key of HKEY_USERS and stored in this hive.

4. HKEY-LOCAL-MACHINE

- The configuration settings for hardware and software for all users for the computer are stored in this hive.
- The information stored here is computer specific and not user specific.
- The information stored in this hive is used by all the users who log onto this computer.

5. HKEY-CURRENT-CONFIG

- The current hardware configuration settings, pointing to HKEY_LOCAL_MACHINE\CONFIG are stored in this hive.
- This hive is dynamic, meaning it is built on the run.

6. HKEY-DYN-DATA:

- This hive points to the part of HKEY_LOCAL_MACHINE, for use with the plug-and-play features of Windows.
- This section is dynamic and will change as devices are added and removed from the system.

***Note:**

1. Sometimes, the presence of a key is all the data that an application requires; other times, an application opens a key and uses the values associated with the key.
2. A key can have any number of values, and the values can be in any form. There are three types of values; string, binary, and DWORD – the use of these depends upon the context.
3. Each key has a name consisting of one or more printable characters.
4. Key names are not case sensitive.
5. Key names cannot include the backslash character (\), but any other printable character can be used.
6. Value names and data can include the backslash character.
7. The name of each sub-key is unique with respect to the key that is immediately above it in the hierarchy.

2.8.2. Uses of windows registry

1. The windows registry serves an archive for collecting and storing the configuration settings of windows components, installed hardware, software, applications and more.
2. A windows component, hardware or software, retrieves the registry entries or keys relating to it, every time it is started. It also modifies the registry entries or keys

corresponding to it, in its course of execution. When keys are added to the registry, the data are stored as computer specific data in order to support multiple users.

3. The registry also serves as an index to the operation of the kernel, revealing run-time information of the system.
4. The registry allows access to counters for profiling system performance.

2.9. EXPLAIN GENERAL STEPS INVOLVED IN THE INSTALLATION OF WINDOWS OS

There are four methods for installing Windows XP. Review the following methods and select the method that is appropriate for your installation.

Generally, the first method is normally used for installing Windows XP by most of the users.

Method 1: Perform a clean install of Windows XP

A clean installation consists of removing all data from your hard disk by repartitioning and reformatting your hard disk and reinstalling the operating system and programs to an empty (clean) hard disk.

To perform a clean installation of Windows XP, follow these steps:

Step-1:

- Back up all important information before you perform a clean installation of Windows XP. Save the backup to an external location, such as a CD or external hard disk.

Step-2:

- Before inserting the CD, you'll need to set your computer to boot from a CD instead of from the hard drive. This will allow you to load the Windows XP

setup files before your computer boots to its installed operating system. You can change the boot order from the BOOT menu in your BIOS.

- To enter the BIOS of your computer, you usually press F9 or DEL when your computer starts or notifies you that you can enter "setup". Click the green "BIOS" link for more information.
- In the BOOT menu, set the order so that your CD/DVD-ROM drive is set as the 1st Boot Device.

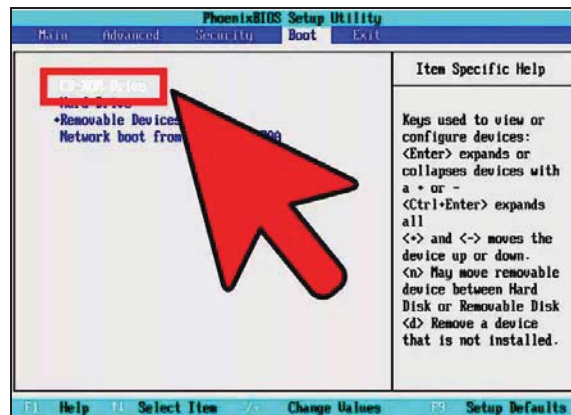


Fig. 2.9(a) : Setting CD/DVD-ROM drive as the 1st Boot Device.

Step-3:

- Now start your computer from the Windows XP CD. To do this, insert the Windows XP CD into your CD drive or DVD drive and then restart your computer.
- When you see the "Press any key to boot from CD" message, press any key to start the computer from the Windows XP CD (see fig. 2.9 b).
- At the Welcome to Setup screen, press ENTER to start Windows XP Setup (see fig. 2.9 (c)).



Fig. 2.9

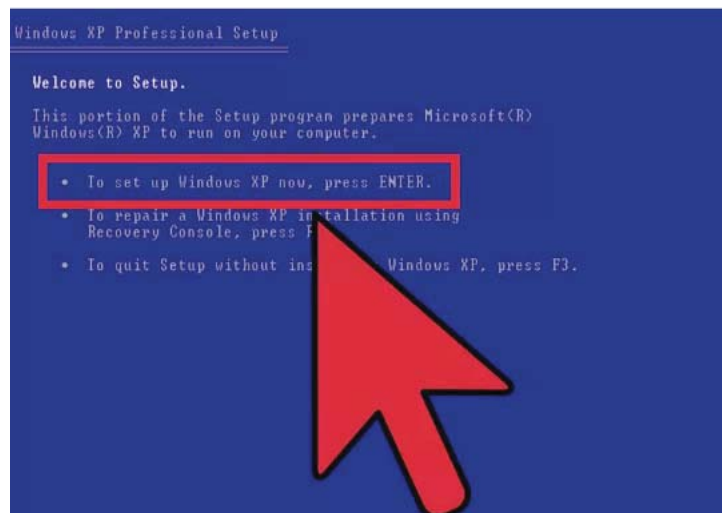


Fig. 2.9(c)

Step-3:

- Read the Microsoft Software License Terms, and then press F8.

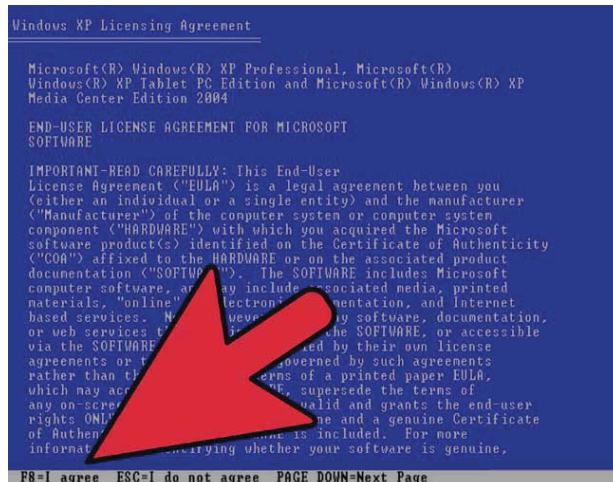


Fig. 2.9(d) : License agreement

Step-4:

- Next, the install process gives you the option to repair Windows XP or to install a fresh copy. Press ESC to install a new copy of Windows XP.

Step-5:

- Next, the partition setup will appear. If a partition already exists and you do not plan on having multiple operating systems on the computer, then press ENTER to install Windows XP in a selected partition.
- However, we recommend that you delete the existing partition and then create a new partition before continuing the setup.
- **To delete a partition:** Select the partition and press D, then ENTER. Press L to delete the partition and then press ENTER.
- **To create the partition:** Select the unpartitioned space to create a new partition, then press C. Specify the size of

the partition in MB (the default is to use all available space) and press ENTER (see fig. 2.9. (f)).

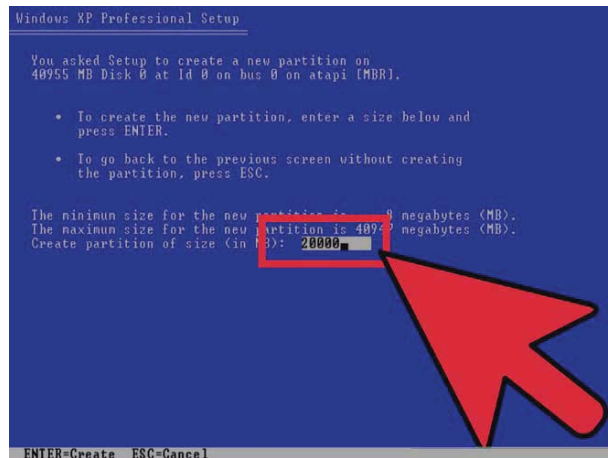


Fig. 2.9 (e)

- Once the new partition has been created for Windows XP to be installed on, press ENTER to install Windows XP.

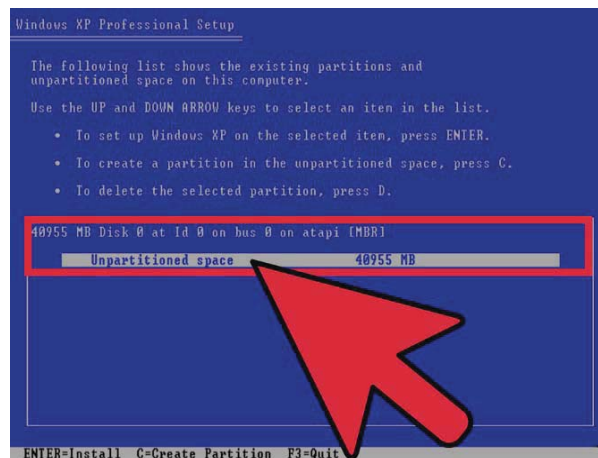


Fig.2.9 (f) : creating a new partition

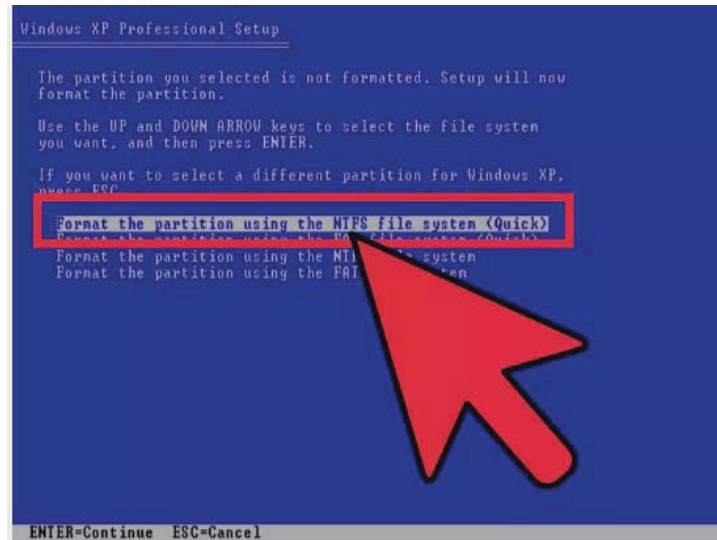


Fig. 2.9.(g)

***Note:**

1. If you have multiple partitions, we suggest deleting all partitions, unless you plan on using these partitions.
2. Deleting each of the other partitions can be done using the same steps above for each additional partition.

Step-6:

- Now you need to select whether the drive will use FAT or NTFS (see fig. 2.9 (g)).
- We suggest NTFS for users who are not sure what file system they want to use.
- After selecting the file system, press Enter.
- The computer will start formatting the hard drive, which can take several minutes or more, depending on the size of the partition (fig. 2.9(h)).

- After the format process has completed, Windows will begin installing the files (fig. 2.9.(i)) and then take you through a wizard to continue with the remainder of the installation and setup.

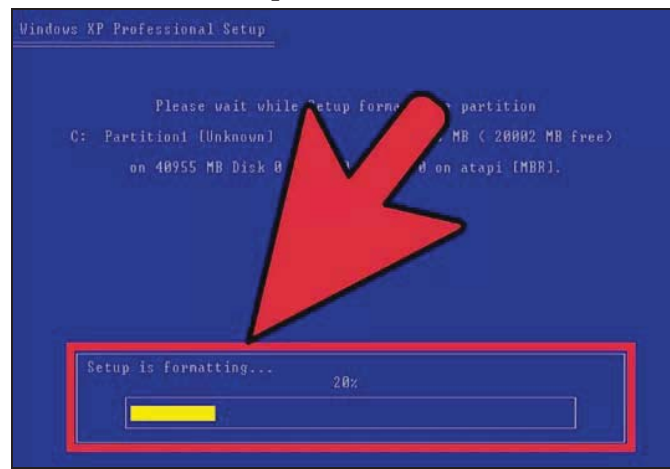


Fig. 2.9.(h)

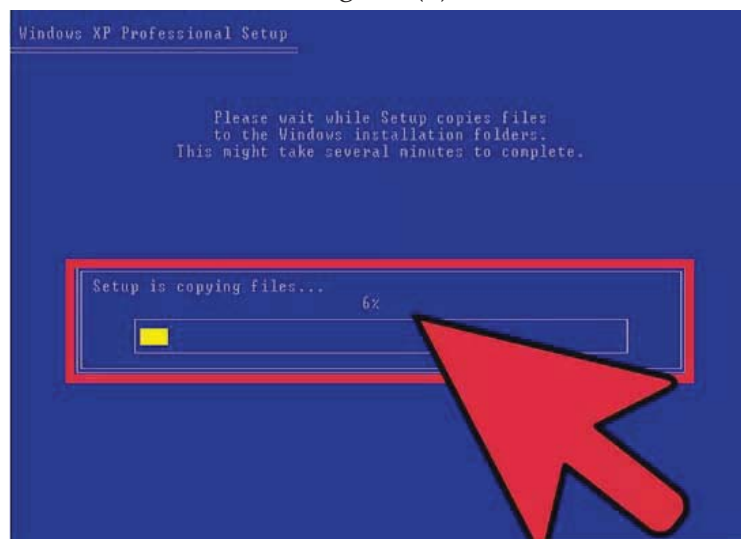


Fig. 2.9. (i)

Step-7:

- Follow the instructions on the screen to complete the Windows XP Setup.
- If you have successfully installed Windows XP, you are finished.



Fig. 2.9. (j)

The remaining three methods for installing Windows XP are clearly explained in the following additional information section.

Additional Information**Introduction to Device drivers**

In computing, a **Device driver** (commonly referred to as a driver) is a computer program that operates or controls a particular type of device that is attached to a computer. A driver provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details of the hardware being used. Fig. 5.9(a) shows the

interaction between the operating system and the device drivers.

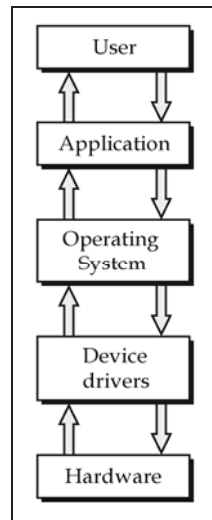


Fig. 2.9 (a)

Drivers are hardware dependent and operating – system – specific. This means that if you download a printer driver but it’s not meant for the printer that you’re using or the operating system that’s installed on your computer, it won’t work.

2.10. STATE THE NEED FOR INSTALLATION OF DEVICE DRIVERS.

- A Device driver acts as a translator between a hardware device and the applications or operating systems that use it.
- So Programmers can write the higher-level application code independently of whatever specific hardware the end-user is using.
- Therefore, device drivers simplify programming.

- Each device has its own set of specialized commands. All the application programs access devices by using generic commands. The device driver accepts the generic commands from a program and then translates them into the corresponding specialized commands for the device. In this way, device drivers simplify programming.

Additional Information

Installing Device drivers

The device driver medium contains driver software for chipset, LAN, audio/video components. The steps to install the driver software are as follows:

1. First of all, the driver DVD is inserted in the optical drive. If the auto-run feature is enabled, the above step displays the opening page of the installer utility. The display of the opening window varies with different motherboard manufacturers. In case of device driver installer for Intel motherboards, the opening window shows a number of options on its left side. Status details of the driver components are displayed on the right side.
2. Selecting the driver by checking the check box activates the Install button at the bottom.
3. Clicking the Install button initiates the installation of the selected device driver in the hard disk.
4. A rebooting of the system is necessary to bring the installed driver software into effect.

2.11. List different types of viruses and ways of removing viruses.

- Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.
- A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk.

- Computer viruses are often spread by attachments in e-mail messages or instant messaging messages.
- **Multipartite Viruses:** Multipartite viruses are distributed through infected media and usually hide in the memory. Gradually, the virus moves to the boot sector of the hard drive and infects executable files on the hard drive and later across the computer system.
- **Direct Action Viruses:** The main purpose of this virus is to replicate and take action when it is executed. When a specific condition is met, the virus will go into action and infect files in the directory or folder that it is in and in directories that are specified in the AUTOEXEC.BAT file PATH. This batch file is always located in the root directory of the hard disk and carries out certain operations when the computer is booted.
- **Overwrite Viruses:** Virus of this kind is characterized by the fact that it deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected. The only way to clean a file infected by an overwrite virus is to delete the file completely, thus losing the original content.
- **Boot Virus:** This type of virus affects the boot sector of a floppy or hard disk. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to boot (start) the computer from the disk. The best way of avoiding boot viruses is to ensure that floppy disks are write-protected and never start your computer with an unknown floppy disk in the disk drive.
- **Macro Virus:** Macro viruses infect files that are created using certain applications or programs that contain

macros. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one

- **Directory Virus:** Directory viruses change the paths that indicate the location of a file. By executing a program (file with the extension .EXE or .COM) which has been infected by a virus, you are unknowingly running the virus program, while the original file and program have been previously moved by the virus.
- **Virus Prevention**
 - The only solution to never risk getting a computer virus is to keep the computer disconnected from the internet and off which is not practical.
 - Keep your operating system up to date.
 - Keep your web browser updated.
 - Keep your software programs updated.
 - Have an Active antivirus client installed that prevents virus infections and keep the program updated.

2.12. List popular Anti-Virus Software available in market

- Kaspersky Anti-Virus
- McAfee AntiVirus Plus
- Symantec Norton AntiVirus
- Bull guard AntiVirus
- Webroot SecureAnywhere AntiVirus
- Bitdefender Antivirus
- Avast Pro Antivirus
- ESET NOD32 Antivirus
- F-Secure Anti-Virus

CHAPTER 3

BASICS OF DATA COMMUNICATION AND OSI REFERENCE MODEL

-: Objectives :-

On completion of the study of the chapter a student should be able to comprehend the following:

- 3.1. Define data communication
- 3.2. Define computer network and state its use
- 3.3. State the need for data communication networking.
- 3.4. Define network topology
- 3.5. List different network topologies
- 3.6. Explain Bus, Star, Ring network topologies
- 3.7. Compare the performances of the above three topologies.
- 3.8. Draw the ISO: OSI 7 layer architecture and explain the functions of each layer.
- 3.9. Draw TCP/IP reference model and explain the functions of each layer
- 3.10. Compare ISO :OSI 7 layer model with TCP/IP reference model

3.0 BASICS OF DATA COMMUNICATION AND OSI REFERENCE MODEL

3.0.1 Introduction

Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

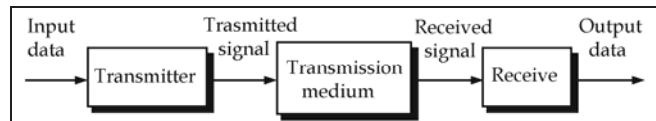


Fig. 3.0

ISO (International Standardization Organization) standard has its own architecture as the OSI (Open Systems Interconnection). The architecture ISO is the first to be defined, and so relatively parallel to the Internet. The distinction between the two is that the ISO formally defines the different layers architecture, while the Internet architecture is applied to achieve a practical environment.

3.0.2. Basic elements of data communication system

Data Communication System is made up of 5 components.

- **Message:** A message is the information (data) to be communicated. It consists of text, numbers, pictures, sound, video or any combination of these.

- **Sender:** The sender is a device that sends the data message. It can be a computer, telephone, handset, video camera and so on.
- **Receiver:** A receiver is a device that receives the message. It can be a computer, telephone handset, video camera and so on.
- **Medium:** A transmission medium is the physical path by which a message travels from sender to receiver. It consists of twisted pair or coaxial cable or fiber optic cable or radio waves etc.
- **Protocol:** A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating just as a person speaking French cannot be understood by a person who speaks only Japanese.

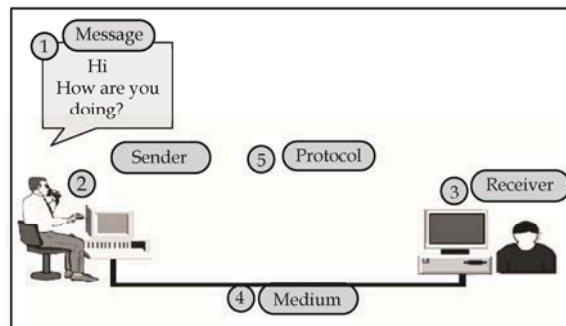


Fig. 3.0. Data Communication System Components

3.1 DEFINE DATA COMMUNICATION

(Oct/Nov-2015; Apr/May-2015; Mar/Apr-2009)

Data communication is defined as “The exchange of data between two computers (or) two devices (or) two persons through transmission medium”.

(or)

Data communication is the exchange of data (in the form of 0's & 1's) between two devices through the transmission medium.

For data communication to occur, the communicating devices must be part of a communication system made up of hardware and software. The effectiveness of a data communication system depends on three fundamental characteristics.

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the device (or) user.
2. **Accuracy:** The system must deliver data accurately.
3. the case of Audio, video and voice data, timely delivering means delivering data as they are produced and without delay Time Lines: The System must deliver data in a timely manner. In.

3.2 DEFINE COMPUTER NETWORK AND STATE ITS USE

- A network consists of two or more of computer systems that are interconnected to each other through the media links (communication channels) for exchange the information is called **computer network**.
- Two computers are said to be interconnected, if they are able to exchange information.
- The major reasons for the use of computer networks are listed below:
 1. Resource Sharing
 2. High reliability of communication
 3. Cost effective

-
4. Mode of communication among widely separated users
 5. Electronic messaging
 6. Transfer file
 7. Share printers
1. **Resource Sharing:** Using computer network it is possible to share the programs, data and other resources among several users on the network can access their data, even if they are at geographically distant location, with the help of computer networks.
 2. **High Reliability of Communication:** High reliabilities achieved by having alternate sources of resources supply.
 3. **Cost Effective:** Computers network allows sharing of resources that is why it is called cost effective.
 4. **Mode of Communication among widely separated users:** Using a computer network, users who are at distance locations can communicate easily. A live example of this is teleconferencing. Tele conferencing allows people to communicate without the need for them to get under a common roof.
 5. **Electronic Messaging:** The most widely used computer network application is electronic mail (E-Mail).
 6. **Transfer file:** To copy the files quickly from one computer to other computer without exchange hard disks.
 7. **Share printer:** Using LAN, we can share the one or more printers among several workstations(computers).

