INFORMATION & COMMUNICATION TECHNOLOGY SYSTEM MAINTENANCE

NSQF LEVEL - 4

2nd Year

TRADE THEORY

SECTOR: IT & ITES

(As per revised syllabus July 2022 - 1200 Hrs)

Directorate General of Training

DIRECTORATE GENERAL OF TRAINING
MINISTRY OF SKILL DEVELOPMENT & ENTREPRENEURSHIP
GOVERNMENT OF INDIA

NATIONAL INSTRUCTIONAL MEDIA INSTITUTE, CHENNAI

Post Box No. 3142, CTI Campus, Guindy, Chennai - 600 032

Sector : IT & ITES

Duration : 2 Years

Trades : Information & Communication Technology System Maintenance - Trade Theory - 2nd Year - NSQF Level- 4 (Revised 2022)

Developed & Published by

National Instructional Media Institute
Post Box No.3142
Guindy, Chennai - 600 032
INDIA
Email: chennai-nimi@nic.in
Website: www.nimi.gov.in

First Edition : April 2024 Copies : 500

Rs.300/-

FOREWORD

The Government of India has set an ambitious target of imparting skills to 30 crores people, one out of every four Indians, to help them secure jobs as part of the National Skills Development Policy. Industrial Training Institutes (ITIs) play a vital role in this process especially in terms of providing skilled manpower. Keeping this in mind, and for providing the current industry relevant skill training to Trainees, ITI syllabus has been recently updated with the help of Media Development Committee members of various stakeholders viz. Industries, Entrepreneurs, Academicians and representatives from ITIs.

The National Instructional Media Institute (NIMI), Chennai, has now come up with instructional material to suit the revised curriculum for **Information & Communication Technology System Maintenance - Trade Theory - 2nd Year - NSQF Level - 4 (Revised 2022) - in IT & ITES Sector** in **Annual Pattern.** The NSQF Level - 4 (Revised 2022) Trade Theory will help the trainees to get an international equivalency standard where their skill proficiency and competency will be duly recognized across the globe and this will also increase the scope of recognition of prior learning. NSQF Level - 4 (Revised 2022) trainees will also get the opportunities to promote life long learning and skill development. I have no doubt that with NSQF Level - 4 (Revised 2022) the trainers and trainees of ITIs, and all stakeholders will derive maximum benefits from these Instructional Media Packages IMPs and that NIMI's effort will go a long way in improving the quality of Vocational training in the country.

The Executive Director & Staff of NIMI and members of Media Development Committee deserve appreciation for their contribution in bringing out this publication.

Jai Hind

ATUL KUMAR TIWARI, *I.A.S*
Additional Secretary/Director General (Training)
Ministry of Skill Development & Entrepreneurship
Government of India.

April 2024
New Delhi - 110 001

PREFACE

The National Instructional Media Institute (NIMI) was established in 1986 at Chennai by then Directorate General of Employment and Training (D.G.E & T), Ministry of Labour and Employment, (now under Directorate General of Training, Ministry of Skill Development and Entrepreneurship) Government of India, with technical assistance from the Govt. of Federal Republic of Germany. The prime objective of this Institute is to develop and provide instructional materials for various trades as per the prescribed syllabus under the Craftsman and Apprenticeship Training Schemes.

The instructional materials are created keeping in mind, the main objective of Vocational Training under NCVET/NAC in India, which is to help an individual to master skills to do a job. The instructional materials are generated in the form of Instructional Media Packages (IMPs). An IMP consists of Theory book, Practical book, Test and Assignment book, Instructor Guide, Audio Visual Aid (Wall charts and Transparencies) and other support materials.

The trade practical book consists of series of exercises to be completed by the trainees in the workshop. These exercises are designed to ensure that all the skills in the prescribed syllabus are covered. The trade theory book provides related theoretical knowledge required to enable the trainee to do a job. The test and assignments will enable the instructor to give assignments for the evaluation of the performance of a trainee. The wall charts and transparencies are unique, as they not only help the instructor to effectively present a topic but also help him to assess the trainee's understanding. The instructor guide enables the instructor to plan his schedule of instruction, plan the raw material requirements, day to day lessons and demonstrations.

IMPs also deals with the complex skills required to be developed for effective team work. Necessary care has also been taken to include important skill areas of allied trades as prescribed in the syllabus.

The availability of a complete Instructional Media Package in an institute helps both the trainer and management to impart effective training.

The IMPs are the outcome of collective efforts of the staff members of NIMI and the members of the Media Development Committees specially drawn from Public and Private sector industries, various training institutes under the Directorate General of Training (DGT), Government and Private ITIs.

NIMI would like to take this opportunity to convey sincere thanks to the Directors of Employment & Training of various State Governments, Training Departments of Industries both in the Public and Private sectors, Officers of DGT and DGT field institutes, proof readers, individual media developers and coordinators, but for whose active support NIMI would not have been able to bring out this materials.

Chennai - 600 032 **EXECUTIVE DIRECTOR**

ACKNOWLEDGEMENT

National Instructional Media Institute (NIMI) sincerely acknowledges with thanks for the co-operation and contribution extended by the following Media Developers and their sponsoring organisation to bring out this IMP for the trade of **Information & Communication Technology System Maintenance - 2nd Year - Trade Theory - NSQF Level - 4 (Revised 2022)** under the **IT & ITES** Sector for ITIs.

MEDIA DEVELOPMENT COMMITTEE MEMBERS

Smt. M. Subhameena	_	Junior Training Officer, Govt. I.T.I. (Woman) Cuddalore.
Smt. P. Maheswari	_	Assistant Training Officer, Govt. I.T.I. (Woman) Guindy.
Smt. S. Sasikala	_	Assistant Training Officer, Govt. I.T.I. Madurai.

NIMI - COORDINATORS

Shri. Nirmalya Nath	_	Deputy Director, NIMI, Chennai - 32.
Shri. G. Micheal Johny	_	Manager, Co-ordinator, NIMI, Chennai - 32.
Shri. N. Sundararajan	_	Assistant Manager, NIMI, Chennai - 32.

NIMI records its appreciation of the Data Entry, CAD, DTP Operators for their excellent and devoted services in the process of development of this Instructional Material.

NIMI also acknowledges with thanks, the invaluable efforts rendered by all other staff who have contributed for the development of this Instructional Material.

NIMI is grateful to all others who have directly or indirectly helped in developing this IMP.

INTRODUCTION

TRADE PRACTICAL

The trade practical manual is intended to be used in workshop . It consists of a series of practical exercises to be completed by the trainees during the 2nd year course of the **Information & Communication Technology System Maintenance** under **IT & ITES Sector.** Trade supplemented and supported by instructions/ informations to assist in performing the exercises. These exercises are designed to ensure that all the skills in compliance with NSQF Level - 4 (Revised 2022) syllabus are covered.