3.3. STATE THE NEED FOR DATA COMMUNICATION NETWORKING.

(Oct/Nov-2013; Mar/Apr-2009)

Data communication networking is necessary to perform the following tasks.

1. Signal Generation
 2. Synchronization
 3. Transmission System Utilization
 4. Error detection and correction
 5. Flow control of data
 6. Addressing
 7. Routing
1. **Signal Generation:** The communicating device must be able to generate and receive the signals. The generated signal is capable of being propagated through the transmission medium and that signal is received by the receiver.
 2. **Synchronization:** The receiver and transmitter must be synchronized unless the receiver will not be able to understand the transmitted signal at the receiving end. Receiver should know when the transmission of data starts and when the data ends.
 3. **Transmission System Utilization:** Transmission system utilization refers to a need to make efficient use of transmission channel, which are generally shared by many communicating devices.
 4. **Error Detection and Correction:** In any communication system, the transmitted signal getting distorted in transmission medium (or) errors introduced by intermediate devices. At the receiver, the errors

present in the transmitted signal are detected and corrected by using error detection and correction methods.

Error detection methods → Parity checking, LRC, VRC, CRC etc.

Error correction methods → Hamming codec, ARQ, etc

5. **Flow Control of Data:** There is a possibility of **transmitter** generating data faster than the receiver device capable of handling. To handle this there should be some kind of *data flow control* mechanism agreed upon between two communicating devices.
6. **Addressing:** When more than two devices share a transmitting facility, a source system must indicate the identity (address) of the destination. The transmission system must send the data to correct destination by using its addressing.
7. **Routing:** The transmission System must ensure that the data being sent (or) routed only to the destination system by using *router*.

Additional Information

Categories Of Computer Networks

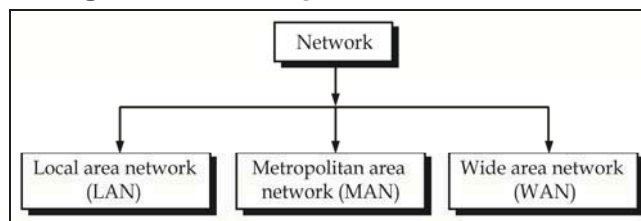


Fig. : Categories of Network

Computer networks mainly classified as Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN). Into which category a network

falls is determined by its size, its ownership, the distance it covers and its physical architecture.

3.4 DEFINE NETWORK TOPOLOGY

3.5 LIST DIFFERENT NETWORK TOPOLOGIES

(Apr/May-2011)

Topology is the layout of the connections formed between the computers.

(or)

Topology defines a physical arrangement of links in a network.

The reliability and efficiency of a network is determined by its structure. The topology is described how the devices in a network are interconnected.

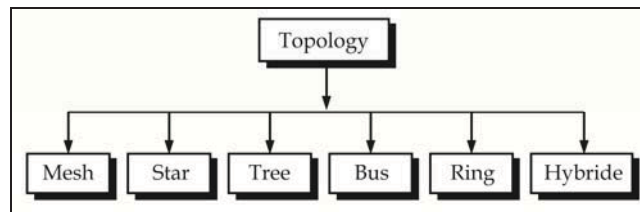


Fig.3.4. Categories of Topology

3.6. EXPLAIN BUS, STAR, RING NETWORK TOPOLOGIES

3.6.1. BUS TOPOLOGY

(Oct/Nov-2015,2013, 2009; Mar/Apr-2013,2008)

- A bus topology is a multipoint configuration. In this topology one single and long cable (acts as a back bone) used to leave all other devices in the network.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection between the device and the main cable. A tap is a connector used to contact with the metallic core of the main cable and drop lines.

- In bus topology any computer can send data to any other computer's because all computers attached to the main cable.

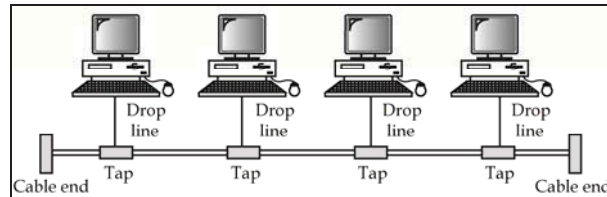


Fig. 3.6 Bus Topology

Advantages:

1. Easy of installation.
2. This topology requires least amount of cables to connect the computers and therefore less expensive.

Disadvantages:

1. A fault or break in the bus cable (Main cable) stops all transmission.
2. The speed of the bus is slow when heavy traffic.

3.6.2. Star Topology

(Oct/Nov-2015,2014,2013,2012, 2009; Mar/Apr-2014,2013,2008)

- In a star topology, each device has a dedicated point to pint link only through a central controller, usually called a hub. The devices are not directly linked to each other.
- A star topology does not allow direct traffic between devices. The controller acts as an exchange. If one device wants to send data to another, it sends the data to the controller, which then deliver the data to the appropriate destination.
- Best example of star topology is telephone network

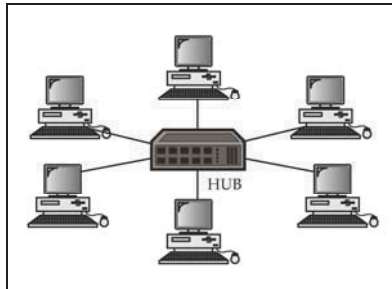


Fig. 3.6 Star Topology

Advantages:

1. Less expensive than Mesh Topology.
2. In a star topology each device needs only one line and only one I/O port.
3. Easy to install and reconfigure.
4. Less cabling is needed.
5. If one link fails, only that link is effected all other links remain active.
6. Fault identification is easy.

Disadvantages:

1. It requires long length of cable.
2. If the central hub is failed the nodes attached to it are all disabled.
3. The cost of hub is high.
4. Message delay.

3.6.3. Ring Topology

(Oct/Nov-2015,2014,2013,2012; Mar/Apr-2014,2013,2008)

- In a ring topology, each device has a dedicated point to point line configuration. All devices are connected point to point in the shape of ring. A signal is passed along the ring in one direction from device to device until it reaches its destination.

- Each device in the ring can act as a repeater because each device in a ring receives the signal and regenerates the bits and then send to the another device.

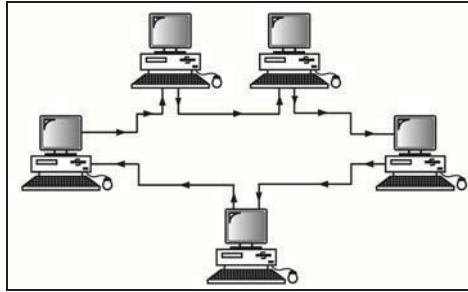


Fig. 3.6 Ring Topology

Advantages:

1. Easy to install and reconfigure.
2. Fault identification is easy.
3. A signal can travel long distance because each device in a ring can acts as a repeater.


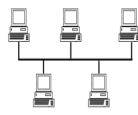

Disadvantages:

1. It is a unidirectional.
2. If anyone device fails in the ring topology the entire network fails.
3. Time delay of the signal is more.

3.7 COMPARE THE PERFORMANCES OF THE ABOVE THREE TOPOLOGIES.

(Oct/Nov-2013)

S.No	Parameter	STAR	BUS	RING
1	Installation cost	moderate	low	low
2	Fault detection	Easy	Difficult	Difficult

3	Single node failure	Whole network not failure only failure node disconnected	Whole network not failure only failure node disconnected	Whole network failure
4	Network robustness	Moderate	Low	Low
5	Reconfiguration	Easy	Easy	Difficult
6	Connection media	Twister pair	Optical fiber or coaxial cable	Optical fiber or coaxial cable
7	Device adding	Easy	Easy	Easy
8	configuration figure			

3.8 DRAW THE ISO: OSI 7 LAYER ARCHITECTURE AND EXPLAIN THE FUNCTIONS OF EACH LAYER.

3.8.1. 7- LAYER OSI ARCHITECTURE

(Apr/Ma-2015;Mar/Apr-2013, Oct/Nov-2008)

- Open System Interconnection (OSI) was developed by ISO (International Standard Organization) in 1983, for sending and receiving of data, between two computers.
- It deals with connecting open system i.e., system that follow a standards are open for communicating with other systems, irrespective of a manufactures.

- OSI represents a concept of Intel process communication so that any open system may be able to communicate with another open system.
- The OSI architecture decomposes the communication process into functional layers. Each layer is responsible for performing special functions. Therefore, OSI architecture is reference model to all open system inter connections.
- OSI reference model consists of 7 layers, as shown in Fig. 3.8 (a).

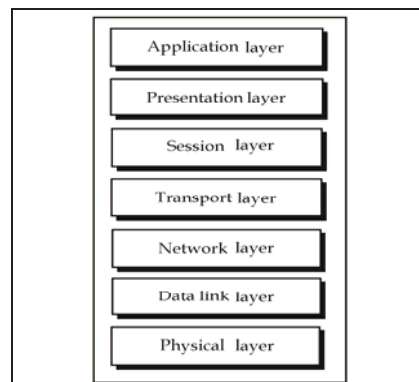


Fig. 3.8: OSI reference model

3.8.2. FUNCTIONS OF EACH LAYER IN OSI ARCHITECTURE

(Oct/Nov-2015,2014,2012, 2010,2009;Apr/May-2014,2011)

Data Transmission from Source to Destination Through Different Layers of OSI.

- **Application Layer:** It provides end user for processing of data and supports for services such as e-mail, file transfer, shared data management, network software services and other types of distributed information services. This layer acts as an interface between end user

and network. This layer mainly allows access to network resources.

- **Presentation Layer:** Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. It translates the Application into network format and vice versa. It provides format and encrypt / decrypt data to be send across a network.

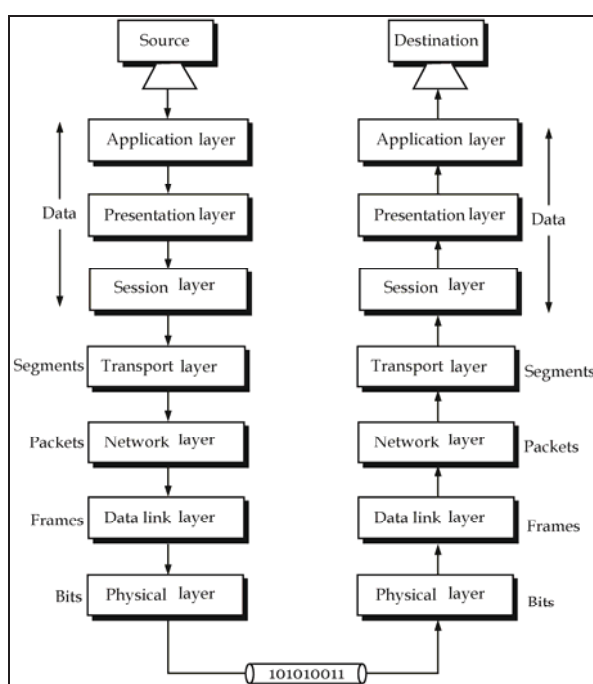


Fig 3.8: OSI Architecture

- **Session Layer:** It allows to establish, maintains and disconnect between communicating systems. It allows the communication between two devices either in simplex or half duplex mode of transmission. It allows a

process to add checkpoints (Synchronization points) into a stream of data.

- **Transport Layer:** The transport layer is responsible for source to destination (end-to end) delivery of the entire message. This layer converts data into smaller “segments” for sending and at the receiving end the segments are converted into original data. This layer is also responsible for error control and flow control.
- **Network Layer:** This layer converts data segments into packets and at the receiving end, the packets are converted into data segments. This layer determines paths (routing) for transmitting data from source to destination.
- **Data Link Layer:** This layer converts data packets from network layer into frames and at the receiving end, this layer converts frames into packets.

The data link layer divides the stream of bits received from the network layer into manageable data units called frames. If frames are to be distributed to different system on the network. The data link layer adds a header to the frame to define the physical address of the sender (source address) and receiver (destination address) of the frame.

Data link layer receives the data to be sent from the network layer, adds header and trailer to it which is now known as a **frame**. This frame is then transmitted to the physical layer.

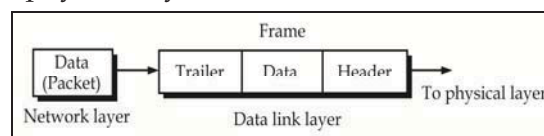


Fig. 3.8 (a): Role of Data Link Layer

- **Physical Layer:** The physical layer is responsible for transmitting raw bits over a communication channel.

It converts frames from the data link layer into bits and at the receiving end, bits from the physical layer is given to the data link layer.

For sending raw bits from source to destination, to do this, the source and destination nodes have to agree on a number of factors such as what voltage constitute a bit value '0' what voltage constitute a bit value '1', what is the bit interval, whether the communication is in only one direction or both the directions simultaneously i.e., simplex, half duplex or full duplex and so on.

The functions of physical layer are: Signal encoding, Medium, Bit Synchronization, Transmission Byte, Transmission mode, Multiplexing .

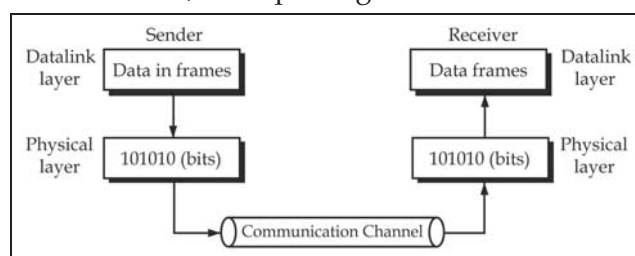


Fig. 3.8.(b): Relation of Physical Link Layer with Communication Channel

3.9 DRAW TCP/IP REFERENCE MODEL AND EXPLAIN THE FUNCTIONS OF EACH LAYER

(Oct/Nov-2015,2013; Apr/May- 2011, Mar/Apr-2008)

The Transmission control protocol/Internet Protocol (TCP/IP) suite of protocols forms the basis of the Internet. TCP/IP was developed in early 1970s.

The TCP / IP is a set of protocols that describes how all transmissions are to be handled across the internetwork. The

TCP / IP has been used to provide effective delivery of information around the world.

Layers present in TCP / IP do not match exactly with those in OSI. TCP / IP suit consists of five layers. The TCP / IP reference model does not have session or presentation layers.

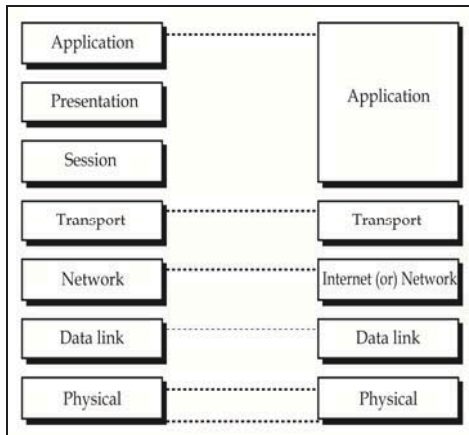


FIG 3.9 Layers in TCP / IP and OSI

3.9.1. FUNCTION OF EACH LAYER IN TCP/IP

(Mar/Apr-2013,2009; Oct/Nov-2012,2011,2009;Apr/May-2012)

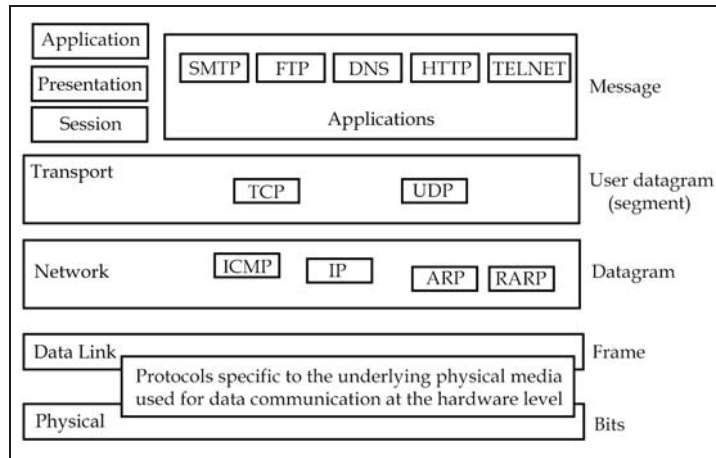


FIG 3.9.1: Layers and protocols in TCP/IP

The IP portion of TCP/IP deals with this layer routes and forward a data gram to the next hope. But it is not responsible for accurate and timely delivery of all data grams to the destination in a proper sequence.

Various other protocols are defined in this layer. They are address resolution protocol. The ARP takes IP address of host as input and gives its corresponding physical address has output. The RARP takes physical address as input and gives IP address has output. The ICMP is a error reporting protocol which gives the messages.

TCP/IP reference model have five layers. They are

1. **Application Layer:** It is used to access the network for providing applications such as DNS, TELNET, FTP, HTTP.
2. **Transport Layer:** It provides end-to-end data transmission. It also provide flow control and error control. In TCP / IP, transport layer is represented by two types of protocols.
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)

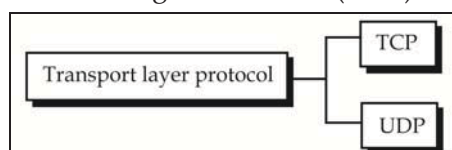


FIG 3.9.1 (a): Transport Layer Protocols on the Internet

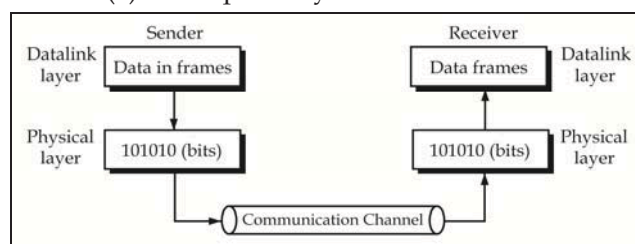


Fig 3.9.1 (b): Relation of Physical Link Layer with Communication Channel

-
- **TCP:** It is a reliable connection oriented protocol i.e., connection must be established between both ends of a transmission, before they transmits data. TCP is makes the Internet reliable. TCP subdivides the incoming message stream of bytes into manageable discrete messages and transmits these into network (internet) layer. At destination, the TCP reassembles the received messages into the original form.
 - **UDP:** It is a unreliable, connection less protocol, widely used for client-server applications where speed of delivery is more important than accurate delivery. In multimedia transmissions or voice, transmission speed is a major concern than accurate delivery of the message.
3. **Internet Layer (or) Network Layer:** At network layer, the main protocol defined by TCP / IP is Internet protocol (IP). Internet Layer is concerned with routing of data. The job of the Internet layer is to deliver I P packets to the destination.
 4. **Data Link Layer:** This Layer converts data packets from network layer into **frames** and at the receiving end, this layer converts frames into packets. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. If frames are to be distributed to different system on the network.
 5. **Physical Layer:** The physical Layer is responsible for transmitting raw bits over a communication channel. It converts frames from data link layer into bits. These bits are sending from source to destination through the communication channel.

3.10 COMPARE ISO: OSI 7 LAYER MODEL WITH TCP/IP REFERENCE MODEL

BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	TCP/IP- Transmission Control Protocol/ Internet Protocol	OSI- Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
No. Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Usage	Mostly used	Never used

OR

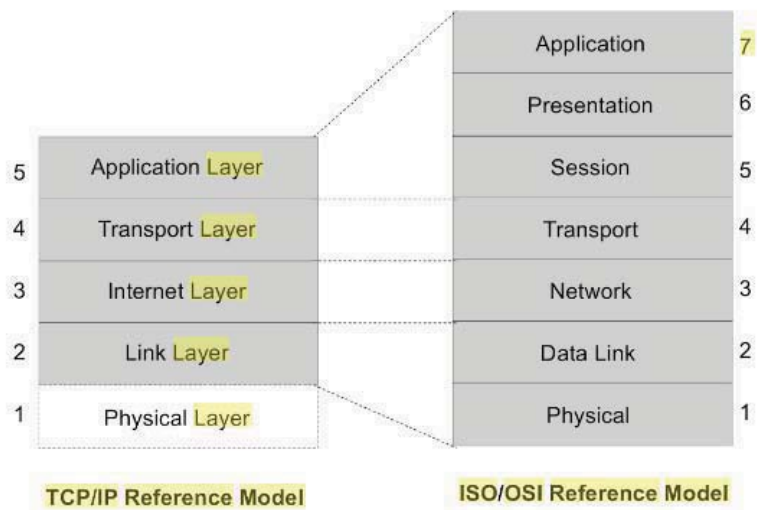
	OSI	TCP
1.	7 layers	4 layers
2.	Model was first defined before implementation takes place.	Model defined after, protocol were implemented.
3.	OSI model based on three concept i.e. service, interface and protocol.	TCP/IP model did not originally clearly distinguish between service, interface and protocol.
4.	OSI model gives guarantee of reliable delivery of packet.	Transport layer does not always guarantee the reliable delivery of packet.
5.	OSI does not support internet working.	TCP/IP support.
6.	Strict layering.	Lossely layered.
7.	Support connectionless and connection - oriented communication in the network layer.	Support only connection - oriented communication in the transport layer.

The layers, TCP/IP, has are:

- Network Interface Layer,
- Internet Layer,
- Transport Layer,
- Application Layer.

The seven layers of the model are:

- Application Layer,
- Presentation Layer,
- Session Layer,
- Transport Layer,
- Network Layer,
- Data Link Layer,
- Physical Layer.



CHAPTER 4

PHYSICAL LAYER AND DATA LINK LAYER

-: Objectives :-

On completion of the study of the chapter a student should be able to comprehend the following:

a) Physical Layer:

- 4.1. List the different types of physical transmission media used in networking
- 4.2. Explain the cross sectional diagrams of UTP, STP, Coaxial and Fiber optic cable and their use in networking
- 4.3. List the three types of switching techniques used in networking
- 4.4. Explain circuit switching and packet switching
- 4.5. Define virtual circuit and datagram approaches in packet switching
- 4.6. State the use of repeater/ hub

b) Data Link Layer:

- 4.7. Define the word protocol used in computer networks
- 4.8. State the need for protocols in computer networks.
- 4.9. Explain CSMA/CD and CSMA/CA.
- 4.10. Explain Ethernet LAN and its frame format
- 4.11. Explain the working of token ring network
- 4.12. Explain the topology of wireless LAN and explain its frame format (IEEE 802.11)
- 4.13. Know about CAN and SkyWAN
- 4.14. Explain the features of Bluetooth technology.
- 4.15. Explain the use of switch, bridge in constructing networks
- 4.16. Differentiate between repeater, switch and bridges.

4.1 LIST THE DIFFERENT TYPES OF PHYSICAL TRANSMISSION MEDIA USED IN NETWORKING

(Oct/Nov-2010)

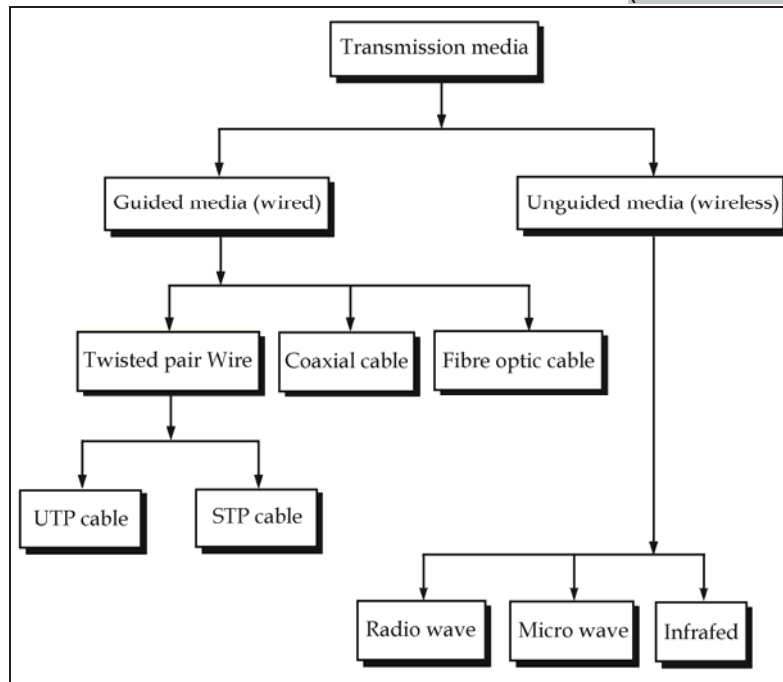


Fig. 4.1 Categories of Transmission Media

Transmission media are the physical infrastructure components, which carry data from one computer to another computer. They are at the basis of data communications. Examples of simple forms of transmission media are telephone wires that connect telephones to the central offices (i.e., telephone exchanges) and coaxial cables that carry cable television transmission to homes. Transmission media need not always be in the form of a physical wire they can be invisible as well. Broadly, all transmission media can be divided into the following categories as shown in Fig. 1.9.

4.2 EXPLAIN THE CROSS SECTIONAL DIAGRAMS OF UTP, STP, COAXIAL AND FIBER OPTIC CABLE AND THEIR USE IN NETWORKING.

4.2.1. Twisted pair wires

(Mar/Apr-2014, 2012,2008;Apr/May-2011)

Twisted pair wires are mainly used for carrying voice and data signals. There are two classes of twisted pair wires.

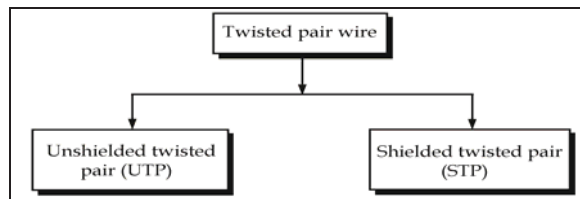


Fig. 4.2.1.(a) Categories of Twisted Pair Wire

1. Unshielded Twisted Pair (UTP):

This is the most commonly used medium today, due to its usage in the telephone system; this cable can carry both voice as well as data. The unshielded twisted pair cable mainly consists of two conductors (usually copper). Earlier the wires used to be kept parallel; however, this resulted in far greater levels of noise. Hence, the wires are normally twisted. This results in the reduction of noise to a great extent, although it is not eliminated completely. The copper conductors are covered by PVC or some other insulator.

UTP is flexible, cheap and easy to install. Electronic Industries Association (EIA) has developed standards for UTP cables. Each one is manufactured differently for a specific purpose.

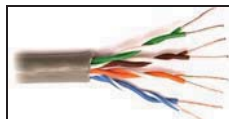


Fig. 4.2.1.(b) Unshielded Twisted Pair (UTP) Cables

Advantages:

1. It is cheap.
2. Flexible
3. Easy to install
4. Easy to use

Disadvantage:

1. Cross talk is present

2 . Shielded Twisted Pair (STP):

STP cable has a metal shield covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or cross talk. It is Bulkier and Expensive.

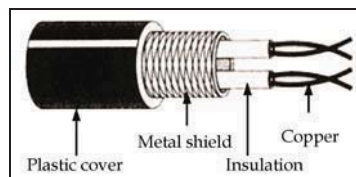


Fig. 4.2.1.(c) Shielded twisted pair (STP) Cable

Advantages:

1. Flexible
2. Cross talk is eliminated
3. Easy to install.
4. Easy to use.

Disadvantages:

1. Cost is high
2. Bulkier

applications of twisted pair cables

1. Voice communication
2. Data communication
3. Can handle data speed of 100 Mbps

4. Suitable for voice and data communication
5. Used in telephone networks

Note: Categories of unshielded twisted pair cables:

Category	Usage
1.	The basic cable used in the telephone system. This is fine for voice communication, but is unsuitable for data communication, except at very low speed.
2.	Suitable for voice and data communication up to the speed of 4 Mbps.
3.	Can carry voice and data up to 10 Mbps. It requires minimum three twists per foot. Today, these are more regularly used in telephone networks.
4.	These are similar to the category 3, but can handle data up to 16 Mbps.
5.	Can handle data speed of 100 Mbps.

4.2.2. COAXIAL CABLE

(Mar/Apr-2014, 2012,2008;Apr/May-2011; Oct/Nov-2012,2010)

Coaxial cable (also called coax) has an inner central conductor surrounded by an insulating sheath, which in turn is enclosed in an outer conductor shield. This outer conductor is covered by a plastic cover.

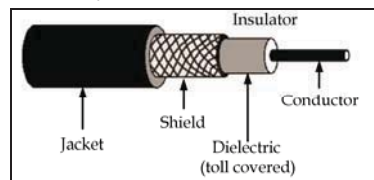


Fig. 4.2.2.(a) Co-axial Cable

As compared to UTP & STP, coaxial cable is more expensive, less flexible and more difficult to install in a

building where a number of twists and turns are required. It is much reliable and can carry far higher data rates.

Co-axial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

Category	Impedance	Use
RG - 59	75 Ω	Cable TV
RG - 58	50 Ω	Thin Ethernet
RG - 11	50 Ω	Thick Ethernet

Table: Coaxial Cable Standards

Advantages:

1. High Data rates.
2. High Bandwidth.
3. Cross talk is less

Disadvantages:

Bandwidth and data rate is low compared to fiber optic cable

Applications of co-axial cables

1. Used in cable TV
2. Used for data and voice communication
3. Used in thick Ethernet and thin ethernet

4.2.3. FIBER OPTIC CABLE

(Mar/Apr-2014, 2012,2008;Apr/May-2011; Oct/Nov-2012,2010)

Fiber Optic Cable is a combination of plastic and glass or glass or plastic which is capable of transmitting information voice, video, data in the form of light. An optical fiber consists of core, cladding and protecting cover.

Core and cladding materials are made of glass or plastic and the protecting cover is made of steel or fiber glass or plastic.

Fiber Optic communication works on the principle of total internal reflection. The light ray totally reflects back in the same medium is known as "Total Internal reflection.

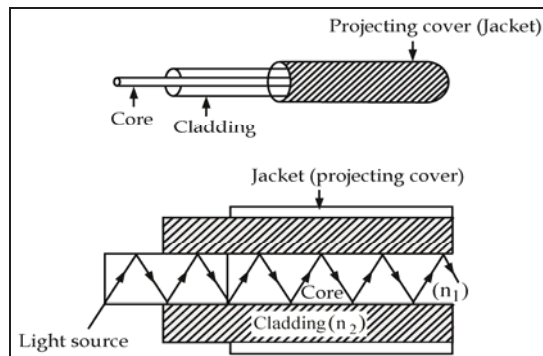


Fig. 4.2.3. Fiber Optic Cable

Advantages of Fiber Optic Cables:

The following are the advantages of optical fiber cables in communication.

- 1. High Information Capacity:** Optical fiber communication systems have much information capacity than metallic cables due to large band-width available with optical frequencies optical fibers are available with bandwidth up to 10 GHz.
- 2. More Secure:** Optical cables are more secure than copper cables. It is impossible to tap into a fiber cable without the user's knowledge. For this reason optical fibers are used in military applications.
- 3. Less repeaters are required:** Fiber optic cables have less loss and hence require less number of repeaters between transmitters and receivers.

4. **Less expensive:** Fibers Optic Cables are less expensive than copper cables. This is because many miles of optic cables are easier and less expensive to install than the same amount of copper cables.
5. **Resistant to electric shock:** Fiber optic do not cause electric shocks because they do not carry electricity.
6. **Less Interference:** Fiber optics use light signals instead of electricity the signal do not interfere with each others.
7. **Digital transmission:** Computer networks need digital information since fiber optic cables send information digitally.
8. **High Speed:** It uses light waves for communication of extremely high frequency signals of about 13×10^6 GHz. Hence it has high speed.
9. **Small in Size:** Due to small in size, large number of optical fibers can be fitted in small cable.
10. It has less attenuation over a very long distance than copper cables.
11. Light in Weight
12. These are more flexible and strong.

Applications of Optical Fibers

Optical fibers are used in:

1. Cable TV System.
2. Tele Communication.
3. Communication network for LAN & MAN.
4. Ethernet & Giga bit Ethernet.
5. Local Telephone and long distance telephone lines.
6. Aircraft Communication.
7. Secure Communication systems of military bases.

8. College campus communication.
9. Closed circuit TV (CCTV) Systems
10. Inter connection of measuring and monitoring instruments in industrial plants & laboratories
11. Ship board communications.
12. Under ocean communication.

4.3 LIST THE THREE TYPES OF SWITCHING TECHNIQUES USED IN NETWORKING

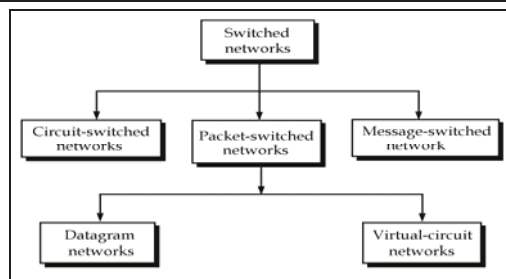


Fig. 4.3 Types of Switched Network

A switched network is made up of a number of interlinked nodes, called switches. A switch is a hardware (as well as software) device that allows a connection to be established between two or more devices.

4.3.1. Differences Between Circuit, Packet And Message Switching Techniques Used In Networking

S.No	Circuit switching	Message switching	Packet switching
1.	Dedicated Transmission path	No dedicated transmission path	No dedicated transmission path
2.	Continuous transmission	Transmission of message	Transmission of packets

	of data		
3.	Operates in real time	Not real time	Near real time
4.	Message not stored	Message stored	Message held for short time
5.	Path established for entire message	Route established for each message	Route established for each packet
6.	Call setup delay	Message transmission delay	Packet transmission delay
7.	Busy signal if called party is busy	No busy signal	No busy signal
8.	Blocking may occur	Blocking may not occur	Blocking may not occur
9.	User responsible for message-loss protection	Network responsible for loss messages.	Network responsible for each packet but not for entire message.
10.	No speed or code conversion	speed and code conversion	speed and code conversion
11.	Fixed bandwidth transmission (i.e., fixed information)	Dynamic use of bandwidth	Dynamic use of bandwidth

	capacity)		
12.	No overhead bits after initial setup delay	Overhead bits in each message	Overhead bits in each packet

4.4 EXPLAIN CIRCUIT SWITCHING AND PACKET SWITCHING

4.4.1. CIRCUIT SWITCHING

(Oct/Nov-2014,2008; Mar/Apr-2008)

- In Circuit Switching, a **dedicated path** is established between two computers. That means, the direct physical connection path is established between sender and receiver to send data, no other computer is sharing that connection for that time slot until the sender and receiver stop communicating. This is similar to a telephone call.
- **For example:** when you call up somebody over the phone, a dedicated connection is established between your phone and the phone of the other person through various exchanges or switches. This dedicated connection continues until the call is complete.
- A circuit switch is a device with 'm' inputs and 'n' outputs. It creates a "temporary dedicated connection between an input device and an output device".

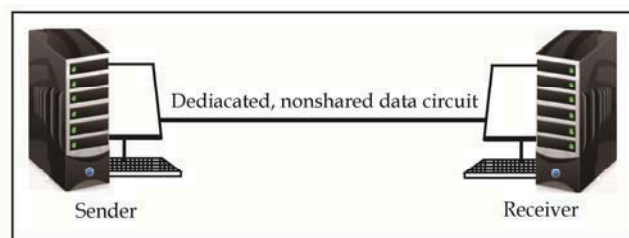


Fig 4.4.1

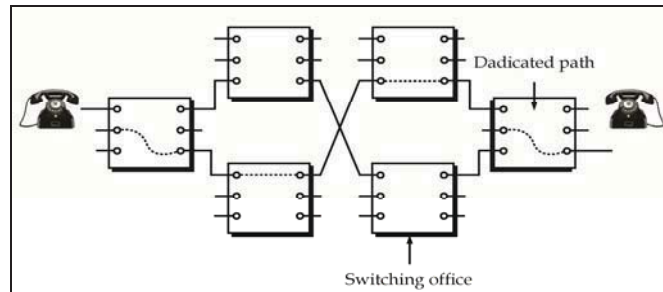


Fig. 4.4.1.(a): Circuit Switching

- Circuit Switching was mainly used for telephone communications. In telephone calls, this type of temporary dedicated connection is very useful for the duration of the call.
- However, for computer to computer communications, circuit switching is not so efficient, this is because, unlike conversations between humans (which are continuous once started), a computer might send some data to another, and they may not send any more data for quite some time. That is, communication between computers is less predictable and occurs in bursts. This means that if a dedicated line is established between the two computers, chances are that this line may not be utilized most of the time. Another problem with circuit switching is that once a connection is established, that connection is used throughout the session of the conversation.

Advantages of Circuit Switching:

- The circuit is very simple.
- Once the circuit is established, the network is effectively transparent to users.
- The delay at each node is negligible.

Disadvantages of Circuit Switching:

- Circuit Switching is inefficient.
- Channel capacity is not properly utilized.
- There is a delay prior to signal transfer or call established.
- Channel capacity must be reserved between each pair of nodes in the path. Channel is dedicated for the duration of the connection.
- It is suitable for voice communication but not for data communication.
- Less flexible.

4.4.2. PACKET SWITCHING

(Oct/Nov-2008; Mar/Apr-2008)

- Considering all the limitations of circuit switching, packet switching has developed as the standard switching technology for computer to computer communication.
- In Packet switching, no dedicated path is established more time and all the packets belongs to same message need not go by one route to reach the destination. The packet can go from different paths to reach destination with orderly.
- In packet switching, data are transmitted as discrete blocks, called packets, which are potentially variable length. Each packet contains data to be transferred and also the control information such as the sender's address and the destinations address.

The packet switching networks allow any computer to send data to any other computer without reserving the circuit. Multiple paths between a pair of sender and receiver may exist in a packet switched network.

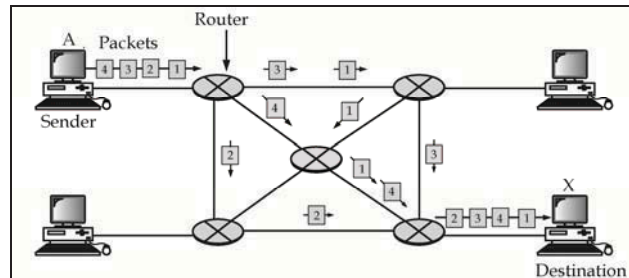


Fig. 4.4.2 Packet switching (datagram packet switching)

One path is selected between source and destination. Whenever the sender has data to send, it converts them into packets and forwards them to next computer or router. The router stores this packet till the output line is free.

Then this packet is transferred to next computer or router. This way, it moves to the destination. All the packets belonging to a transmission may or may not take the same route. The route of a packet is decided by network layer protocols.

Packet switching can be classified into two types: They are

- **Datagram Approach:** In the datagram approach of packet switching, each packet is sent to source to destination through different routes.
- **Virtual Circuit Approach:** A single route is chosen between the source and the destination before all packets belonging to the same message take the same route from the source to destination.

Datagram And Virtual Circuit Approaches In Packet Switching

(Oct/Nov-2013)

- In packet switching networks, any computer to send data to any other computer without reserving the physical path. In packet switching, data are transmitted

as discrete blocks, called packets, which are potentially variable length. Each packet contains data and also the control information such as the sender's address and the destination address.

- **Packet switching can be classified into two types:**
They are
 1. **Datagram** Packet switching
 2. **Virtual Circuit** Packet switching

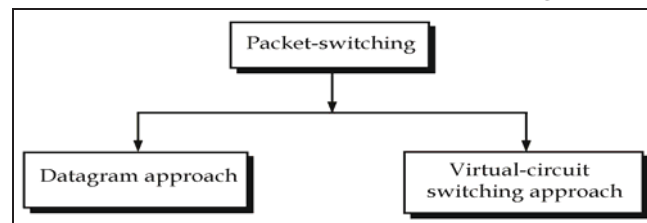


Fig. 4.4 Types of Packet Switching

Datagram Packet switching:

- In Datagram Packet switching no dedicated path is established and all the packets belongs to same message need not go by one route to reach the destination. The packet can go from different paths to reach destination with orderly.
- The packets in this approach are called **datagrams**. Every packet contains source and destination address.
- In the datagram approach of packet switching, each packet is sent to source to destination through different routes. Fig. Shows the how datagram packet switching network is used to deliver four packets from source 'A' to destination 'D'. All the four packets belongs to same message but they may transmitted through different routes to reach the destination i.e destination 'D' via by different routers.

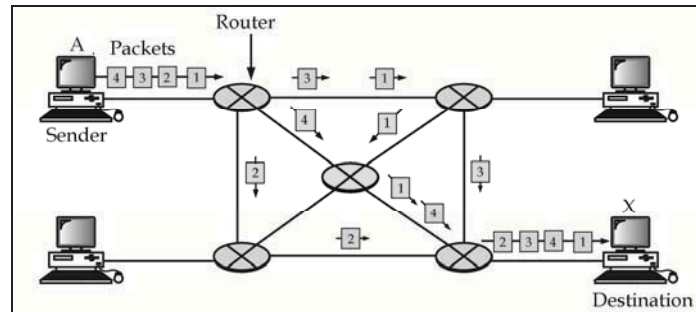


Fig. 4.4.2. (a): A Datagram Network

Virtual Circuit Packet switching :

- The virtual circuit packet switching is different from the datagram packet switching. In virtual circuit approach, all packets belonging to the same message transmitted from source to destination through same route.
- A single pre-planned route is chosen between the source to destination before packets are transmitted based on the network conditions. Example of virtual circuit approach as shown in Fig.4.4.2. (b).

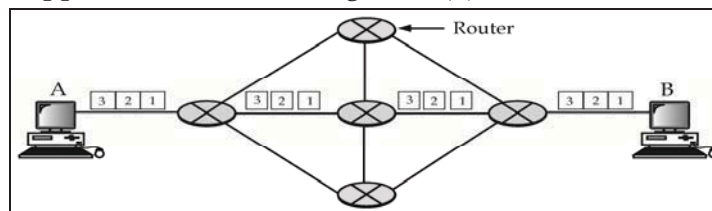


Fig 4.4.2. (b) : A Datagram Network

FIG 4.4.2.(b): In virtual switching packets are transmitted from 'A' to 'B' through pre-planned route is established before packets are transmitted.

4.4.3.DIFFERENCES BETWEEN CIRCUIT AND PACKET SWITCHINGS

(Mar/Apr- 2013,2009,2008;Apr/May-2010; Oct/Nov-2011,2010)

S.No	Circuit Switching	Packet Switching
1.	Dedicated path is established between transmitter & receiver	No dedicated path established between transmitter & receiver
2.	Continuous transmission of data	Transmission of packets
3.	Message not stored	Message are stored
4.	Call set-up delay	Packet transmission delay
5.	Busy signal if called party is busy	No busy signal
6.	Blocking may occur	Blocking can not occur.
7.	Fixed Band width	Dynamic usage of Bandwidth
8.	Message loss - users responsibility	Message loss - network Responsibility
9.	Speed is less	Speed is more
10.	It is mainly used for voice	It is mainly used for data i.e. (non voice applications).

4.5 DEFINE VIRTUAL CIRCUIT AND DATAGRAM APPROACHES IN PACKET SWITCHING

4.5.1. Datagram And Virtual Circuit Approaches In Packet Switching

(Oct/Nov-2013)

- In packet switching networks, any computer to send data to any other computer without reserving the physical path. In packet switching, data are transmitted

as discrete blocks, called packets, which are potentially variable length. Each packet contains data and also the control information such as the sender's address and the destination address.

- **Packet switching can be classified into two types: They are**

3. **Datagram** Packet switching

4. **Virtual Circuit** Packet switching

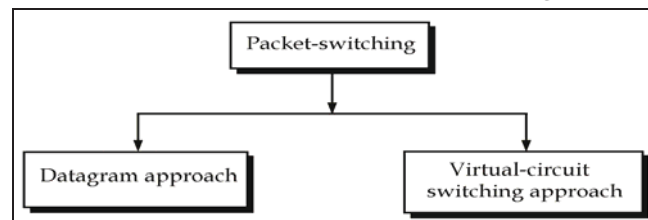


Fig. 4.5.1 Types of Packet Switching

Datagram Packet switching:

- In Datagram Packet switching no dedicated path is established and all the packets belongs to same message need not go by one route to reach the destination. The packet can go from different paths to reach destination with orderly.
- The packets in this approach are called **datagrams**. Every packet contains source and destination address.
- In the datagram approach of packet switching, each packet is sent to source to destination through different routes. Fig. Shows the how datagram packet switching network is used to deliver four packets from source 'A' to destination 'D'. All the four packets belongs to same message but they may transmitted through different routes to reach the destination i.e destination 'D' via by different routers.