This manual is divided into Thirty Three modules. The Thirty Three modules are given as below

Module 1	**LINUX Operating System**
Module 2	**Printers & Plotters**
Module 3	**Scanner and MFD**
Module 4	**Monitor, Display Card and Driver**
Module 5	**Sound Card**
Module 6	**UPS - (Uninterruptible Power Supply)**
Module 7	**Modem**
Module 8	**System Resources**
Module 9	**Practice on add on Cards, Cables & Connectors**
Module 10	**POST Code**
Module 11	**Upgrading of System**
Module 12	**Practice on Backup Drives**
Module 13	**Maintenance and Troubleshooting of PC**
Module 14	**Tablet / Smart Devices**
Module 15	**Internet and Web Browser**
Module 16	**Cloud Computing**
Module 17	**Components of the Computer Network**
Module 18	**Crimping & Punching**
Module 19	**Cabling**
Module 20	**Install and Configure a Network**
Module 21	**Configuration of Data Communication Equipments**
Module 22	**IP Addressing & TCP/IP**
Module 23	**Other Network Protocols**
Module 24	**Sharing Resource & Internet Connection**
Module 25	**Network Protection & Troubleshooting**
Module 26	**Control & Monitoring of Network Devices**
Module 27	**Network Security**
Module 28	**Server Installation & Basic Configuration**
Module 29	**Install and Configure DNS**
Module 30	**Routing and Remote Access**

Module 31	**Server Configuration and Back up**
Module 32	**Maintaining Network Infrastructure**
Module 33	**Linux Server Installation and Configuration**

The skill training in the shop floor is planned through a series of practical exercises centered around some practical project. However, there are few instances where the individual exercise does not form a part of project.

While developing the practical manual a sincere effort was made to prepare each exercise which will be easy to understand and carry out even by below average trainee. However the development team accept that there is a scope for further improvement. NIMI, looks forward to the suggestions from the experienced training faculty for improving the manual.

TRADE THEORY

The manual of trade theory consists of theoretical information for the two years course of the **Information & Communication Technology System Maintenance 2nd year** Trade Theory NSQF Level - 4 (Revised 2022) under **IT & ITES Sector**. The contents are sequenced according to the practical exercise contained in the manual on Trade practical. Attempt has been made to relate the theoretical aspects with the skill covered in each exercise to the extent possible. This correlation is maintained to help the trainees to develop the perceptional capabilities for performing the skills.

The Trade theory has to be taught and learnt along with the corresponding exercise contained in the manual on trade practical. The indicating about the corresponding practical exercise are given in every sheet of this manual.

It will be preferable to teach/learn the trade theory connected to each exercise atleast one class before performing the related skills in the shop floor. The trade theory is to be treated as an integrated part of each exercise.

The material is not the purpose of self learning and should be considered as supplementary to class room instruction.

CONTENTS

LEARNING / ASSESSABLE OUTCOME

On completion of this book you shall be able to

S.No.	Learning Outcome	Ref. Ex.No.
1	Install and customize Linux operating system. (NOS: SSC/N9428)	2.1.260 - 2.1.264
2	Install Printer, Scanner and troubleshoot their faults. (NOS: SSC/N9429)	2.2.265 - 2.3.298
3	Install/Replace Display Driver Card, perform servicing and configure various display unit. (NOS: SSC/N9430)2	2.4.299 - 2.4.306
4	Install/Replace Sound Card and set properties to adjust sound quality. (NOS: SSC/N9431)	2.5.307 - 2.5.314
5	Perform maintenance and servicing of UPS. (NOS: SSC/N9432)	2.6.315 - 2.6.322
6	Install and configure Modem, System Resources, Add on Cards, Cables & Connectors. (NOS: SSC/N9433)	2.7.323 - 2.9.325
7	Upgrade, maintain and troubleshoot PC. (NOS: SSC/N9434)	2.10.326 - 2.13.349
8	Assemble, replace and troubleshoot various parts of Tablet/ Smart Devices. (NOS: SSC/N9435)	2.14.350 - 2.14.361
9	Browse internet and work with Cloud Computing. (NOS: SSC/N9436)	2.15.362 - 2.16.368
10	Set up and configure Networking System using various network devices. (NOS: SSC/N9437)	2.17.369 - 2.23.389
11	Share and control resource and Internet connection through network. (NOS: SSC/N9438)	2.24.390 - 2.24.394
12	Implement Network Security to protect from various attacks on networking. (NOS: SSC/N9439)	2.25.395 - 2.25.398
13	Share and control resource and Internet connection through network. (NOS: SSC/N9438)	2.26.399 & 2.26.400
14	Implement Network Security to protect from various attacks on networking. (NOS: SSC/N9439)	2.27.401 - 2.27.403
15	Perform installation and basic configuration of Windows Server. (NOS: SSC/N9440)	2.28.404 - 2.28.408
16	Demonstrate installation, configuration of DNS, Routing and user account customization. (NOS: SSC/N9441)	2.29.409 - 2.30.416
17	Configure Server and manage Server Network security and Infrastructure. (NOS: SSC/N9442)	2.31.417 - 2.32.423
18	Perform installation and basic configuration of Linux server. (NOS: SSC/N9443)	2.33.424 - 2.33.431

SYLLABUS

2nd Year **Duration: Two years**

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 25Hrs; Professional Knowledge 10 Hrs	Install and customize Linux operating system. (NOS: SSC/ N9428)	**Linux operating system** 260. Installing UNIX/ LINUX. (05 hrs) 261. Preparing functional system UNIX/ LINUX. (05 hrs) 262. Adding new users, software, material components. (05 hrs) 263. Making back-up copies of the index and files. (05 hrs) 264. Dealing with the files and indexes. (05hrs)	• Basic Linux commands. • Linux file system, The Shell, Users and file permissions, VI editor, X window system, Filter Commands, Processes, Shell Scripting. (10 hrs.)
Professional Skill 70 Hrs; Professional Knowledge 20 Hrs .	Install Printer, Scanner and troubleshoot their faults. (NOS: SSC/ N9429)	**Printers & Plotters** 265. Testing front panel controls. Interface pins, cables, measurement of voltages and waveforms. (2 hrs) 266. Installing a printer and carrying self- test. (1hrs) 267. Replacing ribbon in a DMP. (1 hr) 268. Refilling ribbon tape of DMP. (1 hrs) 269. Testing and rectifying defective cable. (1 hrs) 270. Removing and cleaning printer head. (1 hr) 271. Replacing a new printer head. (2 hrs) 272. Testing and servicing Printer power supply. (1 hrs) 273. Changing rollers and other mechanical parts. (2 hrs) 274. Tracing the control board and identifying defective components. Servicing of control board. (2 hrs) 275. Replacement of toner cartridge of laser printers. (1 hrs) 276. Refilling toner cartridge of laser printers. (1 hrs) 277. Drum cleaning and replacement in of laser printers. (2 hrs) 278. Testing and servicing Printer power supply of laser printers. (2 hrs)	• Types of printers, Dot Matrix printer's laser printer, Ink jet printer, line printer. Block diagram and function of each unit head assembly, carriage, and paper feed mechanism. Front panel controls and interfaces. Pin details of interface port. • Installation of a printer driver. And self-test. • Ribbon types used. • Refilling of ribbons. • Printer cable testing defects, effect and servicing. • Printer head, types, cleaning procedures. • Precaution to be taken while removing and replacing printer head assembly. • Pinter power supply, circuit analysis, defects, servicing. Circuit, function, probable defects, servicing. • Carriage motor assembly, paper feed assembly, sensors. Procedure for dismantling and replacing mechanical parts. • Printer control board, circuit, function, probable defects, servicing. • Working principle of LASER printer.