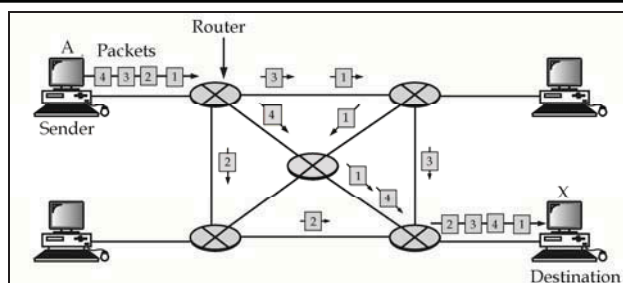


Fig. 4.5.1 (a): A Datagram Network

Virtual Circuit Packet switching:

- The virtual circuit packet switching is different from the datagram packet switching. In virtual circuit approach, all packets belonging to the same message transmitted from source to destination through same route.
- A single pre-planned route is chosen between the source to destination before packets are transmitted based on the network conditions. Example of virtual circuit approach as shown in Fig.4.5.1 (b).

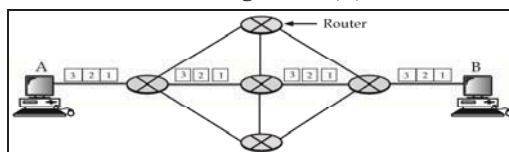


Fig 4.5.1 (b) : A Datagram Network

FIG 4.5.1(b): In virtual switching packets are transmitted from 'A' to 'B' through pre-planned route is established before packets are transmitted.

4.6 STATE THE USE OF REPEATER/ HUB

(Oct/Nov-2015; Mar/Apr-2015)

Use of repeater/Hub:

A repeater, also called a regenerator, is an electronic device that simply regenerates a signal. It works at the physical layer of the OSI reference architecture.

Signals travelling across a physical wire travel some distance before they become weak (in a process called attenuation), or get corrupted as other signals noise interfere. A repeater receives such a signal, which is likely to have become weak or corrupted, and regenerates it.

Example: Computer works on a convention that 5 volts represent 1 and '0' volts represent '0'. If the signal becomes weak (distorted and the voltage becomes 4.5, the repeater has the intelligence to realize that it is still a bit 1 and therefore, it can regenerate the bit (i.e., 5 volts). That is, the repeater simply recreates the bit pattern of the signal and puts this regenerated signal back on to the transmission medium. In effect, the original signal is created once again.

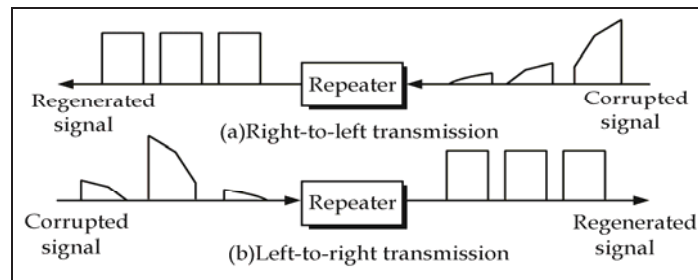


Fig. 4.6. Repeater

The only responsibility of a repeater is to take a stream of bits, in the form of a signal, regenerate it so that the signal is accurate now and send it forward. It does not perform any intelligent functions.

Working of repeater/Hub:

For instance, in the sample network (LAN) as shown in Fig.4.6. Host A wants to send a packet containing the bit stream 01100110 to host D. Note that the two hosts are on the same LAN, but on different portions of the LAN. By the time the signal sent by host A can reach host D, it becomes very weak. Therefore, host D may not be able to

get it in the form of the original signal. Instead, the bits could change to say 01100111 before the signals reaches host D. Of course, at a higher level, the error control functions would detect and correct such an anomaly. However, even before this can happen, at the lowest level, the repeater simply prevents this from occurring by taking the input signal corresponding to bits 01100110, regenerating it to create a signal with the same bit format and the original signal strength, and sending it forward.

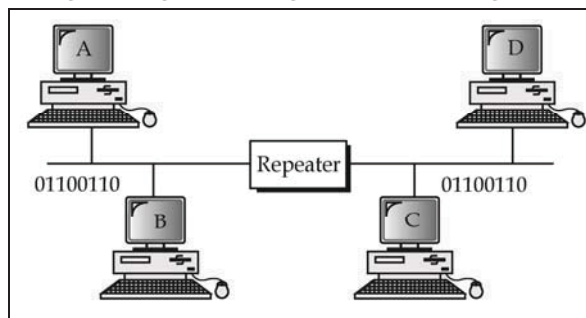


Fig. 4.6. (a) : Repeater Regenerating a Signal

Note: Difference between repeater and amplifier

People sometimes confuse repeaters and amplifiers. However, they are different. An amplifier is used for analog signals, where it is impossible to separate the original signal and the noise. An amplifier, therefore amplifies an original signal as well as the noise in the signal, as it cannot differentiate between the two. On the other hand, a repeater knows that the signal has to be identified as either 0 or 1 only. Therefore it does not amplify the incoming signal ; it regenerates the original bit pattern.

b) Data Link Layer:

4.7 DEFINE THE WORD PROTOCOL USED IN COMPUTER NETWORKS**4.8 STATE THE NEED FOR PROTOCOLS IN COMPUTER NETWORKS.**

- A protocol is a set of rules that governs data communication. It represents an 'agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.
- What is communicated, how it is communicated and when it is communicated is termed as "protocol".

Need of Protocols:

- Everything is ok. and the train can start by a green flag is also a protocol.
- When we write a letter, we follow a certain protocol the place where we write the address, the place where we write the name of the recipient and the way we write your's lovingly or yours sincerely etc. All define a protocol.

The key elements of a protocol are **syntax, semantics, timing.**

1. **Syntax (What is to be communicated ?):** Syntax refers to the format or structure of the data, meaning the order in which they are presented.
2. **Semantics (How it is to be communicated?):** Semantics refers to the meaning of each station of bits.
3. **Timing (When it is to be communicated ?) :** Timing refers to two characteristics, they are :
 - When data should be sent.
 - How fast they can be sent.

4.9 EXPLAIN CSMA/CD AND CSMA/CA.

4.9.1. CARRIER SENCE MULTIPLE ACCESS(CSMA)

(Oct/Nov-2013;Apr/May-2012;2010;Mar/Apr-2013,2009,2008)

All the Stations share a common communication channel for transmitting their data. A station can transmits its data on a channel, when a transmission is in progress. If another station also send their data through a same channel, at that time, collision (overlapping) of two stations data. If collision occurs, some of the transmissions data are lost and also available channel time is wasted as shown in Fig. 4.9(a).

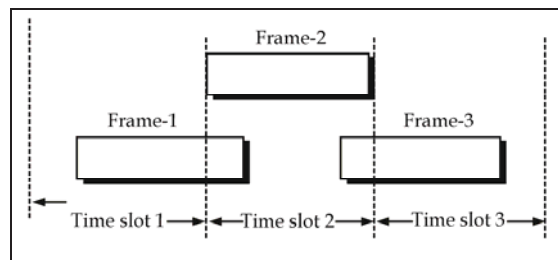


Fig. 4.9.(a)Collision of Frames

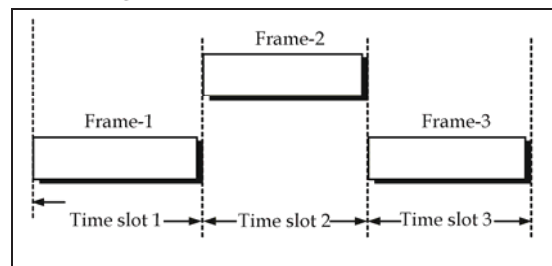


Fig. 4.9.(b) Without Collision of Frames

Fig. 4.9.(b) shows that Wasted channel time due to collision can be reduced when the channel time is divided into time slots (like TDM) and the stations are allowed to transmit at specific instants of time, so that all transmissions arrives aligned with a time slot boundaries.

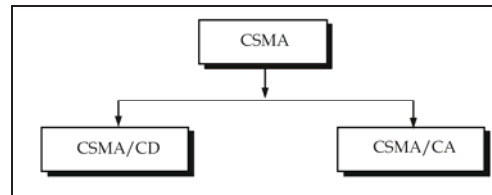


Fig. 4.9.(c).Types of CSMA

Working of CSMA

When all the stations can share a common communication channel for transmitting their data, a collision may occur. A collision can be avoided by using CSMA. In CSMA the “Carrier sense” means detecting presence or absence of a data on a common communication channel and “Multiple access” means multiple users can access, (or) share common communication channel.

In CSMA, a station checks a common communication channel either it is busy or idle (idle means no data present in the channel) before sending its data. If there is a carrier (data) on the channel, it does not commence its transmission. If the channel is idle (free) it transmits its own data through the channel. That is why it is called “CSMA”. All the stations sending their data through a common communication channel without collision based on this principle. In CSMA an algorithm is needed to specify when a station can transmit. Once the channel is found busy because there can be several stations waiting to transmit.

These can be several Approaches as described below:

1. I-Persistence Method
2. Non-persistence Method
3. P-Persistence Method

1. I-Persistence Method: In this scheme, when a station wants to transmit its frame, it checks the medium

continuously until the medium is free and then it transmits immediately.

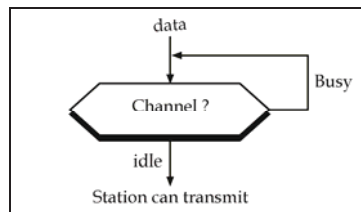


Fig. 4.9.(d).Persistence Method

This method has the highest chance of collision because two or more stations may find channel idle and send their frames immediately, at that time collision occurs.

2. **Non - Persistence Method:** In this scheme, a station that has a frame to send, checks the medium and if the medium is idle it sends immediately. If the medium is busy, it waits a random amount of time and then checks the medium again, if the median is idle (free), it transmits.

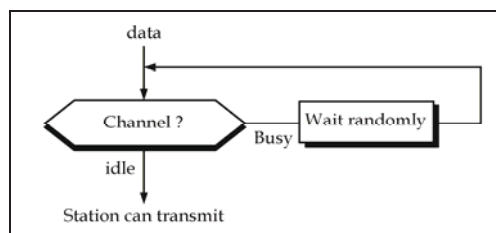


Fig. 4.9.(e) Non - Persistence Method

The problem with this method is time is wasted when the channel is not in use by any station.

3. **P-persistence Method:** In P-Persistence method, P-means probability : To reduce the probability of collision is I-persistent CSMA, not all the waiting stations are allowed to transmit immediately after the

medium is free. A waiting station transmits with probability 'P' if the medium is free.

This method has advantage of other two methods (I - Persistence and non persistence methods) is that it reduces the chance of collision.

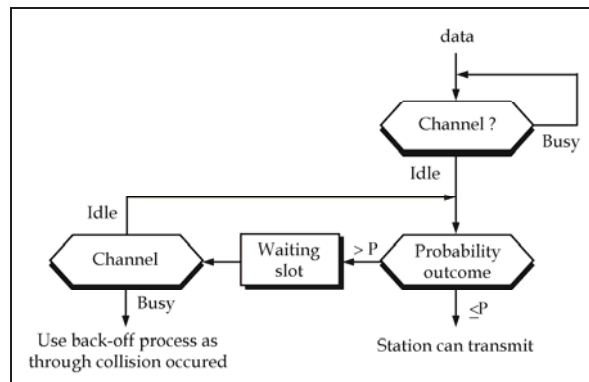


Fig. 4.9.(f). Persistence Method

4.9.2. CARRIER SENSE MULTIPLE ACCESS COLLISION DETECTION (CSMA/CD)

In CSMA / CD, before sending the last bit of the frame, the sending station must detect a collision. It monitor in order to detect, a transmission is finished or a collision is detected.

If a collision has not been detected, it means that transmission is complete; otherwise a collision occurred. If collision occur that send a jamming signal to station. CSMA/CD works as follows:

1. If a station wants to transmit, the station senses (listens to) the channel. If there is no carrier, the station transmits and checks for a collision. If the channel is in use, the station keeps listening until the channel becomes idle. When the channel becomes idle (free), the station starts transmitting again.

2. If two stations transmit frames at the same time on the bus, the frames will collide. The station that detected the collision first, sends a jamming code on the bus (a jam signal is 32 bits of all ones), in order to inform the other stations that there is a collision on the bus.
 3. The two stations that were involved in the collision wait according to the back-off algorithm (a method used to generate random waiting times for stations that were involved in a collision), and then start retransmission.
- Fig. 4.9.2. shows the flow chart of CSMA/CD.

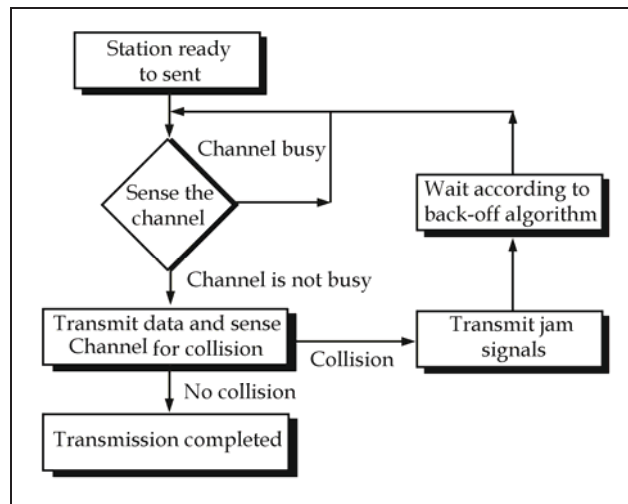


Fig. 4.9.2. CSMA / CD Flow Chart

4.9.3. CARRIER SENSE MULTIPLE ACCESS COLLISION AVOIDANCE (CSMA/CA)

The basic idea behind CSMA / CD is that a station needs to be able to receive while transmitting to detect a collision.

- When there is no collision, the station receives one signal, its own signal.

- When there is a collision, the station receives two signals, its own signal and the signal transmitted by a second station i.e., the signal from the second station is added to signal created by the first station resulting in destroyed data.

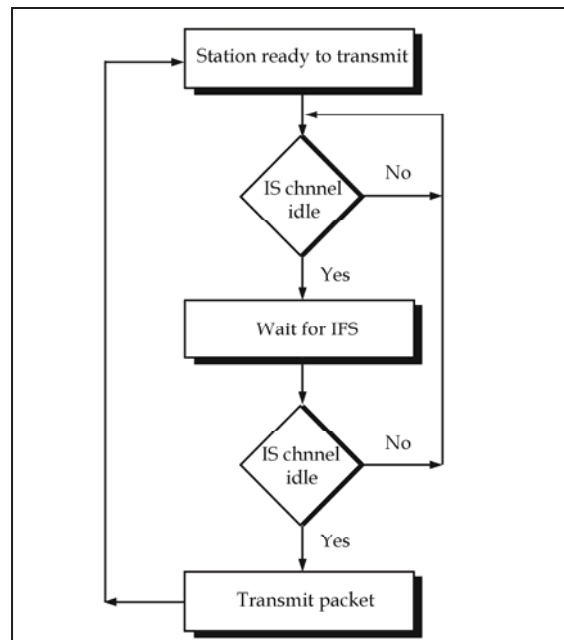


Fig. 4.9.3. CSMA / CA Flow Chart

Carrier sense multiple access with collision avoidance (CSMA/CA) is similar to CSMA/CD. In CSMA/CA when a station wants to transmit a frame, first it listens to the medium. If there is no traffic, it continues to wait for a short Inter Frame Space (IFS) and if there is still no traffic on the medium, then the station will start transmitting. Otherwise, it has to wait for the medium to become clear. Fig. 4.9.3. shows a CSMA/CA flow chart operation.

Inter Frame Space: When an idle channel is found the station does not send immediately. It waits for a period of time called interframe space (I.F.S.). Even though the channel may appear idle when it is sensed.

Additional Information

Need For Framing In Data Link Layer

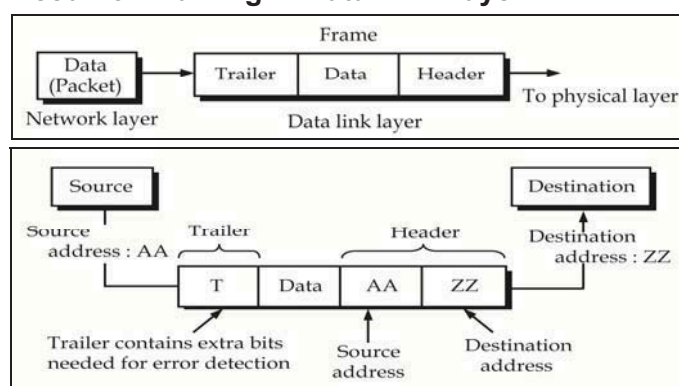


Fig:4.9.3. Frame format of data link layer

- The data link layer, needs to pack bits into frames, so that each frame is distinguishable from another. Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.
- The data link layer divides the stream of bits received from the network layer into manageable data units called frames. If frames are to be distributed to different system on the network. The data link layer adds a header to the frame to define the physical address of the

sender (source address) and receiver (destination address) of the frame.

- Data link layer receives the data to be sent from the network layer, adds header and trailer to it which is now known as a frame. This frame is then transmitted to the physical layer

4.10 EXPLAIN ETHERNET LAN AND ITS FRAME FORMAT

(Apr/May-2015; Oct/Nov-2010,2008; Mar/Apr-2014,2009)

A block of data transmitted on the network is called frame. Fig. shows the IEEE 802.3 Ethernet frame format. Ethernet is a popular packet switching LAN technology that uses a single coaxial cable as the transmission medium.

Preamble	Start frame delimiter (SFD)	Destination address (DA)	Source address (SA)	Length	Data frame	Frame check sequence (FCS)	End of frame delimiter (EFD)
7 bytes	1 bytes	6 bytes	6 bytes	2 bytes	42-1497 bytes	4 bytes	1 bytes

Fig. 4.10 Ethernet Frame Format (IEEE 802.3)

1. **Preamble:** It has 7 bytes (56 bits) of alternating 1's and 0's i.e., (10101010 . . .) It provides signal synchronization.
2. **Start of Frame Delimiter (SFD):** It represents the start of the frame. It is series of two 1's whose purpose is to indicate the end of the preamble and beginning of data frame. It contains 1 byte or 8 bits.

101010 . . .	11
--------------	----

Preamble

SFD

3. **Destination Address (DA):** It is the address of the destination node to receive the frame. It contains 6 bytes (48 bits). This is the hardware NIC address. On receiving this frame, the NIC of the destination

compares it with its own hardware address and if it is matches, accept it, otherwise reject it.

4. **Source Address (SA):** It represents the address of the source from which the frame is originated. It contains 6 bytes (48 bits).
5. **Frame Type (or) length:** It contains 2 bytes (16 bits) and this field identifies the type of data carried in the frame. It indicates the length of the data field.
6. **Data Frame:** This field contains the actual data of the frame, which can be of variable length. Its minimum size is 46 bytes and maximum size is 1500 bytes.
7. **Frame Check Sequence:** It is used for error detection to determine if any information was corrupted during transmission. It uses CRC (Cyclic Redundancy Check) for error detection. It contains 4 bytes (32 bits).
8. **End of Frame Delimiter (EFD):** It simply indicates the end of the frame.

4.11 EXPLAIN THE WORKING OF TOKEN RING NETWORK

(Oct/Nov-2011)

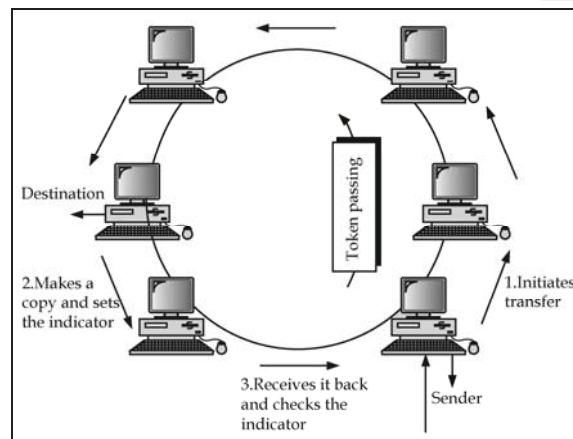


Fig. 4.11.(a) Token Ring

- Token ring is developed by IBM and it is defined by the IEEE is IEEE 802.5 Token ring network is based on ring topology.
- A token ring network employs a mechanism called token passing. In a token ring, a special bit pattern, known as token. A token ring consists of number of interconnected in the form of a ring stations (hosts or computers or nodes).
- Through point-to-point links each station acts as a repeater for regenerates the received signals and sends them to next host. The ring is unidirectional.
- When a host on the ring wants to transmit data, it cannot send immediately, it must wait for the permission. However, once a host gets permission for data transmission, it is guaranteed that no other host would be allowed to transmit data at the same time.

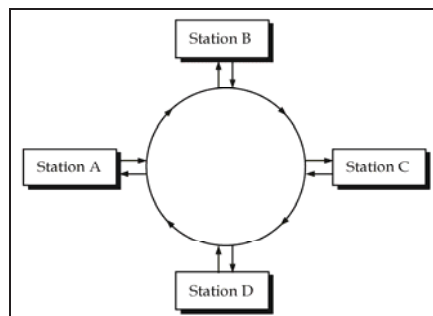


Fig. 4.11.(b) Token Ring LAN

- The sending computer transmits a frame to destination, which travels across the ring. The frame passes to each host on the ring has to accept it and compares the destination address in the frame, if the destination address is found makes copy of it (i.e., accept it) otherwise that frame pass to next host.

- At the destination node, checks the CRC if any error present in the frame, if no error is in the frame, that frame accept it . And the frame circulates on the ring until it reaches the source, which removes the frame from the ring.
- **Example:** Suppose station A wants to send a frame to station D as shown in Fig.4.11. The frame has destination address (D) and source address (A) the frame passes through the stations 'B' and 'C' which acts as repeater and forward the frame to the next link, they do not copy the frame as the frame is not addressed to them. Station 'D' finds its address on the frame and copies it. The frame continues its journey and reaches station 'A'. The frame does not circulate again around the ring and a station 'A' the frame does not circulate again around the ring and a station 'A' removes the frame from the ring.

4.12 EXPLAIN THE TOPOLOGY OF WIRELESS LAN AND EXPLAIN ITS FRAME FORMAT (IEEE 802.11)

(Mar/April-2009;Oct/Nov-2008)

Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere wireless LANs can be found on college campus, office buildings and many public areas. IEEE 802.11 wireless LANs sometimes called wireless Ethernet and blue tooth, a technology for small wireless LAN's. Although both protocols need several layers to operate, we concentrate mostly on the physical and data link layer. IEEE has defined the specifications for wireless LAN called IEEE 802.11.

wireless LAN frame format (IEEE 802.11)

IEEE 802.11 standard defines two kinds of services.

- Basic Service Set (BSS)
- Extended Service Set (ESS)

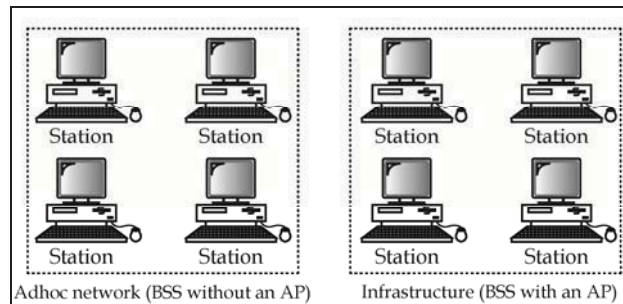


Fig. 4.12.(a) Service Set's (BSS's)

Basic Service Set (BSS): IEEE 802.11 defines the basic service set (BSS) as the building blocks of wireless LAN. Basic service Set is made of stationary or mobile wireless station and an optional central base station, known as the "access point" (AP). An access point (AP) is a wireless hub. It is connected to a wired LAN and provides coordination between users. An 'AP' is made of three components an antenna, a receiver and a transmitter.

The BSS without an AP is a stand alone network and cannot send data to other BSS. It is called an Adhoc architecture. In this architecture stations can form a network without the need of an AP. They can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an "infrastructure network".

Extended Service Set (ESS): An extended service set (ESS) is made up of two or more BSS. In this case the BSS are connected through a distribution system, which is usually a wired LAN. The distribution System connects the AP's in the BSS. IEEE 802.11 does not restrict the distribution

system. It can be any IEEE LAN such as an Ethernet. Note that extended service set uses two types of station.

- Mobile
- Stationary

The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

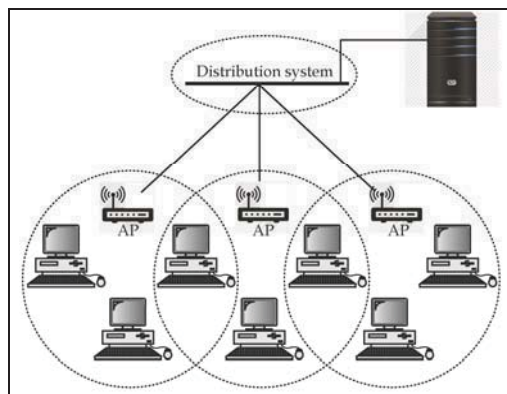


Fig. 4.12.(b) Extended Service Sets (ESS)

When BSS are connected, the stations within reach of one to another can communicate without the use of an AP. However communication between two stations in two different BSS usually occurs via two AP's. The idea is similar to communication in a cellular network. If we consider each BSS to be a cell and each AP to be a base station. Note that a mobile stations can belong to more than one BSS at the same time.

Station Types: IEEE 802.11 defines 3 types of stations based on their mobility in a wireless LAN :

- No transition
- BSS transition
- ESS transition mobility

No Transition: A station with no transition mobility is either stationary (not moving) or moving only inside a BSS.

BSS Transition: A station with BSS transition mobility can move from one BSS to another, but the movement is confined inside one ESS.

ESS Transition: A station with ESS transition mobility can move from one ESS to another.

4.14 EXPLAIN THE FEATURES OF BLUETOOTH TECHNOLOGY.

(Oct/Nov-2011)

Bluetooth was originally started as a project by the Ericsson company. It is named for Harald Blaatand, the king of Denmark. Blaatand translates to Bluetooth in English. Today Bluetooth technology is defined by IEEE 802.15 standard. Bluetooth is a wireless LAN technology designed to connect different devices such as cellphones, notebooks, computers (desktop and laptops), cameras etc. Bluetooth operates in the range of 10 meters and current data is 1 Mbps with a 2.4 GHz bandwidth. Bluetooth uses frequency hopping spread spectrum (FHSS) method for security purpose. Bluetooth has two types of networks. They are:

1. Piconet
2. Scattered

- 1. Piconet:** A bluetooth network is called a piconet or a small net. A piconet can have upto eight devices, one of which is called the "primary device" or "master", the remaining devices are called "secondary devices" or "slaves". All the secondary devices synchronize their clocks and hopping sequences with the primary. The communication between the primary and the secondary can be one to one or one to many. A piconet is a centralized TDM System with master controlling the

clock and the time slots of devices for activation. Master can communicate to slave and vice versa but slave to slave communication is not possible.

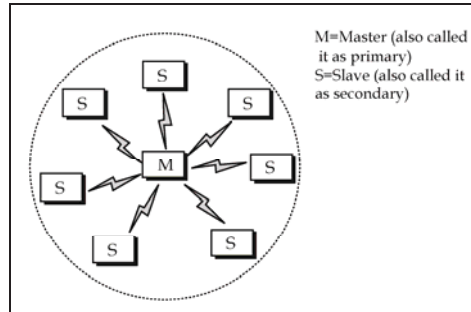


Fig.4.14.(a) : Piconet

2. **Scatternet:** Collection of interconnected “piconets” can be called as “Scatternet”. A secondary device (slave) in one piconet can be the primary (master) in another piconet. This device receive messages from the primary in the first piconet (as a secondary) and acting as a primary, deliver them to secondaries in the second piconet. We can secure a Bluetooth connection by using a secure Personal Identification Number (PIN) between two devices (cellphones, computers, laptops etc.).

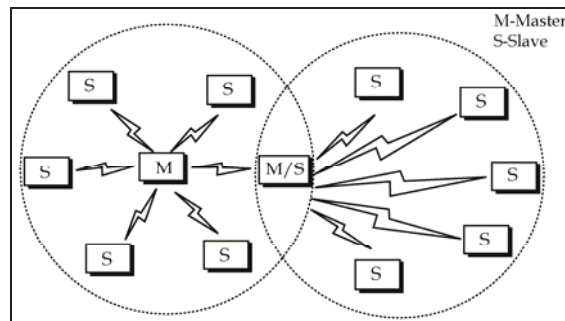


Fig. 4.14.(b) : Scatter net

4.15 EXPLAIN THE USE OF SWITCH, BRIDGE IN CONSTRUCTING NETWORKS

4.15.1. USE OF SWITCH

- A network switch is a computer networking device that connects devices together on a computer network. It receives packet, checks the address and decides where to send the message and then start forwarding immediately.
- A switch performs the function similar to a hub, but more efficiently. A switch is device which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segments in LAN.
- The switch has buffer for each link to which it is connected. When the switch is receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If the outgoing link is free, the switch sends the frame to that particular link. Architecture of a switch is shown in fig:4.15.1.

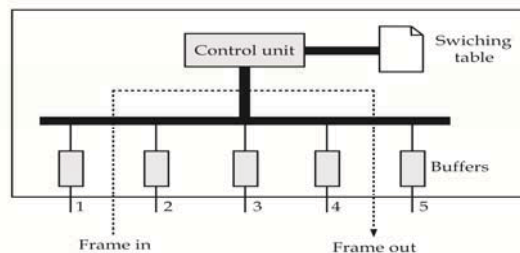


Fig:4.15.(a). illustration of switch

- In switch, a frame arrives at port 2 in frame in and is stored in the buffer and checks the address to find the outgoing link. If the outgoing link is free, the switch

sends the frame to the frame out output port. The frame is then sending out to port 5 as shown in fig:

- Switches can connect different network types (such as Ethernet and Fast Ethernet) or networks of the same type. Many switches today offer high-speed links, like Fast Ethernet.

(Apr/May-2015, 2012;Oct/Nov-2010)

- A bridge is a computer that has its own processor, memory and two NIC cards to connect to two portions of a network. A bridge does not run application programs; it instead facilitates host-to-host communication within a network.

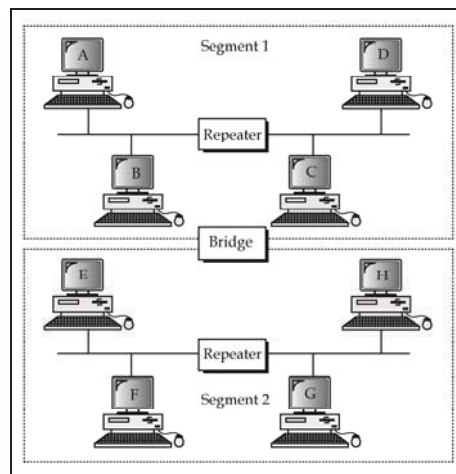


Fig. 4.15.(b): Bridge Connecting Two Segments

- It operates at the physical as well as data link layers of the OSI Protocol hierarchy.
- The main idea of using a bridge is to divide a big network into smaller sub networks, called segments. This is shown in Fig. 4.15(b). Here, the bridge splits the entire network into two segments, shown by dotted

lines. The two segments act as a part of a single network because of the bridge.

- The main advantage of a bridge is that it sends the data frames only to the concerned segment, thus preventing excess traffic.
- bridge serves the following purposes :
 1. Unwanted traffic is minimized.
 2. Busy links or links in error can be identified and isolated, so that the traffic does not go to them.
 3. Security features or access controls (e.g., rules like a host on segment 1 can send frames to a host on segment 2 but not to segment 3), can be implemented.

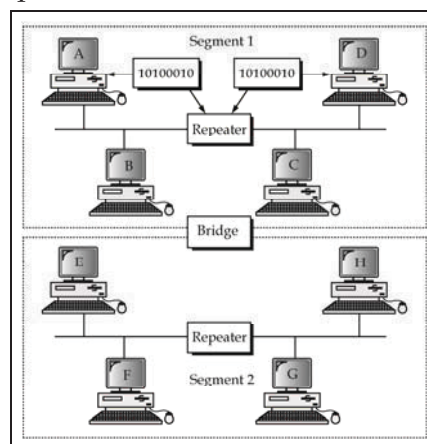


Fig. 4.15.(c) : A Bridge Minimizes Unwanted Traffic

NOTE: Suppose, host A wants to send a frame to host D, then, the bridge does not allow the frame to enter the lower segment even if both segments belong to the same network. Instead, the frame is directly relayed to host D of course the repeater might regenerate the frame as shown

in Fig. 4.15. By forwarding frames only to the segment where the destination host resides

4.15.2. USE OF BRIDGE

(Apr/May-2015, 2012; Oct/Nov-2010)

- A bridge is a computer that has its own processor, memory and two NIC cards to connect to two portions of a network. A bridge does not run application programs; it instead facilitates host-to-host communication within a network.
- It operates at the physical as well as data link layers of the OSI Protocol hierarchy.

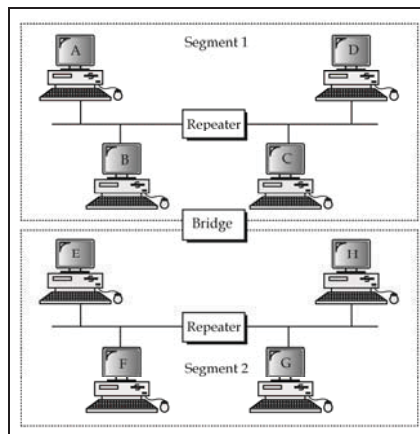


Fig. 4.15.2. : Bridge Connecting Two Segments

- The main idea of using a bridge is to divide a big network into smaller sub networks, called segments. This is shown in Fig. 4.15.2. Here, the bridge splits the entire network into two segments, shown by dotted lines. The two segments act as a part of a single network because of the bridge.

- The main advantage of a bridge is that it sends the data frames only to the concerned segment, thus preventing excess traffic.
- bridge serves the following purposes :
 1. Unwanted traffic is minimized.
 2. Busy links or links in error can be identified and isolated, so that the traffic does not go to them.
 3. Security features or access controls (e.g., rules like a host on segment 1 can send frames to a host on segment 2 but not to segment 3), can be implemented.

NOTE: Suppose, host A wants to send a frame to host D, then, the bridge does not allow the frame to enter the lower segment even if both segments belong to the same network. Instead, the frame is directly relayed to host D of course the repeater might regenerate the frame as shown in Fig. 4.15. By forwarding frames only to the segment where the destination host resides

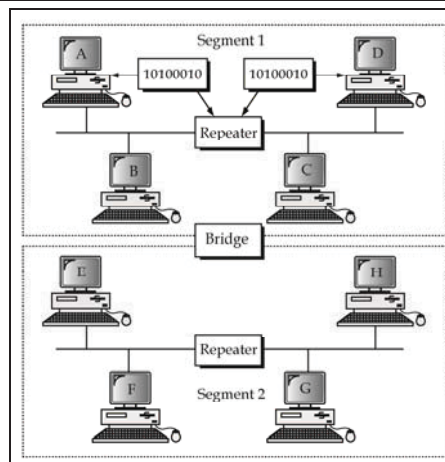


Fig. 4.15.2.(a) : A Bridge Minimizes Unwanted Traffic

4.16 DIFFERENTIATE BETWEEN REPEATER, SWITCH AND BRIDGES.

S.NO	BRIDGE	REPEATER	SWITCH
1	It is used to divide big network into smaller sub networks	It is used to receive weak or corrupted signal, regenerates it and forward to next receiver	It is used to connects devices together on a computer network.
2.	It operates at physical and data link layer	It operates at physical layer	It operates at data link layer
3.	It doesn't run any application program	It can run application program	It doesn't run any application program
4.	It cannot be regenerates a signal	It can be regenerates a signal	It cannot be regenerates a signal
5	Low cost	Low cost compared to switch but more than bridge	costly
6	It is point-to-point device	It is a broadcast device	It is point-to-point device

CHAPTER 5

NETWORK LAYER, TRANSPORT LAYER AND APPLICATION LAYER

-: Objectives :-

On completion of the study of the chapter a student should be able to comprehend the following:

a) Network Layer:

- 5.1. Define the terms Internet and Intranet.
- 5.2. Explain classful addressing and classless addressing in IPv4.
- 5.3. State the use of routers in networking
- 5.4. Explain the concept of routers and routing.
- 5.5. Distinguish among cut through, store-and-forward and adaptive switch mechanisms.
- 5.6. Explain the packet transfer mechanism using routers and IP address.

b) Transport Layer

- 5.7. List the features of Transmission Control Protocol (TCP)
- 5.8. Explain the flow control in TCP
- 5.9. Explain error control in TCP
- 5.10. Explain the connectivity of systems using TCP (Three way hand shake)
- 5.11. Explain end-to-end connectivity in TCP using ports and sockets.
- 5.12. Describe the features of User Datagram Protocol (UDP)
- 5.13. Compare the features of TCP and UDP
- 5.14. State the use of Gateways.

c) Application Layer:

- 5.15. Mention the role of DNS server
- 5.16. Explain how email is transferred
- 5.17. Discuss POP server and SMTP server
- 5.18. Explain file transfer operation using FTP
- 5.19. Explain the working of Web server
- 5.20. Describe the web browser architecture
- 5.21. Explain the internal architecture of ISP
- 5.22. Write the purpose of proxy server
- 5.23. Explain remote login

a) Network Layer:**5.1 DEFINE THE TERMS INTERNET AND INTRANET.**

(Apr/May-2015,2012,2011; Oct/Nov-2008)

Internet:

Definition: The **Internet** is a global system of interconnected computer networks that use the standard **Internet** protocol suite (TCP/IP) to link several billion devices worldwide. Simply "A Network of computer networks is called as **internet**".

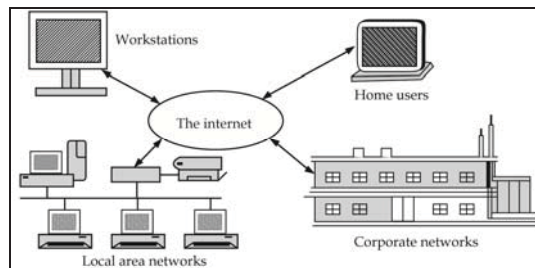


Fig : 5.1

- The **internet** is an informal term for the world-wide communication network of computers. The internet is used to send information quickly between computers around the world.
- It has millions of smaller domestic, academic, business, and government networks and websites, which together carry many different kinds of information (facts and details) and services. So in other words, the Internet is a network of networks.
- The internet is used for many things, such as electronic mail, online chat, file transfer, and the interlinked web pages and other documents of the World Wide Web. The most used service on the internet is the World Wide Web (which is also called the "Web").

NOTE: Network: A network is a set of devices (computers or any other device capable of sending and / or receiving data) connected by media links. (Communication channel).

Ex: LAN, MAN, and WAN.

Computer Network: A network consists of two or more computers that connected for the purpose of sharing data or resources that network is called Computer Network.

(Oct/Nov-2014,2012, 2010; Apr/May-015,2012,2010;Mar/Apr-2014, 2008)

Definition: An INTRANET is a TCP/IP network inside a company that allows employs to access the company information resources, through an internet.

- Any person anywhere in the world can access their information by using internet.
- A company however may not want the entire world to view one or more of its web pages. For example, a company may want to allow its employs easy to access to a database, but not allow to access to any one outside the company. It is possible to offer an internet like service to the company employees only and this type of network is called as Intranet.
- An INTRANET is a TCP/IP network inside a company that allows employs to access the company information resources, through an internet.
- An INTRANET is a private computer network that uses internet connection to securely share part of an organizations' information with its employees.
- Briefly an INTRANET can be understood as a private version of the internet.

Additional Information

TYPES OF INTERNET PROTOCOL(IP) ADDRESSING

Internet Protocol(IP) addressing can be divided into two types They are:

1. IPv4 (IP version 4) addressing
2. Ipv6 (IP version 6) addressing

IPv4 (IP version 4) addressing: The Internet addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses if there is no confusion.

IPv6 (IP version 6) addressing: The need for more addresses, a IPv6 (IP version 6) addressing is used. In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation.

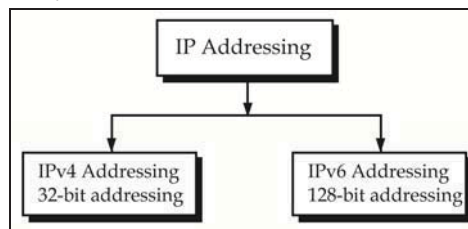


Fig: Classification of IP addressing

5.2 EXPLAIN CLASSFUL ADDRESSING AND CLASSLESS ADDRESSING IN IPV4.

(Oct/Nov-2015,2014,2013,2010;Apr/May-2010; Mar/Apr2014,2009)

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.
- IPv4 addresses are unique because of each address defines one and only one, connection to the Internet.

Two devices on the Internet can never have the same address at the same time.

- The IPv4 addresses are universal because, the addressing system must be accepted by any host that wants to be connected to the Internet.
- IPv4 addresses can be divided into two types based on their classes
 1. Classful addressing
 2. Classless addressing

5.2.1. Classful Addressing

IPv4 addressing used the concept of classes. This architecture is called classful addressing.

In classful addressing, the address space is divided into five classes: A,B,C,D and E . Each class occupies some part of the address space.

Notation of IPv4 address: We can find the class of an address, there are two notations of IP address are used.

1. Binary notation
2. Dotted-decimal notation

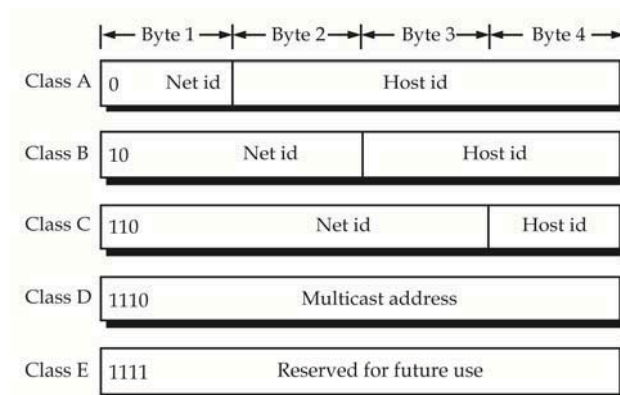


Fig:5.2.1.

	First byte	Second byte	Third byte	Fourth byte		First byte	Second byte	Third byte	Fourth byte
Class A	0				Class A	0-127			
Class B	10				Class B	128-191			
Class C	110				Class C	192-223			
Class D	1110				Class D	224-239			
Class E	1111				Class E	240-255			

Fig:5.2.1.(a)

(i) Binary notation: In binary notation, the IP address is displayed as 32 bits. Each octet is often referred to as byte. So it is common to hear an IP address referred to as 32 bits address or a 4 byte address.

Eg : 01110101 10010101 00011101 00000010

(ii) Decimal Notation : To make the IP address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.

10000000	00001011	00000011	00011111
↓	↓	↓	↓
128	11	3	31

Parts of IP Address: The IP address is of 3 parts namely:

1. Class
2. Network number
3. Host number

Class	Network Number	Host Number
-------	----------------	-------------

Classes of IP Address: The IP address space is divided into five classes. They are:

1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

Each class occupies some part of the address space:

- **Class A Address:** It is designed for large organizations with a large number of attached hosts or routers.
- **Class B Address:** These were designed for mid size organizations with tens of thousands of attached hosts or routers.
- **Class C Address:** These were designed for small organizations with a small number of attached hosts or routers.
- **Class D Address:** It were designed for multi casting. Each address in this class is used to define one group of hosts on the Internet.
- **Class E Address:** It is reserved for future use; only a few were used resulting in another waste of addresses.

In class D and class E many addresses were wasted.

That is In classful addressing, a large part of the available addresses were wasted.