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		279. Changing mechanical parts of laser printers. (2 hrs) 280. Tracing the control board circuit and identifying defective components. Servicing of control board of laser printers. (2 hrs) 281. Replacement of ink cartridge of desk jet/ inkjet printers. (1 hrs) 282. Refilling ink cartridge of desk jet/ inkjet printers. (1 hrs) 283. Drum cleaning and replacement in desk jet/ inkjet printers. (2 hrs) 284. Testing and servicing Printer power supply of desk jet/inkjet printers. (1 hrs) 285. Changing mechanical parts of desk jet/inkjet printers. (2 hrs) 286. Tracing the control board and identifying defective components. Servicing of control board of deskjet/ inkjet printers. (1 hrs) 287. Connecting and using high speed line printers. (1 hrs) 288. Replacing spares of line printers. (1 hrs) 289. Self-test procedures in printers. (1 hrs) 290. Use of diagnostics software for serving printers. (1 hrs)	• Toner cartridge, types, replacing toner cartridges • Refilling toner cartridges, equipment available for refilling and procedure. • Printer drum, function, cleaning and replacing procedure. • Power supply in laser printers, circuit, defects, servicing. • Mechanical parts and sensors on laser printer, function, replacement procedure. • Control board(s) in laser printer, circuit diagram, defects and servicing procedure. • Working principle of Inkjet/ Deskjet printers. Type of ink used and replacement of ink cartridge. • Refilling of ink, equipment available, quality of refilled cartridges. • Printer drum, function, cleaning and replacing procedure. • Power supply in inkjet printers, circuit, defects, servicing. • Mechanical parts and sensors on inkjet printer, function. • Working principle of Plotter and its common faults. (14 hrs.)
		Scanner & MFD 291. Scanner - Installation, configuration, using Automatic Document Feeder (ADF), OCR. (3 hrs) 292. Barcode Scanner - Installation and configuration. (3 hrs) 293. Network Scanner - Installation and configuration. (3 hrs) 294. Troubleshooting of Scanner. (6 hrs) 295. Multifunction Printer - Installation, Replacing supplies and spares, troubleshooting. (4 hrs)	• Working principles of Network Scanner. • Working principles of Multifunction Printer. • Working principles of Passbook printer. • Working principles of High Speed Printer. • Working principles of Line Printer. • Working principles of Network Printer. • Working principles of Print Server. (6 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		296. Passbook Printer - Installation, calibration, configuration & troubleshooting. Replacement of Supplies and maintenance. (5 hrs) 297. Network Printer – Installation and configuration, troubleshooting. (5 hrs) 298. How to update the flash of Motherboard, printer, scanner and modem etc. (6 hrs)	
Professional Skill 25 Hrs; Professional Knowledge 15 Hrs	Install/Replace Display Driver Card, perform servicing and configure various display unit. (NOS: SSC/N9430)	**Monitor, Display Card and Driver** 299. Identify the type of monitor connected to PC. Specifications, front panel controls and settings. (2 hrs) 300. Identify the specifications of the display driver card installed in the PC. (2 hrs) 301. Remove the display driver card and identify the main components and connectors on the display driver card. (4 hrs) 302. Replace the display driver card and re-install. (before practicing this skill set, the already installed driver should be removed from device manager). (4 hrs) 303. Change the exiting display card with a different card given and install. (2 hrs) 304. Servicing of monitors, changing fuses, adjusting colors, brightness and contrast. Setting resolution, loading drivers. Checking and replacing components on the PCB. Checking and adjusting LCD Monitors. (3 hrs) 305. Install, configure and operate LCD Projector. (6 hrs) 306. Install and Configure Touch Pad. (2 hrs)	• Types of monitor, Monochrome and color, CGA, EGA, VGA, SVGA, Digital Analogue, interlaced non-interlaced. Specifications and Comparison of Monitors. Front panel controls brightness, contrast, and horizontal and vertical height settings. • Display cards, bus standards, types CGA, EGA VGA, SVGA, AGP, memory and drivers. • Main components and connectors on display cards, display controller IC, RAM chips and dual port feature principle of working and use of display memory. • Installing display drivers, setting features. • Information required before changing the display driver card and precautions to be taken while installing a display driver card. • LCD and TFT Monitors. • Understanding the difference between flat screens and CRT display systems. • Understanding the displays memory and its effect on quality and performance. • Working principle of LCD Projector, its specification, configuration and common faults. • Working Principle of Touch Pad. (15 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 20 Hrs; Professional Knowledge 8 Hrs	Install/Replace Sound Card and set properties to adjust sound quality. (NOS: SSC/N9431)	**Sound Card** 307. Identify the specifications of the installed sound card in the PC. (3 hrs) 308. Identify and adjust the playback and recording properties of sound card/ driver. (3 hrs) 309. Remove the sound card from PC and identify the main components on the card. (3 hrs) 310. Replace the card and reinstall the sound card and set properties. (2 hrs) 311. Change the existing sound card with a different card given and install. (2 hrs) 312. Connect the speaker and microphone, adjust the controls for better quality sound and testing. (2 hrs) 313. Interconnect laptop to a multimedia projector and carryout adjustments. (3 hrs) 314. Replace battery pack in laptops and carryout general maintenance. (2 hrs)	• Specifications of sound card 16/32 bit stereo moNo. • Frequency response, sound files format, compression and decompression. • Principle of working and functional units of sound card. • Installation procedure of sound cards. • Main components on a sound card and its working. • Properties and specification of sound cards. • Information and resources required before installation of sound card. (8 hrs.)
Professional Skill 35 Hrs; Professional Knowledge 15 Hrs	Perform maintenance and servicing of UPS (NOS: SSC/N9432)	**UPS** 315. Identify the specifications of UPS. (4 hrs) 316. Switch-on and Switch-off procedure of UPS. (5 hrs) 317. Measurement of Input/ output voltage/ current levels, battery charge level. (4 hrs) 318. Identifying status of UPS from front panel indicators. (4 hrs) 319. Carryout routine maintenance of battery, battery terSSCals, loose contacts etc. (4 hrs) 320. Test UPS as per specification. Verification of back-up time. (4 hrs) 321. Circuit tracing and fault finding practice. (4 hrs) 322. Servicing of UPS by simulating more likely faults and systematic approach to identify and rectify them. (6 hrs)	• Study of typical working UPS circuit, explanation of each stage involved. Voltage, current, frequency and KVA specifications. • Controls of different type of UPS: On-line, Off- line, Line interactive etc. • Typical circuit blocks. • Routine maintenance of battery and UPS. • Back-up time, its dependence on battery, load and its calculations. • Possible problems in UPS, fault finding procedures. • Simulated faults and serving of UPS. (15 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 25Hrs; Professional Knowledge 07Hrs	Install and configure Modem, System Resources, Add on Cards, Cables & Connectors. (NOS: SSC/N9433)	**Modem** 323. Installation and configuration of different types of Modem e.g. DSL, ADSL, Data Card, Dongle etc. (08 hrs) **System Resources** 324. Practice on setting IRQ, DMA, Memory Address, I/O address, Resource Conflict, Plug & Play. (08 hrs) **Practice on Add on Cards, Cables & Connectors** 325. AGP, PCI Express, TV Tuner Card, DVR card, Video Capture, SCSI. USB, NIC, Fire wire, Card reader, network storage, Game video card, Camera etc. (09 hrs)	• Modem Fundamentals. • Band width, baud rate, wireless communication, synchronous/ asynchronous transmission. • IRQ, DMA, Memory Address, I/O address, Resource Conflict, Plug & Play Concept. • Different latest Add on Cards - (Identification in terms of I/O slot and connectors). (07 hrs.)
Professional Skill 125 Hrs; Professional Knowledge 34 Hrs	Upgrade, maintain and troubleshoot PC. (NOS: SSC/N9434)	**POST Code** 326. Rectify the serial, parallel and USB problem by reinsertion or replacement. (3 hrs) 327. Rectify the printer's problem by reinsertion or replacement. (3 hrs) 328. Rectify the MODEM problem by reinsertion or replacement. (3 hrs) 329. Rectify the windows start-up problem by reinsertion or replacement. (4 hrs) 330. Rectify the illegal operational problem by reinsertion or replacement. (3 hrs) 331. Rectify the virus protection utility problem by reinsertion or replacement. (3 hrs) 332. Rectify the networks problem by reinsertion or replacement. (3 hrs) 333. Rectify the external devises problem by reinsertion or replacement. (3 hrs)	• Recognize POST error message code as an indication of a serial, parallel and USB problem. • Recognize POST error message code as an indication of a printer's problem. • Recognize POST error message code as an indication of a MODEM problem. • Recognize POST error message code as an indication of a windows start-up problem. • Recognize POST error message code as an indication of an illegal operational problem. • Recognize POST error message code as an indication of a virus protection utility problem. • Recognize POST error message code as an indication of a networks problem. • Recognize POST error message code as an indication of an external devises problem (08 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		Upgrading of System 334. Mother board, Memory, CPU, Graphic Card, BIOS up- gradation, Additional features, Updating of System Software & Application Software (Requirement & How to update). (30 hrs) **Practice on Backup Drives** 335. Pen Drive U3 format, Zip Drive, Tape Drive, USB External Drive (HDD, CD/ DVD writer), Types, capacity, interface connector, write protection, Troubleshooting, Interface, Installation, casing for external drive. (20 hrs)	• Understand the limitation of a PC and scope for upgrading. • Understand technical specifications for PC upgrading. • SSCor repairs and maintenance of CD ROM drives. • Technology, working principle, capacity, and media of ZIP drives. • Important parts and functions of a ZIP drive. • SSCor repairs and maintenance of ZIP drive. • Important parts and functions of DVD ROM drive. • SSCor repair works on a DVD ROM drive. • SSCor repair works on a CD WRITER. • Technology, working principle, capacity, and media of Magneto- Optical Disk (MOD) drives. Applications. • Important parts and functions of MOD drive. • SSCor repair works on MOD. • Latest trends in backup devices/ media. (12 hrs.)
		Maintenance and Troubleshooting of PC 336. Running diagnostics program to identify the health and defects of a PC. Check system performance using third party utilities. Use benchmarking utilities to benchmark systems. (3 hrs) 337. Identify the defect in PC from the audible and observable symptoms such as beep sounds, post messages. Hanged keyboard, erratic display etc., and corrective action. (3 hrs) 338. Tracing the circuit of a KB. (3 hrs)	• Safety precautions in handling PC, sub-assemblies and components, Important points to be considered while purchasing and replacing components. Concept of Preventive and corrective maintenance. Tools required, Active & Passive Maintenance, Maintenance scheduling. Need of diagnostics program. Features, limitations. Examples of commonly used diagnostic programs.