5.2.2. Classless Addressing

- In classful addressing, a large part of the available addresses were wasted. To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.
- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity.

NOTE: For example, a household may be given only two addresses; a large organization may be given thousands of addresses. An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve. Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...)
3. The first address must be evenly divisible by the number of addresses.

5.3 STATE THE USE OF ROUTERS IN NETWORKING

(Apr/May-2010, Oct/Nov-2008)

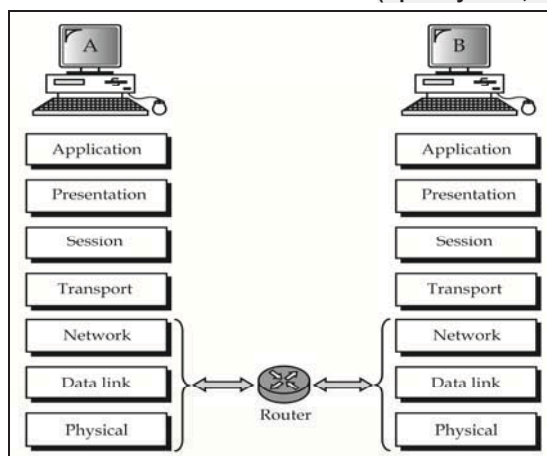


Fig: 5.3

A device that connects two or more computer networks together is called as a "Router".

Router allows two or more different computers to send data to each other. A router is a special purpose computer that is used specially for internet work purposes. A router has a processor (CPU) and memory like computer. However it has more than one I/O interfaces that allows it to connect to multiple computer networks.

Router operates network layer, data link layer and physical layers of OSI model.

5.4 EXPLAIN THE CONCEPT OF ROUTERS AND ROUTING.

5.4.1. CONCEPT OF ROUTER

(Apr/May-2010, Oct/Nov-2008)

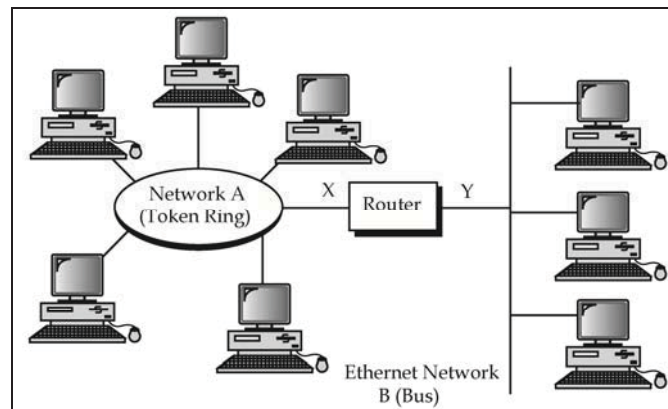


Fig: 5.4.1. Router Connecting a Token Ring and a Bus

A router is useful for interconnecting two or more networks. A router has to determine the best possible transmission path, among the several available.

A network has many computers or nodes attached to it therefore, an address of a node or a computer could be treated as network ID + node ID. Each node has a Network Interface Card (NIC), which has this address. The router is a

special computer that has two NIC's, which is used to connect two networks. The networks shown in Fig., could be both LAN's or WAN's of the same or different types ; or one of them could be a LAN and the other a WAN etc. A router has a capability to connect them together.

The concept of a router can be illustrated with the help of fig:

There is a Token ring network A and an Ethernet network B based on bus architecture. A router connects to the token ring at a point x, and to the Ethernet network at point Y. Since the same router connects to the two networks at these points, it means that this router must have two IC's. Each of the router's NIC is specific to one network type to which it connects. The NIC at point x is a token Ring NIC, where as the NIC at point Y is an Ethernet NIC.

5.4.2. CONCEPT OF ROUTING

(Apr/May-2010, Oct/Nov-2008)

Routing is the process of sending that data in the form of packets called data grams from source to destination computers through many networks.

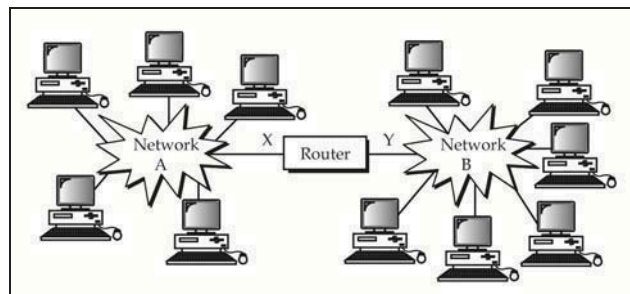


Fig:5.4.2.A Router Connects Two or More Computers Together

Routing is the process of transferring data across an internetwork from a source host to a destination host.

Routing can be understood in terms of two processes: host routing and router routing. Host routing occurs when the sending host forwards a packet. Based on the destination network address, the sending host must decide whether to forward the packet to the destination or to a router. In Fig: 5.4. the Source Host forwards the packet destined for the Destination Host to Router 1.

Router routing occurs when a router receives a packet that is to be forwarded. The packet is forwarded between routers (when the destination network is not directly attached to the router) or between a router and the destination host (when the destination network is directly attached). In Fig: 5.4. (a) Router 1 forwards the packet to Router 2. Router 2 forwards the packet to the Destination Host.

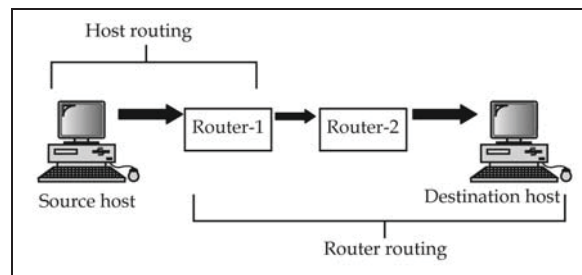


Fig: 5.4. (a) The Routing Process

5.5. DISTINGUISH AMONG CUT THROUGH, STORE-AND-FORWARD AND ADAPTIVE SWITCH MECHANISMS.

(Apr/May-2012; Oct/Nov-2011)

- A network switch is a computer networking device that connects devices together on a computer network. It receives packet, checks the address and decides where to send the message and then start forwarding immediately.

- When the switch receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If the outgoing link is free, the switch sends the frame to that particular link.
- The switch forwards the message in three ways. They are
 1. Cut through Switching
 2. Store and forward Switching
 3. Adaptive Switching

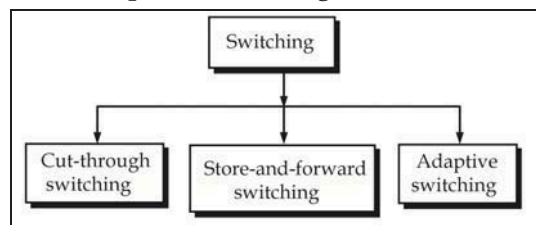


Fig:5.5. Types switching mechanisms

Cut-through switching:

In cut-through switching, the switch examines the header and decides where to send the message and then start forwarding immediately.

It reads the first few bytes of the packet to obtain the source and destination address. The packets are sent to the destination segments without checking of the packet errors.

Cut through switch simply keeps on connecting the links from source to destination. Once link is established, it becomes busy until the information is exchanged. No storage facility available in this switch.

It is extremely fast switching but it has no error checking.

Store-and-forward switching:

(Oct/Nov-2012)

It stores the entire packet and then check for errors in the packet. If a packet contains errors, it is discarded; otherwise the switch forwards the packets to the specified destination.

A store-and-forward switch stores the frame in the input buffer until whole packet is arrived. It waits to receive the entire packet before sending. The switch checks the destination address, source address, and the CRC. Find out where the message should go. If no errors are present, the frame is forwarded to the appropriate destination port.

It performs the error checking but it has low switching speed.

Adaptive switching:

(Oct/Nov-2015)

In Adaptive switching, it receives the packet, checks the destination and sends the message immediately. It provides fast switching and error checking also.

It is designed to operate in Cut through mode normally but if ports error rate is too high the switch automatically reconfigures the port to run in store and forward mode.

5.6 EXPLAIN THE PACKET TRANSFER MECHANISM USING ROUTERS AND IP ADDRESS.

(Mar/Apr-2014,2008;Oct/Nov-2013; Apr/May-2011)

- A router is a special purpose computer that is mainly used for forwarding packets from one network to another over the Internet.
- A router connects two or more networks - A router needs to have IP addresses of networks that are connected to it.

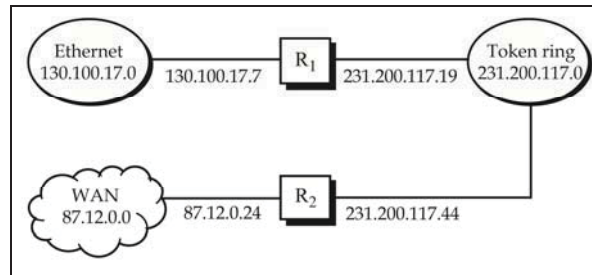


Fig. 5.6. Packet Transfer Mechanism, using Routers & IP addresses

In Fig.5.6 Router (R1) connects Ethernet and a token ring whose IP addresses are 130.100.17.0 (class B) and 231.200.117.0 (Class D) respectively and Router R2 connects token ring and WAN whose IP addresses are 231.200.117.0 (Class-D) and 87.12.0.0 (Class A) respectively.

Routers are assigned IP addresses for both the interfaces that they are connected to it. In Fig.5.6. Router R1 has an IP address 130.100.17.7 on the Ethernet and it has an IP address: 231.200.117.19 on the Token Ring network. By using these IP Addresses of networks routers forward the packets to destination. The same process can be observed in Router R2.

b) Transport Layer

5.7 LIST THE FEATURES OF TRANSMISSION CONTROL PROTOCOL (TCP)

(Apr/May-2015, 2012,2010, Oct/Nov- 2012,2010,2008)

The transmission control protocol (TCP) works extremely well with IP. TCP is makes the internet reliable.

For example, if router has too many packets, it discards some of them, consequently, the packet don't reach the final destination. TCP automatically checks for lost packets and request for their retransmission.

Similarly the internet offers alternate routes (through routers) for data to flow across it, packets may not arrive at the destination in the same order as they were sent. TCP puts packets in orderly. Again, if some packets are duplicated due to some hardware malfunction, TCP discard that packets.

Features of TCP: The main features offered by the TCP position of the TCP / IP protocol suite are:

- Reliability
- Point-to-point communication.
- Connection Oriented.

1. Reliability:

TCP ensure that any data sent arrives at the destination as it was sent. This means there cannot be any data loss or change in the order of data. Reliability at the transport layer (TCP) has four important aspects as shown in the Fig.

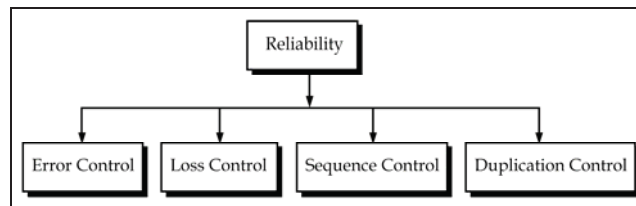


FIG 5.7. Four Aspects of Reliability in Transport Layer Delivery

2. Point to Point Communication:

It is also called port-to-port communication, each TCP connection has exactly two ends points : a source and a destination. They communicate as if there is a direct connection between them, also, there is no confusion about who is sending the data or who is receiving it, simply because only two computers are involved in a TCP connection. Also this communication is full duplex, which means that both the participating computers can send messages to the other simultaneously.

3. Connection Oriented:

TCP is a connection oriented. TCP establishes a virtual connection through the internet between, the sender and receiver. All the packets belonging to a message are then sent over this same path. The term virtual is used because physically there is no direct connection between the computers i.e., it is achieved in the software, rather than in the hardware. This means that a connection must be established between the two ends of a transmission before either can transmit data.

Connection - oriented transmission has three stages:

- Connection establishment
- Data transfer
- Connection termination

5.7.1. Explanation of Reliability in Tcp

TCP ensure that any data sent arrives at the destination as it was sent. This means these cannot be any data loss or change in the order of data. Reliability at the transport layer (TCP) has four important aspects as shown in the Fig. 5.7.1.

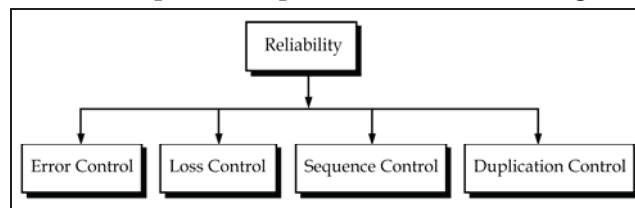


FIG 5.7.1.Four Aspects of Reliability in Transport Layer Delivery

1. **Error Control:** When transferring data, the primary goal of reliability "**error control**". Data must deliver the destination exactly as it was sent. But cannot guarantee error - free delivery between source and destination.

TCP provides its own error control mechanism based on error detection and retransmission methods such as check sum and CRC.

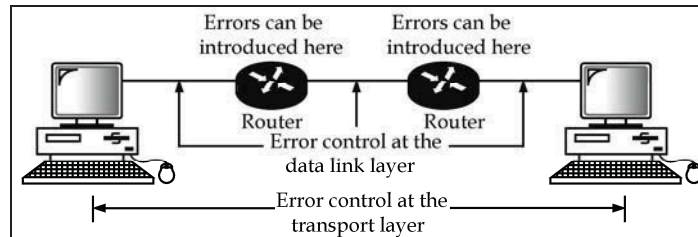


FIG 5.7.1 (a): Transport Layer and Data link Layer Error Control

- 2. Loss Control:** TCP software breaks the original message into packets and these packets send to destination, but some of packets may be lost mid way and never reach the destination.

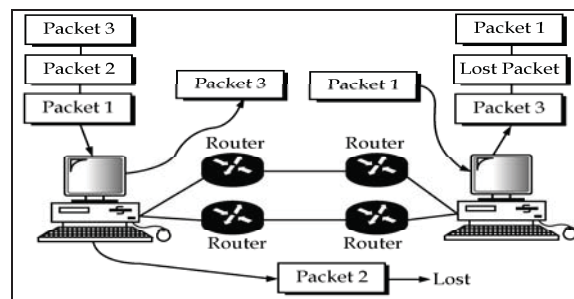


FIG 5.7.1. (b): Loss Control

TCP ensures that the destination knows about this and requests for a retransmission of the missing packets. This is called loss control. **Ex:** TCP breaks the original message into packets and can check if all the three have arrived correctly at the destination. This is shown in Fig. 5.7.1. (b)

- 3. Sequence Control:** Different packets of the same message transmit different routes (through routers), the packets may not arrive at the destination in the sequence as they were sent. TCP is used to control the sequence of packets i.e., at the destination TCP reassembles the packets in order.

- 4. Duplication Control:** In case of loss control, one more loss of packets can be detected. In "**duplication control**" one or

more “**duplicate**” packets are detected since the same packet can arrive at the destination twice or more TCP provides the destination must accept only the first packet and reject all its duplicate copies.

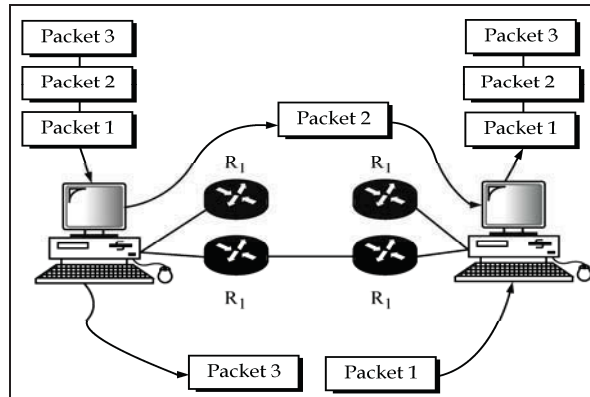


FIG 5.7.1. (c): Sequence Control

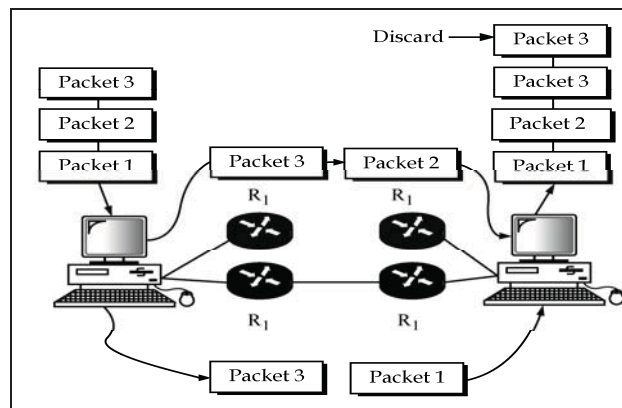


FIG 5.7.1. (d): Duplication Control

Ex. Fig. shows an example of duplication. Here packet 3 arrives at the destination host B two times. The TCP software at host B could detect this and retain only one of them discarding the other [redundant (repeated)] copy.

5.11 EXPLAIN END-TO-END CONNECTIVITY IN TCP USING PORTS AND SOCKETS.

(Mar/Apr-2014, 2009; Apr/May-2010; Oct/Nov-2008)

Ports:

Applications running on different hosts communicate with TCP with the help of a concept called as **ports**. A port is a 16-bit unique number allocated to a particular application. A port can identify a single application on a single computer.

When an application on one computer wants to open a TCP connection with another application on a remote computer, the concept of port comes handy.

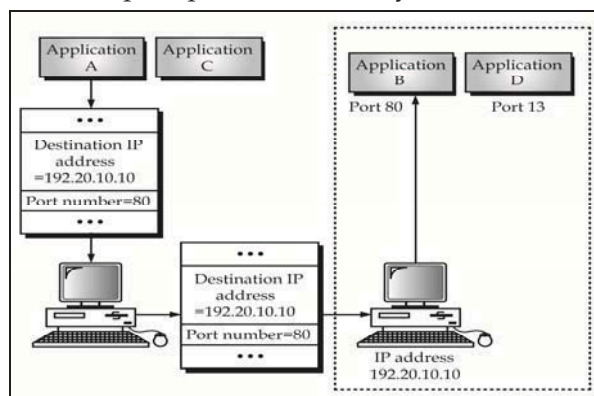


FIG 5.11.(a) Use of Port Numbers

Fig: 5.11.(a). shows an example of using a port number in conjunction with an IP address, an application A running on computer X wants to communicate with another application B running on computer Y. Application A provides the IP address of computer Y (i.e., 192.20.10.10) and the port number corresponding to application B (i.e., 80) to computer X. Using the IP address, computer X communicates with computer Y. At this point, computer Y uses the port number to redirect the message to application B.

This is the reason, why, when an application wants to communicate with another application, on a remote computer, it first opens a TCP connection with the application on the remote computer using the IP address (like the telephone number) of the remote computer and the **port number** of the target application.

Thus the IP protocol enables communication between different two computers, whereas TCP enables the communication between two applications on these different computers.

Sockets:

A port identifies a single application on a single computer. The term socket address or simply socket is used to identify the IP address and the port number as shown in Fig.

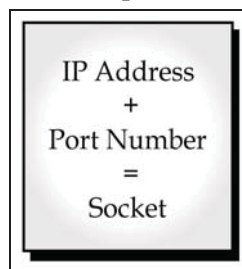


FIG : 5.11.(b) Socket

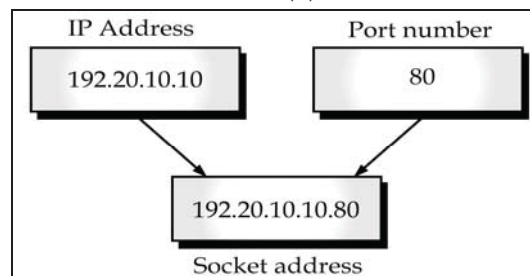


FIG 5.11.(c) Socket Example

For Example, port 80 on a computer 192.20.10.10 would be referred to as socket 192.20.10.10.80. Note that the port

number is written after the IP address, with a colon separating them. This is shown in Fig.

As we can imagine a pair of sockets identifies a TCP connection between two applications on two different hosts, because it specifies the end points of the connection in terms of IP addresses and port numbers, together. Thus, we have a unique combination of **(Source IP address + Source port number + Destination IP address + Destination Port number)** to identify a TCP connection between any two hosts (typically a client and a server).

5.12 DESCRIBE THE FEATURES OF USER DATAGRAM PROTOCOL (UDP)

- The User Datagram Protocol (UDP) is a connectionless, unreliable, transport protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet **Protocol (IP)**. It performs very limited error checking.
- UDP is powerless, because it is a unreliable. why would a process want to use it? With the disadvantages come some advantages. UDP is a very simple protocol using a minimum of overhead. **If a process wants to send a small message and does not care much about reliability, it can use UDP.**
- Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP (Transmission Control Protocol). UDP is suitable for send a small amount of data called **datagram's** and it is not suitable to send bulk data because it is unreliable.
- UDP provides only the basic functions needed for end-to-end delivery of transmission. It does not provide any sequencing or reordering functions and cannot specify the damaged packet.

- 3. Total packet Length:** This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes.

$$\text{UDP length} = \text{IP length} - \text{IP header's length}$$

- 4. Checksum:** This field is used to detect errors over the entire user datagram (header plus data).

THE MAIN FEATURES OF UDP

1. The User Datagram Protocol (UDP) is a connectionless, unreliable, transport protocol.
2. There is no flow control or acknowledgement mechanism
3. It is less complex than TCP and easy to implement
4. It performs very limited error checking
5. UDP is suitable for send a small amount of data called **datagrams** and it is not suitable to send bulk data because it is unreliable.
6. UDP provides only the basic functions needed for end-to-end delivery of transmission.
7. It does not provide any sequencing or reordering functions and cannot specify the damaged packet.
8. UDP contains only checksum; it does not contain an ID or sequencing number for a particular data segment
9. UDP packets, called user datagram's, have a fixed-size header of 8 bytes made of four fields, each of 2 bytes(16 bits)

5.13 COMPARE THE FEATURES OF TCP AND UDP

(Oct/Nov-2011)

Transmission Control Protocol (TCP) :

- TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange

data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.

- It is a reliable connection oriented protocol i.e., connection must be established between both ends of a transmission, before they transmit data. By creating this connection TCP generates a virtual circuit between the sender and the receiver, that connection is only active for the duration of transmission only.
- TCP makes the Internet reliable. For example, if a router has too many packets, it discards some of them. Consequently, the packets do not reach the final destination. TCP automatically checks for lost packets and requests for their retransmission. Similarly, the Internet offers alternate routes (through routers) for data to flow across it, packets may not arrive at the destination in the same order as they were sent. TCP puts packets in order.
- TCP subdivides the incoming message stream of bytes into manageable discrete messages and transmits these into the network (Internet) layer. At destination, the TCP reassembles the received messages into the original form.

User Datagram Protocol (UDP) :

- The **User Datagram Protocol (UDP)** is the simplest Transport Layer communication **protocol** available of the TCP/IP **protocol** suite. It involves a minimum amount of communication mechanism. It is an **unreliable, connectionless protocol** but it uses IP services which provides a best effort delivery mechanism and is widely used for client – server applications where speed of delivery is more important than accurate delivery.

In multimedia transmissions or voice, transmission speed is a major concern than accurate delivery of the message.

(Oct/Nov-2008)

S.NO	TCP	UDP
1.	TCP: transmission control protocol	UDP: user datagram protocol.
2.	It is reliable	It is unreliable
3.	It is connection oriented protocol	It is connection less protocol.
4.	It establishes a virtual connection before sending the data.	It allows computers to send data without needing to establish a virtual connection.
5.	It transmits message from source to destination without errors.	It may transmit message from source to destination with errors
6.	It provides acknowledgement, sequencing or reordering mechanism.	It does not provide for any acknowledgment, sequencing or re-ordering mechanism.
7.	It is used for transferring computer data such as files and messages.	It is used for voice and video transmission.

5.14 STATE THE USE OF GATEWAYS.

(Apr/May-2015, 2011,2010;Oct/Nov-2011, 2010; Mar/Apr-2008)

A **router** can forward packet across different network types (e.g., Ethernet, Token ring). However, all these different networks must use a common transmission protocol (such as TCP/IP) for communication. If they are not using the same protocol, a router would not be able to forward packets from one network to another. A **gateway** can forward packets across different networks that may also use different protocols.

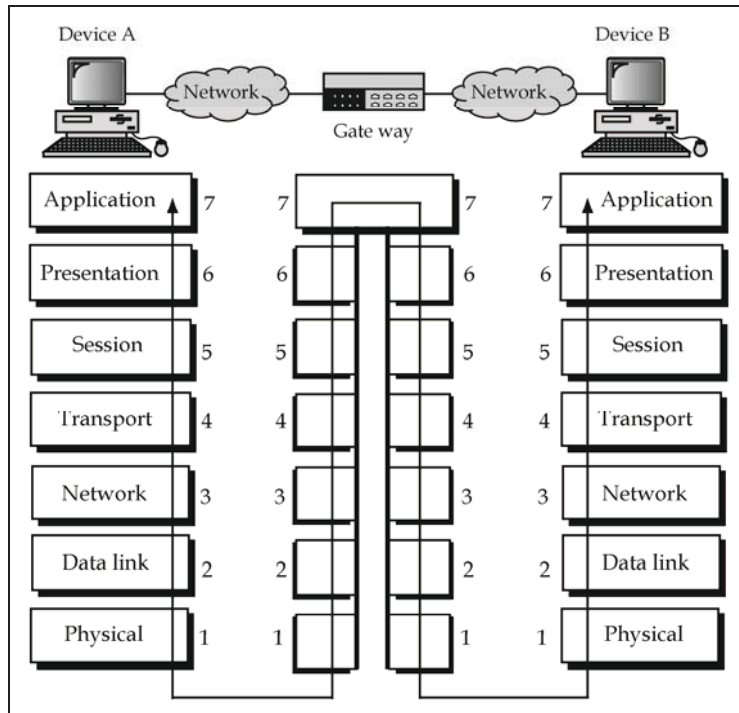


FIG.5.14.(a): Gateway Operates at 7 OSI Layers

That is if network A is a Token Ring Network using TCP/IP and network B is a Novell Netware Network. A gateway can relay frames between these two.

A gateway has to not only have the ability of translating between different frame formats, but also different protocols. The gateway is aware of, and can work with the protocols used by each network connected to a router and therefore, it can translate from one to the other. In certain situations, the only changes required are to the frame header.

A Gateway operates at all the seven layers of the OSI model as shown in Fig: 5.14.(b)

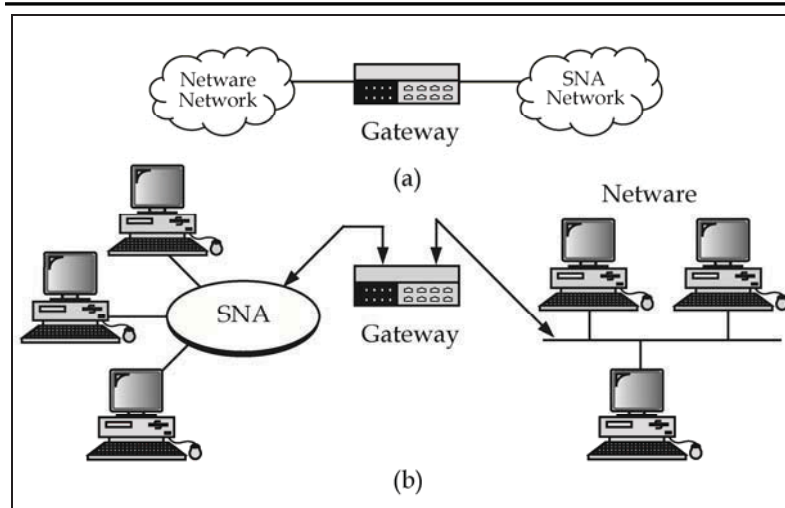


FIG 5.14.(b): Gateway connects the SNA and Networkware

Additional Information

INTRODUCTION

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for the purpose of locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality of the Internet.

The **domain name space** consists of a tree data structure. Each node or leaf in the tree has a *label* and zero or more *resource records* (RR), which hold information associated with the domain name. The domain name itself

consists of the label, possibly concatenated with the name of its parent node on the right, separated by a dot. The tree sub-divides into *zones* beginning at the root zone. A DNS zone may consist of only one domain, or may consist of many domains and sub-domains, depending on the administrative choices of the zone manager. DNS can also be partitioned according to *class*; the separate classes can be thought of as an array of parallel namespace trees

IBM has hundreds of thousands of IP addresses and domain names. IBM would like to maintain its own domain name system server (DNS Server), also called just Domain Name Server, for the IBM.com domain. A domain Name server is simply a computer that contains the database and the software for mapping between domain names and IP addresses. Similarly, India wants to govern the in top - level domain; and Australia wants to take care of the au domain, and so on. IBM is totally responsible for maintaining the name server for IBM.com.

5.15. ROLE OF DNS SERVER

(Apr/May-2015, 2012; Oct/Nov-2013; Mar/Apr-2009)

The DNS server works very similar to a telephone directory inquiry service. You dial up the enquiry service and ask for a person's telephone number, based on the name. In the DNS, you specify the Domain name and ask for its corresponding IP address.

Basically, DNS Servers do two things:

1. Accept requests from programs for converting domain names in to IP addresses.
2. Accept requests from other DNS Servers to convert domain names in to IP addresses.

When such a request comes in, a DNS Server has the following options:

1. It can supply the IP address because it already knows the IP address for the domain.
2. It can contact another DNS Server and try to locate the IP address for the name requested. It may have to do this more than once. Every DNS Server has an entry called alternate DNS Server, which is the DNS Server it should get in touch with for unresolved domains. The DNS hierarchy specifies how the chains between the various DNS Servers should be established for this purpose. That discussion is beyond the scope of the current text.
3. It can simply say, I don't know the IP address for the domain name, it suggests the name of another DNS Server.
4. It can return an error message because the requested domain name is invalid or does not exist this is shown in Fig.

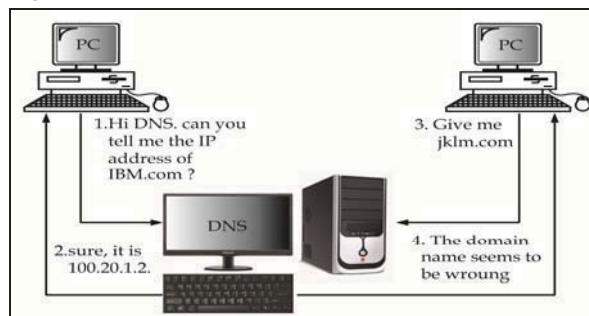


Fig : Interactions between Hosts and a DNS Server

As the figure shows, one host is interested in knowing the IP address of the server at IBM.com. For this purpose, it contacts its nearest DNS Server. The DNS Server looks at the list of domain names and their IP addresses. It finds an entry for the domain and sends it back to the client computer. However, when the DNS Server receives another request

from another computer for jklm.com, it replies saying that such a domain name does not exist. As we know, it might consult other DNS Servers to see if they have any idea about this domain name, or it might suggest the name of another DNS Server that the host should contact.

5.16. DOMAIN NAME SYSTEM

Computers work at their best when dealing with numbers, to identify an entity, TCP / IP protocols use the IP address, which uniquely identifies the connection of a host to the internet. However people prefer to use names instead of address. Therefore, we need a system that can map a name of an address and conversely an address to a name.

We have been using IP address to identify hosts. While these addresses are perfectly suited for processing by routers. Users (humans) are more comfortable with names than with digits. Thus we need a system that maps address to names and vice versa. The naming system used by TCP / IP is called **Domain Name System (DNS)**. This system was developed in 1984 mokapetris.

Internet uses a hierarchical naming system is called **DNS**. In the early days of the internet, all domain names (also called host names) and their associated IP address were recorded in a single file called hosts.txt. The Network Information Center (NIC) in the US maintained this file. A portion of the hypothetical hosts.txt file is shown in Fig. for conceptual understanding.

Host Name	IP address
John.abc.com	120.10.210.90
Pete. xyz.co.uk	131.90.120.71
Julie.pqr.com	171.92.10.89
....

Fig.: Hosts.txt file – A logical view.

5.17. DNS NAME SPACE

(Oct/Nov-2013,2011,2010; Mar/Apr-2008)

In Internet, the domain name space (tree) is divided into three different section:

1. Generic Domain
2. Country Domain
3. Inverse Domain

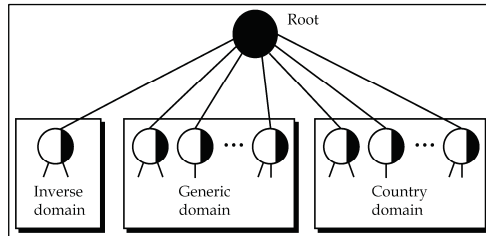


Fig. DNS in the Internet

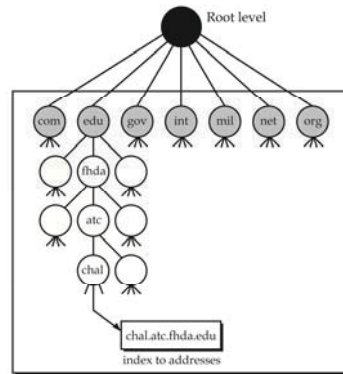
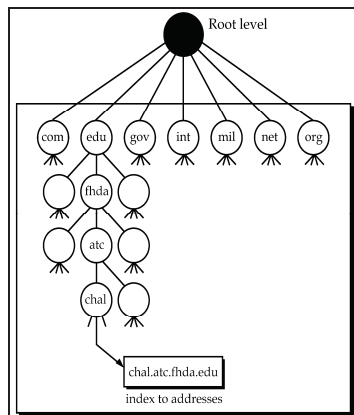


Fig. (a): Generic Domains

1. Generic Domain:

The generic domains define registered hosts according to their generic behaviour. Each node in the tree defines a domain, which is index to the domain name space data base (see in Fig.). Looking at the tree, we see that the first level in the generic domain section allows seven possible three characters labels. These labels describe the organization types as listed in table.

Recently a few more first level labels have been proposed. These are shown in table:

TABLE: Generic Domain Labels **TABLE:** Proposed Generic Domain Labels

.Com	Commercial organization	Arts	Cultural organizations
.Edu	Educational institutions	Firm	Business or firms
.Gov	Government institutions	Info	information service providers
.Int	International organizations	Nom	Personal nomenclatures
.Mil	Military groups	Rec	Recreation/entertainment organizations
.Net	Network support centers	Store	Businesses offering goods to purchase
.Org	Nonprofit organization	Web	Web-related organization

2. Country Domain:

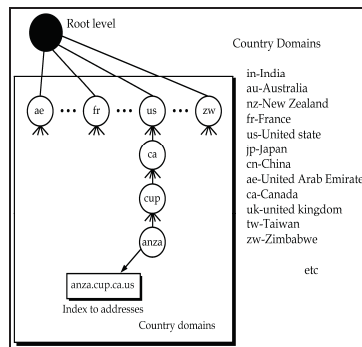


Fig. (b)Country Domains

The country domain section follows the same format as the generic domains but uses two character country abbreviation. (eg. us for United States, in for India, uk for United Kingdom, Jp for Japan and Ge for Germany in place of the three character organizational abbreviations at the first level.

Second level labels can be organizational or they can be more specific, national designations. The united states, for

example, uses state abbreviations as a sub division of US (eg. ca.us).

The address anza.cup.ca.us can be translated to De Anza college in cupertino in california in the United States.

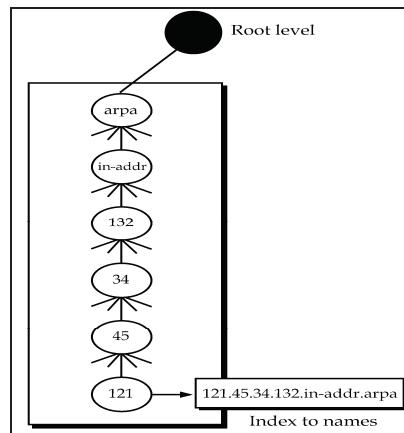
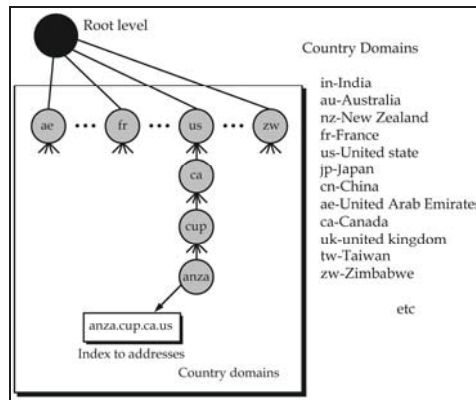


Fig. (c): Inverse Domain

3. Inverse Domain:

The Inverse domain is used to map an address to a name. This may happen, for example, when a server has received a request from a client to a task, where as the server

has a file that contains a list of authorized clients, the server list only the IP address of the client (extracted from the received IP packets). To determine if the client is on the authorized list, it can send a query to the DNS server list, it can send a query to the DNS server list, it can send a query to the DNS server and ask for a mapping of address to name.

5.18. ELECTRONIC MAIL (E-MAIL)

Electronic Mail was created to allow two individuals to communicate using computers. In the early days, email technology allowed one person to type a message and then send it to another person over the internet. It was like posting a card, except that the communication was electronic, instead of on paper, these days, the email facility allows many features such as:

- Composing and sending / receiving a message.
- Storing / forwarding / deleting / replying to a message with normally expected facilities, such as carbon copy (CC) blind carbon copy (BCC) etc.
- Sending a single message to more than one person.
- Sending text, voice, graphics and video.

5.19 How email is Transferred

(Oct/Nov-2013; Mar/Apr-2013, Apr/May-2012)

There are many components of the email architecture as shown in the Fig: as briefly described below:

- **User Agent (UA):** Each User communicates with a program or process is called a User Agent (UA). UA is the electronic mail programme associated with a specific operating system that allows user to type and edit messages.

- **Mail Box:** There is a one mail box for one user which acts as email storage system for that user.
- **Spool:** Spool is a queue of messages. The message in a spool are sent on a first come first scratched basis.
- **Mail Transfer Agent (MTA):** The mail transfer agent is the interface between the email system and the local e-mail server. The application that handled the reception and delivery of e-mail messages. Its operation is similar to the postal system

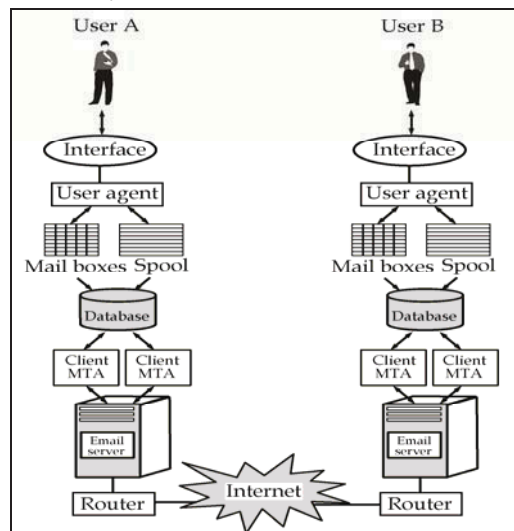


FIG: The Entire e-mail System

5.20. POP SERVER AND SMTP SERVER

(Mar/Apr-2014,2009)

For email messaging, every domain has e-mail server computers. These email servers run protocol software that enable electronic communication. These are two main email protocols.

1. POP and 2. SMTP

- POP is concerned with the retrieval of an email messages stored on a server computer.
- SMTP is actually responsible for transmitting an email message between the sender and the recipient.

Because both the email protocol software programs run on server computers, the server computers themselves are called as POP Server and SMTP Server, respectively. Actually, a single server computer can host both SMTP and POP Server programs.

POP Server:

The Post Office Protocol (POP) provides a standard mechanism for retrieving emails from a remote server for a mail recipient. For instance, suppose that a home user-B usually connects to the Internet using a dial-up connection to an ISP. Also suppose that another person 'A' has sent an email to 'B'. when 'B' is not connected to the Internet . Now the email gets stored in the mailbox for user B provided by the ISP.

When B connects to the internet the next time and wants to see the new emails that have arrived, he opens his email client program. That email client program on his computer in turn invokes a pop client, which contacts the pop server hosted by the ISP. The POP Server then open the mailbox for user-B and sends the emails arrived for him to POP client (i.e. to the user's computer)

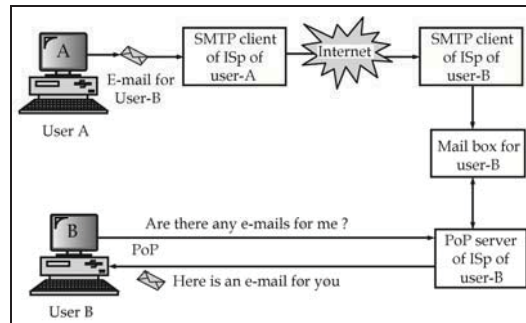


Fig. : SMTP and POP Servers

Step 1: A user A sends an email for another user B. This email travels from the SMPT Client of A via the internet to the SMPT server of B (described later). The SMPT server at the ISP of user B receives and stores this email in the user's mailbox.

Step 2: When the user B connects to the internet the next time, its POP client inquires with the POP server of her/his ISP, for any new material messages. The POP server of the ISP sends the new email for B (which was sent by user Y) in response.

SMTP server :

The simple mail transfer protocol (SMTP) actually transfers the email messages from the SMTP Server of the sender to the SMTP Server of the recipient. Its main job is to carry the email message between the sender and the recipient of course, it uses the TCP / IP protocol.

1. At the sender's end, an SMTP Server takes the messages sent by a user's computer.
2. The SMTP Server at the sender's end then transfers the messages to the SMTP Server of the recipient.
3. The SMTP Server at the recipient's end then takes the email message and gives it to the POP Server at the recipient's end.

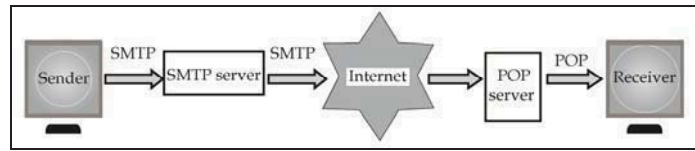


Fig:1SMTP server

5.6.3 DIFFERENCE BETWEEN SMTP AND POP

Although both SMTP and POP communicate over the internet, there are several differences between them, as follows:

- The protocols themselves are different (SMTP and POP).
- SMTP accepts a message from an arbitrary sender, where as POP Server allows only a user to access his mail box offer the user authenticates himself (using a user ID and password).
- SMTP Server can transfer only email messages, where as a POP server can also provide information about the mailbox contents (e.g., the number of un-read mails, a list of sent mails, etc.).

S.No	SMTP	POP
1.	SMTP: Simple Mail Transfer Protocol	POP : Post Office Protocol
2.	SMTP accepts a message from an sender directly	Pop Server does not directly accept the email messages from the user. It allows only a user to access his / her mail box after the user authenticates himself(using a user id and pass word)

3.	SMTP is actually responsible for transmitting an email message between the sender and the receiver.	POP concerned with retrieval (get back) of an email message stored on a server computer.
----	---	--

Fig. Complete Journey of an E-mail Message

5.21. FILE TRANSFER OPERATION USING FTP

(Oct/Nov-2015,2012,2011.2009,2008;Apr/May-2015,2011,2010, 2013,2009, 2008)

Email are usually just short messages. Transferring files from one computer to another is quite different. A special software and set of rules called File Transfer Protocol (FTP) exists for this purpose.

- FTP is the Standard mechanism provided by TCP / IP for copying file from one computer to another.
- Transferring files from one system to another seems simple and straight forward but some problems must be dealt with.

Ex: When a user wants to download a file from a server several issues must be dealt with.

1. The client must have the necessary authorization to download that file.
2. ``Client and Server computers could be different in terms of their hardware and / or operating system. This means that they represents data in different formats.

These problems have been solved by FTP.

- At a high level, a user (the client) requests the FTP Software to either retrieve from or upload a file to a remote server.

- For this, a user at the FTP client host might enter a command such as Get ABC, which means that the client is interested in obtaining a file called as ABC from the specified server. FTP supports other commands such as PUT, OPEN, CLOSE etc.