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		339. Troubleshooting defects related to Keyboard and its related ports loose connections, replacing cable, replacing keys (DIN, PS/2, USB). (3 hrs) 340. Trouble shooting defects related to Mouse and its related ports loose connections, replacing cable, replacing roller and sensing elements. (COM, PS/2, USB). (3 hrs) 341. Study of interface cable connector, replacing of subassemblies of Light pen, scanner, digitizer. (3 hrs) 342. Troubleshooting defects related to HDD, (practice of replacing motor, head, PCB among faulty drives) cable and connector. (4 hrs) 343. Troubleshooting defects related to CD ROM Drive, Attempting for replacement and adjustments) cable and connector. (4 hrs) 344. Troubleshooting defects related Ports to Jumper setting. (4 hrs) 345. Troubleshooting defects related to Processor. (4 hrs) 346. Troubleshooting defects related to RAM memory modules. (4 hrs) 347. Troubleshooting defects related BIOS. (4 hrs) 348. Troubleshooting defects related to CMOS setup. (4 hrs) 349. Troubleshooting defects related to Battery. (4 hrs)	• Probable defects in PC. Localizing faults through its observable visual or audio symptoms and possible methods for rectification/ servicing. Understanding serviceability of component. Economy in repair/ replacement. • Block diagram of a KB, function of controller, LED driver Sample circuit. • Defects related to Keyboard and its related ports (DIN, PS/2, USB) Discontinuity in cable, and bad keys. Servicing procedure. • Defects related to Mouse and its related ports (COM, PS/2, USB) and servicing procedure. • Working principle, electro mechanical circuits of Light pen scanner and digitizer. • Defects and symptoms related to HDD and its cable, connector and servicing procedure. • Defects related to CD ROM Drive jamSSCg of mechanical assembly mal function of control circuit, and its cable, connector and servicing procedure. • Defects related to Ports jumper setting on motherboard and servicing procedure. • Defects related to processor, its socket, cooling and servicing procedure. • Defects related to RAM memory module connector and servicing procedure. • Defects related to BIOS, upgrading and servicing procedure. • Defects related to CMOS, COMS setup and servicing procedure. • Defects related to battery and servicing procedure. (14hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 50 Hrs; Professional Knowledge 12 Hrs	Assemble, replace and troubleshoot various parts of Tablet/ Smart Devices. (NOS: SSC/ N9435)	**Tablet/ Smart Devices** 350. Assembling & disassembling of different types of tablets/ Smart Devices. (5 hrs) 351. Testing of various parts with multimeter. (4 hrs) 352. Replacing of faulty parts. (4 hrs) 353. Fault finding & troubleshooting. (4 hrs) 354. Practice Advanced troubleshooting techniques. (5 hrs) 355. Flashing of various brands of tablets/ smart devices. (4 hrs) 356. Upgrading operating systems. (4 hrs) 357. Formatting of virus affected devices. (4 hrs) 358. Unlocking of handsets through codes and software. (4 hrs) 359. Troubleshooting settings faults. (4 hrs) 360. Working with iOS, Android, Ice-cream sandwich, Jellybeans. (4 hrs) 361. Installation of Phone Gap framework. (4 hrs)	• Circuit Board/ Motherboard Introduction. • Study of parts of a tablet PC/ smart devices. • Testing of various parts with multimeter. • Steps of repairing various hardware problems. • Advanced troubleshooting techniques. • Introduction of various software faults. • Flashing of various brands of tablets / smart devices. • Upgrading operating systems. • Locking &Unlocking of handsets. • Concept of iOS, Android, Ice-cream sandwich, jellybeans. • Concept of Phone Gap. (12 hrs.)
Professional Skill 25Hrs; Professional Knowledge 15 Hrs	Browse internet and work with Cloud Computing. (NOS: SSC/N9436)	**Internet and Web Browser** 362. Practice web browsing using popular web browsing software, Configuring web browser. (1hr) 363. Search for content using popular search engines. (1 hr) 364. Use favourite folder for browsing quickly. (2 hrs) 365. Downloading & Printing Webpages. (2 hrs) 366. Using e-mail – Opening & configuring email client, mailbox: inbox and outbox, Creating and sending e-mail, Replying to an e-mail message, Forwarding and e- mail message, Sorting and searching emails. (2 hrs)	**Internet and Web Browser** • World wide web and website. • Web Browsing and popular web browsing software. • Introduction to Search Engines, Popular Search engines. • Concept of Favorites Folder. • What is an Electronic Mail? • Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM. **Cloud Computing** • Introduction to Cloud Computing, how to access Cloud service providers & to create an account.