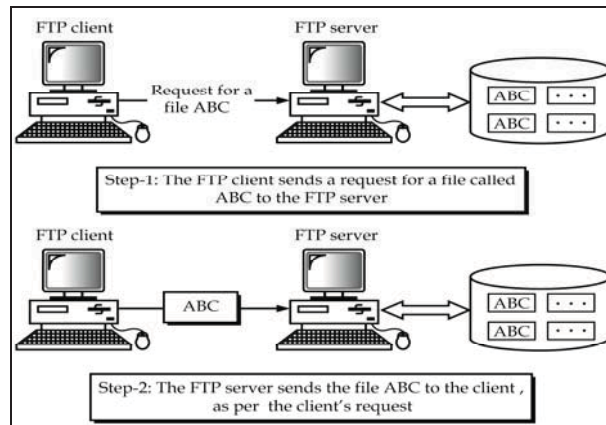


Fig. : How FTP Client can obtain a file ABC from an FTP Server

FTP Operation:

When user download a file from remote computer (server), first user computer establishes a connection with a remote server. FTP contacts the remote server. FTP contacts the computer using the TCP / IP software once connection is established, the user can chose to download a file from the server computer or user can send a file from his computer to the server computer.

FTP uses two connections between a client (user) and a server

- One connection is used for the actual files data transfer and other connection is used for control information commands and responses). This separation of data transfer and commands makes FTP more efficient.

Internally, this means that FTP uses two TCP / IP connections between the client and the server.

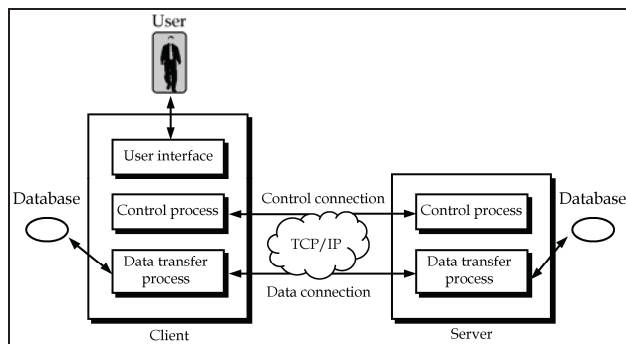


Fig. (a): FTP

- Shown in the Fig. , the client has three components : User Interfaces, the client control process and the client data transfer process and server has two components : Server control process and server data transfer process.
- TCP control connection is made between the control processes of the client and server. And also TCP data transfer connection is made between the data transfer processes of the client and the server.

1. Control Connection:

Over the control connection the FTP communication consists of one request and one response. This request - response model is sufficient for FTP, since the user sends one command to the FTP Server at a time.

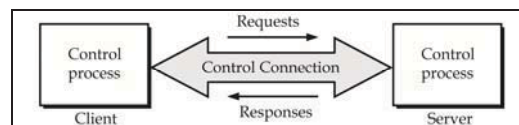


Fig. a.1: Command Processing Using the Control Connection

The requests sent over the control connection are four-character commands such as QUIT (to log out of the system) ABOR (to abort the previous command), DELE (to delete a file), LIST (to view the directory structure), RETR (to retrieve a file from the server to the client), STOR (to upload a file from the client to the server) etc.

2. Data Transfer Connection:

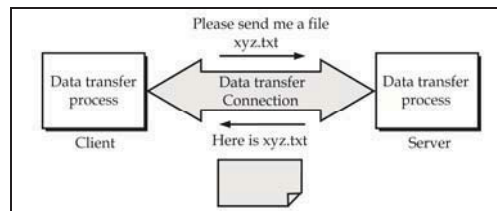


Fig .a.2 : File Transfer using the Data Transfer Connection

The data transfer connection is used to transfer files from the server to the client or from the client to the server, as shown in Fig. This is decided based on the commands that travel over the control connection.

5.22. WORKING OF WEB SERVER

(Oct/Nov-2015, 2014, 2009; Apr/May-2012; Mar/Apr-2009)

Client - Server communication use of TCP /IP Software applying for email, FTP and WWW.

- In case of email, it is the email client and the email server software that communicate.
- In case of FTP, it is the FTP Client and FTP server programs that communicate.
- In case of WWW, the roles are performed by the Web Browser (the client) and the Web Server (Server). In all the cases, whatever is sent from the client to the server (request for a web page) and from the server to client is sent, using TCP / IP.

Working of Web Server:

- A Web Server is a program running on a Server computer. Web Server consists of Web Site containing number of web - pages. A web page is created by using special language called as Hyper Text Mark up Language (HTML). HTML allows text, graphics, sound, video and animation that people want to see or hear.
- Each webpage is stored in HTML format on Server. Every Website has a Server Process (a running instance of program) that listens to TCP connection requests coming from different clients all the time. After a TCP connection is established, the client requests a server for web page. For this the client sends one request and server sends one response. This request and response model is governed by a protocol called Hyper Text Transfer Protocol (HTTP).
- “HTTP Software on the client” request for a web page and the “HTTP Software on the Server” sent response back to the client. Thus both client and Server computers must have HTTP softwares running on them.
- A client requests the server for a specific web page. Each web page is stored in HTML Format on Server. On receiving such request, the Server locates the webpage with the help of the operating system and sends it back to the client using TCP / IP. After receiving the webpage in HTML format and translate into original and it is displayed on screen of the client computer.

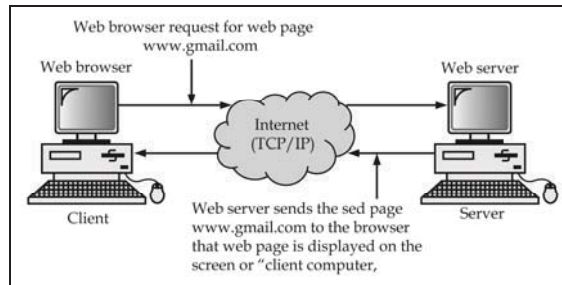


Fig.: Working of Web Server

5.23. WORKING OF WEB BROWSER

(Oct/Nov-2014,2013, 2012,2010 ; Apr/May-2015,2011,2010, Mar/Apr-2014,2008)

A Web browser acts as the client in the WWW interaction. Using this program, a user sends a request for a webpage stored on a web server. The web server, search that web page and sends it back to the client computer. The web browser displays the webpage in HTML format on the client computer's screen.

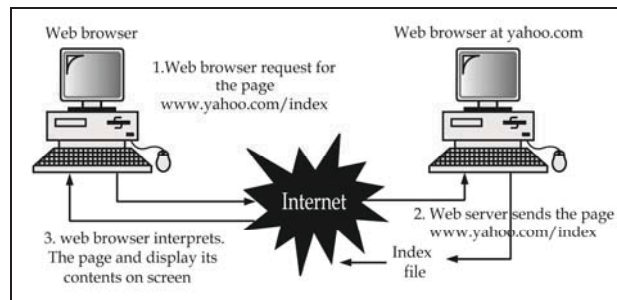


Fig : Interaction between a Web Browser and a Web Server

The typical interaction between a web browser (the client) and a web server (the server) is as shown in Fig.

1. The user on the client computer types the full file name including the domain name of the web server on the screen provided by the web browser program running

on his computer. This full file name is called as Uniform Resource Locator (URL).

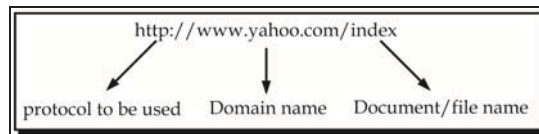


Fig.: Anatomy of URL

Here Forward Slash (/) → It indicates that the file is one of the many files stored in the domain Yahoo.com.

2. DNS browser requests DNS for the IP address corresponding to WWW.Yahoo.com.
3. DNS replies with IP address for WWW.Yahoo.com (let us say it is 120.10.23.21).
4. The browser makes a TCP connection with the computer. 120.10.23.21 (which is a Yahoo Server.).
5. The client request for the web page (WWW.Yahoo.com / index) to the web server using HTTP request.
6. The request is handed over to the HTTP Software running on the client machine be transmitted to the server.
7. The HTTP software on the client now hands over the HTTP request to the TCP / IP software running on the client.
8. The TCP/IP software running on the client breaks the HTTP request into packets and sends them over TCP to the web server (in this case, Yahoo.com)
9. The TCP / IP software running on the web server reassembles the HTTP request using the packets thus received and gives it to the HTTP software application layer running on the web server, which is Yahoo.com in this case.

10. The HTTP software running on the web server interprets the HTTP request. It realizes that the browser has asked for the file index.htm on the server. Therefore, it requests the operating system running on the server for that file.
11. The operating system on the webserver locates index.htm file and gives it to the HTTP software running on the web server.
12. The HTTP software on the web server now hands over this HTTP response to the TCP / IP software running on the web server.
13. The TCP / IP software running on the web server breaks the HTTP response into packets and sends it over the TCP connection to the client. As we know, IP takes care of routing and TCP takes care of reassembly and correctness of the message.
14. The TCP / IP software on the client computer checks the packets for correctness and reassemble them to form the original web page in the HTML format. It informs the TCP / IP software on the server that the web page was received correctly, which informs HTTP on the server.
15. The received web page is in the HTML form and converts into original information and that was displayed on the screen of the client computer.

5.24. HTTP COMMANDS

(Apr/May-2015, 2011,2008;Oct/Nov-2013,2010,2008;Mar/Apr-2008)

A few commands in the HTTP (Hyper Text Transfer Protocol) When a client requests a server for a webpage, as summarized in the Fig.

HTTP Command	Description
GET	Request for obtaining a web page
HEAD	Request to read the header of a web page
PUT	Requests the server to store a web page
POST	Similar to PUT, but is used for updating a web page
DELETE	Removing a web page
LINK	Connects two resources
UNLINK	Disconnects two resources

Fig.: HTTP Request Commands

A browser uses the commands shown in Fig. When it sends an HTTP request to a web server. Let us discuss each of them. Note that these commands are case sensitive.

- **GET:** Sends a request for a Webpage.
- **HEAD:** Request the server to read the header of a webpage.
- **PUT:** This command is the exact opposite of the GET command. It requests the server to store a webpage.
- **POST:** It is used for updating a Web page.
- **DELETE:** This command allows a browser to send an HTTP request for deleting a particular Webpage.
- **LINK:** This command is used to establish hyperlinks between two webpages.
- **UNLINK:** This command is used to remove existing hyper links between two pages.

5.25. PURPOSE OF PROXY SERVER

(Mar/Apr-2014,2009;Oct/Nov-2011;Apr/May- 2010)

The Proxy server reduces the load (i.e., decreases the traffic) on the original servers.

A proxy server is a computer that keeps copies of responses to the recent request. The HTTP Client sends a request to the proxy server, the proxy server checks it cache, the proxy server sends the request to the corresponding

server (original server). The original server sends the request page to the proxy server, then the proxy server sends the response to the HTTP client. The proxy server acts as both server and a client.

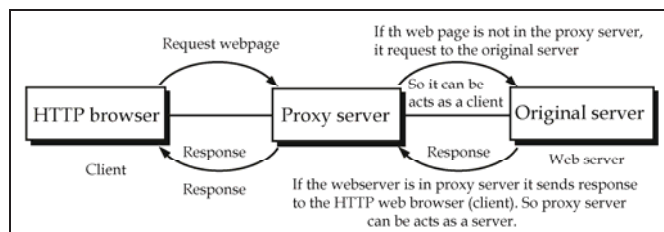


Fig.: Proxy Server can act as Client as well as Server

- A web browser understands HTTP and FTP but not protocols such as Gopher and Many other old protocols. A proxy server acts as an interpreter between the web browser and the web server for transforming a non-HTTP Protocols (FTP, Gopher etc.) to HTTP and Vice Versa.
- A complete proxy server should be able to communicate all the web protocols, the most important ones being HTTP, FTP, Gopher etc.

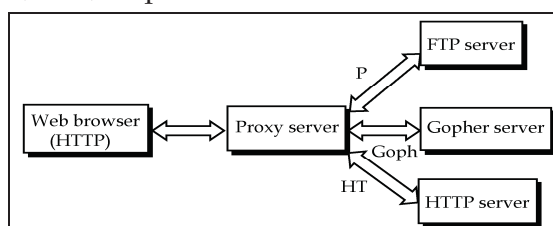


Fig. : Proxy Server

Usually, the proxy server is installed on a dedicated computer in an organization and the organization's connection to the internet directly via the proxy server. This means that every user's internet connection passes via the proxy.

Proxy servers can also be used to filter requests. For example, a company may use a proxy server to prevent its employees from accessing a specific set of websites.

5.26. USE OF HYPERLINKS

(Oct/Nov-2014,2013, 2009, Mar/Apr-2008)

HTML has a very interesting property. It supports the concept of “links”. WWW initially was just a set of linked HTML documents web pages usually offer links to other web pages. For example, suppose we are currently viewing a web page that shows a report on today’s stock market. There might be links in that web page to some of the companies mentioned in the report. These could be shown underlined or in different color to indicate that these are actually links to other web pages. Such links are called “hyper links”. You can point your mouse on any such hyperlink and click. In response, the browser would actually take you to that web page. A conceptual view of how hyperlinks look is shown in Fig.

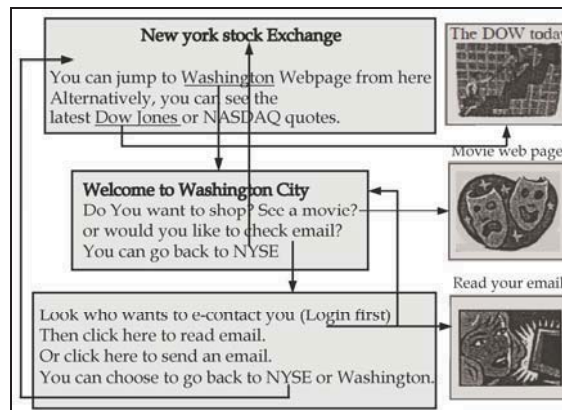


Fig.: Concepts of Hyper links

Suppose the user is presently viewing the “**New York Stock Exchange**” Page. Three hyperlinks are shown to the

user on this page (see the underlined text). By clicking on any of these hyperlinks, the user can go to the corresponding web page. For instance, when the user clicks on the hyperlink **washington**, the browser would take her / him to the “**Washington city**” home page. The “**Washington city**” home page has many hyperlinks that allow the user to either visit a shopping web page or a watch a movie on line.

HTML uses the “anchor tag” for creating hyper links. For example, suppose Linda has a web page from which she wants to allow the user an option of going to the “amazon.com” Web page. What she needs to do is simple. Add an anchor tag, specifying the uniform resource locator (URL) of “amazon.com”, as shown in fig. at appropriate place in her / his web page.

```

<HTML>
<TITLE> Linda's home page </TITLE>
.....
<A HREF="http://www.amazon.com">click here to go to amazon.com </A>

```

```

Linda's Home page!!!
Hi! This ia Linda Johnson's homepage
.....
Click here to go to amazon.com
.....

```

Fig. How to add hyperlinks

As a result, the webpage, when displayed Fig. Note that the URL does not appear on the web page. Instead, the message associated with it is displayed.

5.27. WEB BROWSER ARCHITECTURE

(Oct/Nov-2014,2013,2012,2010 ; Apr/May-2015,2011,2010, Mar/Apr-2014,2008)

1. A browser to open a new TCP Connection and request a specific Web page. When a web server receives such a request, it locates the webpage, and sends it back, closes the TCP connection with that browser and waits for another request.

2. It is the responsibility of the browser to access and display the document on the user's screen when it receives it from the server. A browser consists of several large software components that work together that provides required output.
3. A browser contains some pieces of software that are mandatory and some that are optional depending upon the usage.
4. The HTTP client program (2) and the HTML interpreter program (3) shown in the below Fig. are mandatory.
5. Some other interpreter programs (4), Java interpreter program (5) and other optional interpreter programs (6) are not mandatory.

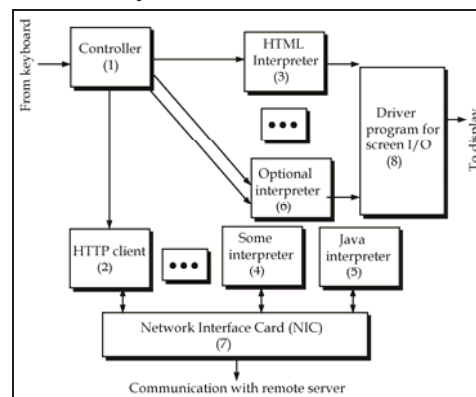


Fig.: Internal Architecture of a Web Browser

6. The browser also has a controller (1), which manages all of them. The controller is like the control unit in a computer's CPU. It interprets both mouse clicks selections and keyboard inputs, based on these inputs, it calls the rest of the browser's components to perform specific tasks. For instance, When a user types a URL, the controller calls the HTTP Client program to fetch the requested web page from a remote web server whose

address is given by the URL. When the webpage is received, the controller calls the HTML interpreter to interpret the tags and display the webpage on the screen.

7. The HTML browser takes an HTML document as input and displays a formatted version of it on the screen. To do this, it interprets the various HTML tags and translates them into display commands based on the display hardware in the user's computer.

5.28. REMOTE LOGIN

(Oct/Nov-2015,2014, 2011,2008;Mar/Apr-2014,2013;Apr/May-2012)

When a user want to access an application program located on a remote machine. He / she performs remote login. Here the telnet client & server programs comes into use.

1. The commands and characters typed by the user are sent to the operating system through the Terminal driver. The operating system does not change the commands and characters entered by the user.
2. The operating system sends these commands and characters to a TELENET Client. The Telenet is located on the same server computer.
3. The Telenet client transforms the characters entered by the user to a universally agreed format called Network Virtual Terminal (NVT) characters and sends them to the TCP / IP Protocol Stack.

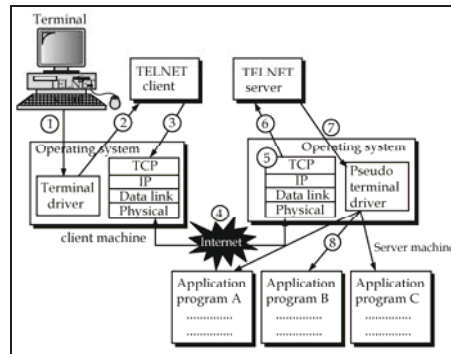


Fig.: Remote Login Using Telenet

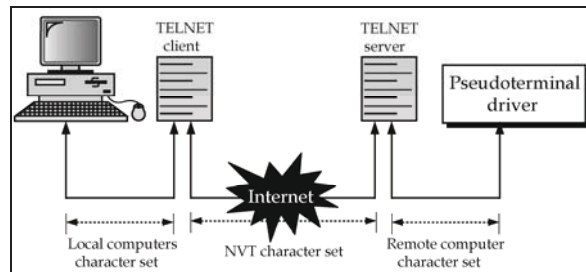


Fig.: Concept of NVT

Network virtual terminal is a uniform data representation that ensures the compatibility of communication between terminals and host that may use very different hardware & software and data formats. The TELENET client translate the user input for terminal device to NVT for transcode to the Telenet server where it is converted to Hosts internal format. The process is reversed output from the server to client.

4. The commands or Text in the NVT format then travel from the client to the TCP / IP stack of the remote computer via the Internet. That is, the commands or text are first broken into TCP and then IP packets, and are sent across the physical medium from client to the remote computer (server computer).

5. At the remote computer's end, the TCP / IP software collects all the IP packets, verifies their correctness / completeness, and reconstructs the original command so that it can hand over these commands & text to that computer's O.S.
6. The characters delivered to operating system and passed through TELENET Server which change the characters understandable by Telenet Server.
7. The characters can not be passed directly to O.S. because the remote operating system is not design receive characters from a Telenet Server. The solution is to add to piece of a software called a pseudo terminal driver, which pretends that the characters are coming from a terminal.
8. The operating system then passes the characters to the appropriate application program.

NOTE: TELENET is an abbreviation for "Terminal Network". It enables the establishment of a connection to a remote system in such a way that the local terminal (client) to be a terminal act the remote system.

TELNET Protocol provides a way for users (Clients) to connect to multiuser computer (or servers), on the Internet. The main task of the Internet and its TCP /IP protocol suite is to provide services for users. A user access any application program (HTTP, FTP, SMTP etc.) on a remote computer i.e., allows the user to logon to a remote computer by using a popular client - server application program called TELENET.

REVIEW QUESTIONS**Short Answer Type Questions:**

1. List the three commonly used WAN technologies.
(Oct/Nov-2011)
2. Write the functions of port and sockets.
3. What is role of gateway.
(Oct/Nov-2011)
4. List the different layers of TCP / IP.
(Oct/Nov-2015,2013; Apr/May- 2011, Mar/Apr-2008)
5. What are the functions of ports & sockets.
(Mar/Apr-2014, 2009; Apr/May-2010;Oct/Nov-2008)
6. Difference between TCP & UDP.
(Oct/Nov-2008)
7. List the features of TCP.
(Oct/Nov-2012;Apr/May-2012)

Essay Type Questions :

1. Explain about WAN architecture.
(Oct/Nov-2015; Apr/May-2011)
2. Describe the working of X.25 WAN Protocol.
(Oct/Nov-2009)
3. Describe the FRAME relay WAN Protocol.
(Apr/ May-2011;Mar/ Apr-2009,2008)
4. Explain ATM WAN Protocol.
(Apr/May-2011, 2010; Oct/Nov-2009; Mar/Apr-2008)
5. Describe the ARPANET.
(Oct/Nov-2008; Mar/Apr-2013)
6. Describe the WWW.
(Mar/Apr-2013)
7. Explain about APRANET & WWW
(Apr/May-2015; Mar/Apr-2013,2008; Oct/Nov-2011)

8. Explain different layers of TCP/IP
(Mar/Apr-2013,2009; Oct/Nov-2012,2011,2009;Apr/May-2012)
 9. Explain the features of TCP
(Apr/May-2015, 2012,2010, Oct/Nov- 2012,2010,2008)
 10. Explain Address Resolution Protocol (ARP).
(Oct/Nov-2010)
 11. Describe the use of Gateways
(Apr/May-2015, 2011,2010;Oct/Nov-2011, 2010; Mar/Apr-2008)
 12. Explain the connectivity of systems using TCP & UDP
(Oct/Nov-2011)
- Describe the features of UDP