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		367. Sending document/ softcopy by email, activating spell checking, using address book, Handling SPAM, Removal of Cookies. (3 hrs) **Cloud Computing** 368. Work with Cloud services. (15 hrs)	**IT Act & Law** • Introduction to Cyber Security. • Introduction to Cyber Laws & IT Act. • Importance of privacy and techniques to manage it. (15 hrs.)
Professional Skill 190 Hrs; Professional Knowledge 60 Hrs	Set up and configure Networking System using various network devices. (NOS: SSC/ N9437)	**Components of the Computer Network** 369. Familiarization with various Network devices, Connectors and Cables. (5 hrs) 370. Understanding the Layout of network. (10 hrs)	• Introduction to Computer Networks – Advantages of Networking, Peer-to-Peer and Client/Server Network. • Network Topologies – Star, Ring, Bus, Tree, Mesh, Hybrid. • Type of Networks – Local Area Networks (LAN), Metropolitan Area Networks (MAN), Wide Area Networks (WAN). • Internet, Ethernet, Wi-Fi, Bluetooth, Mobile Networking, Wire and wireless Networking. • Difference between Intranet and Internet. (12 hrs.)
		Crimping & Punching 371. Crimping practice with straight and cross CAT 5 cables. (15 hrs) 372. Punching practice in IO Box and patch panel. (15 hrs) 373. Crimping and making cables. (20 hrs)	• Communication Media & Connectors – Unshielded twisted-pair (UTP), shielded twisted-pair (STP), Fiber Optics and coaxial cable: RJ-45, RJ-11, BNC. • Understanding color codes of CAT5 cable. 568A and 568B convention. (12 hrs.)
		Cabling 374. Create cabling in a lab with HUB/ Switch and IO Boxes and patch panel. (20 hrs) 375. Fitting Switch Rack. (5 hrs)	• Introduction to Data Communication – Analog and Digital Signals, Simplex, Half- Duplex and Full-Duplex transmission mode. (04 hrs.)
		Install & configure a Network 376. Installing & Configuring a Peer-to-Peer Network using Windows Software. (15 hrs) 377. Making cables by crimping. (5 hrs) 378. Connect computers using Bluetooth. (5 hrs)	• OSI Model - The functions of different layers in OSI model. (04 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		Configuration of Data communication equipments 379. Connecting computers with Network with Drop cable and using Wi-Fi configuration. (08hrs) 380. Basic Programmable switch Configuration Spanning Tree Protocol (STP). (07hrs) 381. Command Line Interface. (05hrs) 382. IP Routing Process. (03hrs) 383. Verifying Configuration. (02hrs)	• Network Components – Modems, Firewall, Hubs, Bridges, Routers, Gateways, Repeaters, Transceivers, Switches, Access point, etc. – their types, functions, advantages and applications. • IP Routing in Network RIP IGRP (09 hrs.)
		IP Addressing & TCP/ IP 384. IP addressing technique (IP4/ IP6) and Subnetting and Supernetting the network. (6 hrs) 385. Installation and Configuration of TCP/ IP Protocol. (6 hrs) 386. Practice TCP/ IP Utilities: PING, IPCONFIG, HOSTNAME, ROUTE, TRACERT etc. (6 hrs) 387. Setup and configure a Virtual LAN. (7 hrs)	• Protocols, TCP/IP, FTP, Telnet etc. • Theory on Setting IP Address(IP4/ IP6) & Subnet Mask, Classes of IP Addressing. • Overview of Virtual LAN. • VLAN Memberships. • Identifying VLAN. • Trunking - VLAN Trunk Protocol (VTP). • Concept of Translator Gateways. (10 hrs.)
		Other Network Protocols 388. Working with SMTP, TELNET, FTP, HTTP, SNMP, LDAP etc. (15 hrs) 389. Practice on configuring DHCP. (10 hrs)	• Simple Mail Transfer Protocol (SMTP), Telnet, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP). • LDAP (Lightweight Directory Access Protocol). • Network Security. Concept of Dynamic Host Control Protocol. (09 hrs.)
Professional Skill 25 Hrs; Professional Knowledge 10 Hrs	Share and control resource and Internet connection through network. (NOS: SSC/ N9438)	**Sharing Resource & Internet connection** 390. Sharing Resource and Advance Sharing Setting. (5 hrs) 391. Installing Proxy Server. (5 hrs) 392. Exposure and using Internet. Setting E-mail accounts. Conferencing. (5 hrs) 393. Installing and Configuring Internet. (5 hrs)	• Concept of Internet. • Architecture of Internet. • DNS Server. • Internet Access Techniques, ISPs and examples (Broadband/ Dialup/ WiFi). • Concept of Social Networking Sites, Video Calling & Conferencing. Concept of UTM and Firewall. (10 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
		394. Connection on a PC using Broadband or Dongle. (5 hrs)	
Professional Skill 25Hrs; Professional Knowledge 10 Hrs	Implement Network Security to protect from various attacks on networking. (NOS: SSC/N9439)	**Network Protection and troubleshooting** 395. Setting up basic protection using public keys and MAC address filters. (10 hrs) 396. Integrate wired with wireless network. (5 hrs) 397. Power over Ethernet (PoE). (5 hrs) 398. Troubleshooting wired and wireless network. (5 hrs)	• Collaborating using wired and wireless networks, Protecting a Network, Network performance study and enhancement. (10 hrs.)
Professional Skill 25Hrs; Professional Knowledge 10 Hrs	Share and control resource and Internet connection through network. (NOS: SSC/N9438)	**Control & monitoring of network devices** 399. Setting up of basic collaboration tool like NetMeeting for activities like chat, application sharing, remote desktop access and control, VoIP. (15 hrs) 400. Setup IP camera for basic surveillance scenario, logging and monitoring of devices/ locations. (10 hrs)	• Surveillance using network devices, collaboration on network for team optimization and support activities. • Remote management of devices. (10 hrs.) • Modern Network Security Threats and the basics of securing a network.
Professional Skill 25Hrs; Professional Knowledge 10 Hrs	Implement Network Security to protect from various attacks on networking.(NOS: SSC/N9439)	**Network Security** 401. Practice on firewall technologies to secure the network perimeter. (10 hrs) 402. Practice LAN security considerations and implement endpoint and Layer 2 security features. (10 hrs) 403. Wi-Fi configuration to implement security considerations. (5 hrs)	• Secure AdSSCistrative Access, LAN security considerations. • Network Security Devices. • Cryptography. • Wi-Fi security considerations. (10 hrs.)
Professional Skill 25Hrs; Professional Knowledge 10 Hrs	Perform installation and basic configuration of Windows Servern (NOS: SSC/N9440)	**Server Installation & Basic Configuration** 404. Identify Server Hardware. (5 hrs) 405. Install and configure Windows Server. (5 hrs) 406. Install and Configure Active Directory. (5 hrs) 407. Implementing AD Services. (5 hrs) 408. Configuration of broadband modem and sharing internet connection. (5 hrs)	• Server concepts, Server Hardware, Installation steps, configuration of server. • Concept of Active Directory. ADS Overview, ADS Database, Active Directory Namespace, Logical & Physical Elements of AD. (10 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 50 Hrs; Professional Knowledge 15 Hrs	Demonstrate installation, configuration of DNS, Routing and user account customization. (NOS: SSC/N9441)	**Install & configure DNS** 409. Installing and Configuring DNS Services - Setup Name resolution – Host names, NetBIOS names. - Installing DNS Server. - Configuring DNS Zones, DNS Clients, Delegating Zones. - Testing DNS with nslookup, dnscmd and dnslint. (13hrs) 410. Installing and Configuring DHCP Services - DHCP Server Configuration. - Setting up of DHCP, Routing and remote access. (12hrs)	• Concept of DNS. • Name resolution – Host names, NetBIOS names. • DNS Overview. • DHCP Overview. • DHCP Clients and Leases. (08 hrs.)
		Routing and Remote Access 411. Configuring RRAS. (5 hrs) 412. VPN implementation. (5 hrs) 413. Configuring Remote Access Authentication Protocol. (5 hrs) 414. Configuring RRAS Policies. (2 hrs) 415. Configuring IAS. (3 hrs) 416. Managing TCP/ IP Routing. (5 hrs)	• Remote Access Overview. • VPN Concepts. • Remote Access Authentication Protocol. • RRAS Policies. • IAS. • TCP/ IP Routing. (07 hrs.)
Professional Skill 50 Hrs; Professional Knowledge 10 Hrs	Configure Server and manage Server Network security and Infrastructure. (NOS: SSC/N9442)	**Server Configuration & Backup** 417. Configure a server as web server. (15 hrs) 418. Configuring Mailbox Servers. (5 hrs) 419. Implementing Backup and Recovery. (5 hrs)	• Introduction to Web Server • Introduction to Messaging Services. • Concept of Backup and Recovery of Server. (05 hrs.)
		Maintaining Network Infrastructure 420. Monitor Network Traffic. (5 hrs) 421. Troubleshoot Internet Connectivity. (10 hrs) 422. Troubleshoot Server Services. (5 hrs) 423. Use Linux Network Tools to check/ maintain/ Manage Network. (5 hrs)	• Managing Network Traffic • Types of Problems of Internet Connectivity. • Types and working of Server Services. (05 hrs.)

Duration	Reference Learning Outcome	Professional Skill (Trade Practical) (With inidcative hour)	Professional Knowledge (Trade Theory)
Professional Skill 25Hrs; Professional Knowledge 05 Hrs	Perform installation and basic configuration of Linux server. (NOS: SSC/N9443)	424. Install Linux Server. (5 hrs) 425. Create new user and group. (2 hrs) 426. Create public and data directory. (2 hrs) 427. Create anlmlhosts file. (3 hrs) 428. Check host file. (2 hrs) 429. Secure and run SWAT. (3 hrs) 430. Filter ports. (3 hrs) 431. Telnet installation and configuration. (5 hrs)	• Configuration Plan. • Public and data directory. • Host file. • SWAT. • Password Authentication. • Telnet. (05 hrs.)

Introduction to LINUX Operating System

Objectives: At the end of this lesson you shall be able to
- **overview of LINUX**
- **define the LINUX commands**
- **explain the various shells in LINUX**
- **explain various editors in LINUX.**

LINUX Operating System

Operating System act as an interface between the user and computer hardware. It is a set of programs that controls and coordinates the operations of a computer and helps to make efficient use of its resources. An OS has two regions - Kernel and Shell. Shell provides user interface and kernel provides hardware interface.

LINUX is a UNIX like operating system that runs on many different computer platforms. LINUX is the operating system kernel which comes with a distribution of software. First released in 1991 by Linus Torvalds. LINUX is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or non commercially by one under the license such as GNU/General Public License. It is most widely used free software license, which guaranties end user the freedom to use, study, share and modify the software. LINUX is a multi-user, multiprogramming, time-sharing operating system. It allows several users to share a CPU on time sharing basis. A disadvantage of the LINUX is that, it tends to fail more often since the hardware gets heavier use.

A LINUX OS is described as shell and kernel. The LINUX operating system can be considered as an assembly of three units.

1 Kernel

It is the heart of operating system controlling the hardware of the system and actually doing things as user's request. It allocates memory and disk storage, controls the flow of data between memory and peripheral devices, handles interrupts and error, schedules the running of processes and responds to processors request for services. LINUX kernel is unique and flexible because it is also modular in nature.

2 Shell

Shell is the command interpreter that provides a user interface to the LINUX system. It stands between user and Kernel. The shell tells the Kernel, the work the user has requested. The shell executes commands that are read either from the terminal or of from a file.

3 Tools

Tools are programs for solving different applications

Linux Shells

Shell is an environment in which we can run our commands, programs, and shell scripts. The prompt, $, which is called the command prompt, issued by the shell. Some of the popular shells are:-

- bash (Bourne - Again Shell) - The Bourne - Again Shell , the default shell on most Linux systems. Bash most powerful shell and is a modern implementation of the older Bourne shell (bsh) developed by the GNU project.
- sh (Bourne Shell)- The Bourne Shell, an older shell which is not so widely used anymore
- csh (C shell) - The C shell uses a command language similar to the 'C' programming language.
- tcsh - an improved version of the 'C' shell
- ksh (Korn Shell) – The Korn shell supports everything in the Bourne shell and it has interactive features.
- dash (Debian Almquist Shell) - Debian Almquist Shell, a shell created by the Debian distribution.

Features of LINUX

In addition to the general features of any operating system, LINUX has following special features.

- **Multitasking Capability:** This feature allows the operating system to perform several tasks simultaneously.
- **Multi-user Capability:** LINUX permits several users to use the same computer and carry out different jobs. To achieve this, several terminals referred to as dumb terminals are connected to a single powerful computer called the LINUX server.
- **Portability:** This feature allows programs written under LINUX to run on any brand of computer which used the same operating system.
- **Communication:** Communication between the LINUX server and user terminals.
- **Security:** LINUX provides several levels of security.
- **Hierarchical File system:** It provides standard file structure in which system files/user files are Arranged.

Boot loader

Bootloader is a program that loads an operating system when a computer system is turned ON. It is also called boot manager; is a small program that places the OS of the computer system into memory. For Linux the two most common used boot loaders are LILO (Linux Loader) and GRUB (GRand Unified Bootloader). GRUB is an advanced boot loader that is capable of booting multiple operating systems on a single machine.

Desktop Environment

Desktop environment consist of bundle of components that make up the Graphical User Interface (GUI) such as icons, toolbars, wallpapers and desktop widgets. It includes various applications and collection of system tools for the user. There are several desktop environments and these determine what your LINUX system looks like and how you interact with. The commonly used desktop environments are:-

- GNOME(GNU Network Object Model Environment)
- KDE (K Desktop environment)
- Xfce
- LXDE
- Budgie

LINUX Distributions

LINUX distribution is an operating system that is made up of a collection of softwares based on LINUX kernel or you can say distribution contains the LINUX kernel and supporting libraries and software. Around 600+ LINUX Distributions are available and some of the popular LINUX distributions are:

- Ubuntu
- Red Hat Linux
- Debian
- OpenSUSE
- Solus
- Fedora Core

LINUX file system or directory structure

All operating system have a directory structure or file system in which system files are stored. User files will also be stored in a directory created by the OS itself unless otherwise specified.

In Linux, the file system creates a tree structure. All the files are arranged as a tree and its branches. The topmost directory called the root (/) directory. All other directories in LINUX can be accessed from the root directory.

LINUX file system has a hierarchal file structure as it contains a root directory and its subdirectories. A partition usually has only one file system, but it may have more than one file system. (Fig 1)

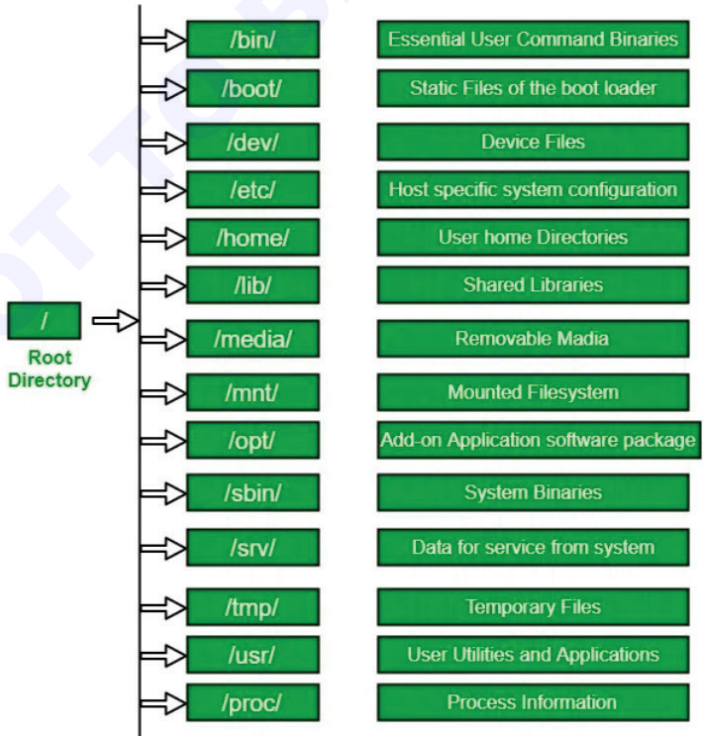
The LINUX file system contains the following sections:

- The root directory (/)
- A specific data storage format (EXT3, EXT4, BTRFS, XFS and so on)
- A partition or logical volume having a particular file system.

LINUX Directories

The LINUX File Hierarchy Structure or the File System Hierarchy Standard (FHS) defines the directory structure and directory contents in LINUX operating systems. In the FHS, all files and directories appear under the root directory /, even if they are stored on different physical or virtual devices.

Fig 1



- **/(root)**

  Every single file and directory starts from the root directory. The only root user has the right to write under this directory. /root is the root user's home directory, which is not the same as /.

- **/bin (binary)**

  It contains binary and executable files. Common LINUX commands used in single-user modes are located under this directory. Commands used by all the users of the system are located here.

  Eg: ls, cp, grep etc.

- **/boot (boot)**

  LINUX boot loader files are stored in /boot directory.

  Eg: kernal

- **/dev (devices)**

  The files representing the hardware devices are stored in /dev.

  Eg: /sda1, /sda2, /usbmon etc.

- **/etc (editable text configuration)**

  It contains configuration files required by all programs. This also contains start up and shutdown shell scripts used to start/stop individual programs.

- **/home**

  Users' home directories, containing saved files, personal settings, etc are stored in /home directory. Eg: /home/ictsm etc.

- **/lib (library)**

  /lib directory stores supporting files for /bin and /sbin.

- **/media**

  Mount points for removable media such as CD-ROMs i.e., /media stores temporary mount directory for removable devices.

  Eg: /media/cdrom for CD-ROM

- **/mnt (mount)**

  All storage media other than LINUX partitions are mounted here. /mnt is a temporary mount directory where system admins can mount file system.

- **/opt(optional)**

  It contains add-on applications from individual vendors. Add-on applications should be installed under either /opt/ or /opt/ subdirectory.

- **/sbin(essential system binaries)**

  Essential system binary files are stored here. Just like /bin, /sbin also contain binary executable. The LINUX commands located under this directory are used typically by system administrator, for system maintenance purpose.

- **/tmp (temporary)**

  It contains temporary files created by system and users. Files under this directory are deleted when system is rebooted.

- **/usr (user)**

  Non critical system files are stored here. Secondary hierarchy for read-only user data; contains the majority of (multi-)user utilities and applications. / usr contains binaries, libraries, documentation, and source-code for second level programs.

- **/proc (process)**

  It contains information about system process. This is a pseudo file system contains information about running process. It contains the real time information about the devices that makeup the personal computer.

Basic LINUX commands

A command is an instruction given by a user to perform a particular task. Commands are generally issued by typing them in at the command line and pressing enter key, which passes them to shell. A Shell is a program that reads commands typed on a keyboard and then executes them. Shells are the most basic method for a user to interact with the system. The default shell on most LINUX systems is bash(Bourne again shell).

Syntax: command options arguments

- An option modifies how the command runs
- An argument specifies data on which the command is to operate

The ls Command

ls : This command creates listing of files and directories in a number of degrees of detail

ls <options> <file or directory>

options	Description
-a	Creates a listing that includes hidden files & directories
-l	Uses a long listing format (with file permissions, owner, size of file etc)

The date command

Purpose : Used to display the current date and time

Eg. : $ date

The clear command

clear: This command clears the screen

Syntax: clear or ctrl+l

The pwd command

The pwd command reports the full path to the current directory. The current directory is the directory in which a user is currently operating while using a command line interface.

Syntax: pwd [option]

Eg. : $ pwd

The History command

This command shows the commands you have entered on your terminal so far:

Eg: $ history

$ history –c : It removes the whole history

The Cat command

Cat command can be used to display the contents of an existing file, creating a new file or append text to an existing file.

To display the content of a file

Syntax: cat [option] <filename>

Eg: cat students.txt

To display the content of multiple files

Syntax : cat [option] <filename><filename>

Eg: $ cat student.txt trainees.txt

To create a file

Syntax: cat > <filename>

Eg: $ cat students.txt

Then type contents and press ctrl+d for saving.

The mkdir command

mkdir: This command is used to create a new directory

Syntax: mkdir <directory>

eg: mkdir test

The cd command

cd: Changes the active(working) directory to the specified directory

Syntax: cd <directory name>

eg: cd test

cd ~ : changes to home directory form any location

cd .. : change to parent or previous directory

The mv command

mv: This command is used to rename or move files and directories

Syntax: mv <old filename> <new filename>

eg: mv abc.txt ras.txt

Syntax: mv <old directory> <new directory>

eg: mv test ictsm

The cp command

cp: This command makes a carbon copy of one file's contents and places those

contents to another file

Syntax: cp <source file> < target>

eg: cp abc.txt tree.txt

Syntax: cp –r <source directory> <target>

Copies a directory and its contents from one location to another

Eg: cp –r LG sony

The rm command

rm : This command is used to remove files and directories

Syntax: rm [options] [-r directories] filenames

rmdir [option] directory names

Eg: rm class.txt

rm –r sony

rmdir LG

The man command

To view the help of a command or manual page

Syntax: man command

eg: man ls

The help command

To view the help documents of a command

Syntax: command --help

eg: ls - -help

The cal command

It displays the calendar of the current month

Syntax: cal

cal month year – displays the calendar of specified month and year

Eg: cal 08 2014 – displays calendar of August 2014

cal year : - Displays the calendar of specified year

eg: cal 2019 – displays calendar of 2019

cal –j year :– displays the calendar of the specified year in Julian format

eg: cal –j 2005

The more command

This command displays whatever you give it as input one screen at a time

Syntax: more <filename> or command |more

eg: cal 2005 |more

The whoami command

The whoami command writes the user name (i.e login name) of the owner of the current login session to standard output. It shows the current logged in terminal username.

Syntax: whoami [option]

The who command

It provides a list of all users currently logged onto the system as well as additional information about each of those users (including login times and terminal numbers)

Syntax: who [option]

The w command

The w shows who is logged on the system and what they are doing.

Syntax: w [options]

The head command

The head command, as the name implies, print the top N number of data of the given input. By default, it prints the first 10 line of the specified files.

Syntax: head filename :- Displays first lines(default 10lines)

Eg : head abc.txt

Syntax: head –n filename: Displays first specified number of lines

Eg : head -5 abc.txt (Displays first 5 lines of abc.txt)

The tail command

The tail command is used to display the last ten lines of one or more files.

Syntax: tail [option] …. <filename>…..

tail filename: Displays last lines(default 10lines)

eg: tail abc.txt

tail –n filename : Displays last number of lines

eg: head -5 abc.txt (Displays last 5 lines of abc.txt)

The tty command

It displays current terminal

Syntax: $ tty

The whatis command

The whatis command provides very brief descriptions of command line programs and other topics related to LINUX and other Unix-like operating systems. It accomplishes this by searching the short descriptions in the whatis database for each keyword provided to it as an argument.

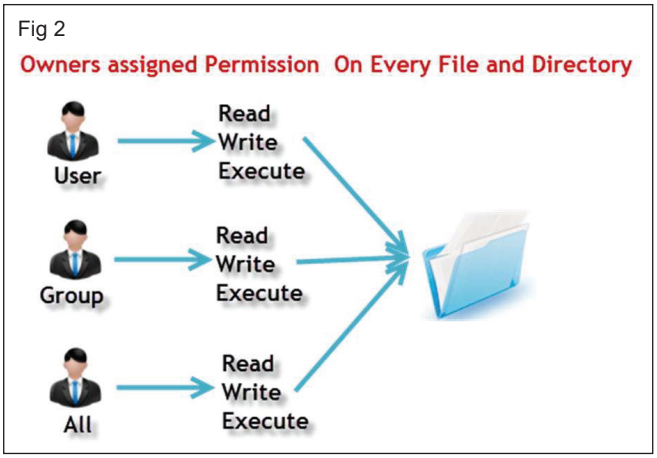
Syntax: whatis keyword(s)

Eg: whatis head

User and File Permission

Users are accounts that can be used to login into a system. Each user is identified by a unique identification number or UID by the system. All the information of users in a system are stored in/etc/passwd file. The hashed passwords for users are stored in /etc/shadow file. (Fig 2)

Fig 2



There are three user types on a LINUX system viz.

i User

ii Group

iii Other

USER

A user is the owner of the file. By default, the person who created a file becomes its owner. Hence, a user is also sometimes called an owner.

GROUP

A user- group can contain multiple users. All users belonging to a group will have the same LINUX group permissions access to the file. Suppose you have a project where a number of people require access to a file.

OTHER

Any other user who has access to a file. This person has neither created the file, nor he belongs to a user group who could own the file. Practically, it means everybody else.

The useradd command

useradd command in LINUX is used to create a new user. Only root or users with sudo privileges can use the useradd command to create a new user accounts.

Syntax: sudo useradd [options] [username]

Eg: sudo useradd ictsm

The passwd command

This command sets password for specified user. passwd command in LINUX is used to change the user account passwords. The root user reserves the privilege to change the password for any user on the system, while a normal user can only change the account password for his account

Syntax: sudo passwd username

Eg: sudo passwd ictsm

The userdel command

userdel command in LINUX system is used to delete a user account and related files.

Syntax: userdel [options] [username]

Eg: userdel ictsm

File Permission

Every file and directory in LINUX system has following 3 permissions defined for all the 3 owners.

Read

This permission gives the authority to open and read a file. Read permission on a directory gives you the ability to lists its content.

Write

The write permission gives the authority to modify the contents of a file. The write permission on a directory gives you the authority to add, remove and rename files stored in the directory.

Execute

The execute permission gives the authority to run a program in LINUX unless otherwise the program is not run.

The chmod command

This command is used to change the access mode or permissions file/directory according to the template mode. We can specify the mode in numbers or by using symbol mode.

Syntax: chmod <mode> <file>

Syntax: chmod –R <mode> <directory>

Representation of different Permissions (Number Mode)

Symbol	Number	Permission	Options
r	4	Read	u(User/Owner)
w	2	Write	g (Group)
x	1	Execute	o (Others)

Eg: chmod 742 abc.txt

Representation of different entities in Symbol mode

Options	Definitions
u	User/Owner
g	Group
o	Others
r	Read
w	Write
x	Execute
+	Add permission
-	Remove permission

Eg: chmod ugo+rwx abc.txt

chmod -R ugo+rwx test

vi editor

The vi editor is a visual editor used for creating and editing text files. It displays the contents of files on the screen and allows a user to add, insert, delete or changes the text. Vi or the Visual Editor is the default text editor that comes with most LINUX systems. The VI editor is the most popular and classic terminal-based text editor in the LINUX family. Below, are some reasons which make it a widely used editor-

i It is available in almost all LINUX Distributions

ii It works the same across different platforms and Distributions

iii It is user-friendly.

Nowadays, there are advanced versions of the vi editor available, and the most popular one is VIM which is vi Improved. Vi editor runs in two modes; the Command mode and the Insert mode.

Syntax: vi <filename>

eg: vi abc.txt

In insert mode we can add contents to file. To enter into insert mode press" I" and make changes. To return to command mode press "esc" and do the following command mode operations.

Command mode operations:

:w (save)

:wq (save and quit)

:q (quit)

:q! (quit without save)

Pine Editor

Pine is a program for accessing email and newsgroups. It is a screen-oriented handling tool.

Syntax: pine [options] [address,address]

Pico editor

Pico is a simple text editor in the style of the pine composer

Joe editor

It is a simple text editor like vi, to create and edit non-formatted text and more user friendly.

X WINDOW System

The X Window System (X11, or simply X) provides the basic framework for the graphical user interface on Linux. It allows to run applications within windows. It also allows moving windows around on the screen as well as clicking on items with mouse.

Filter Commands

Filters are programs that take plain text (either stored in a file or produced by another program) as standard input, transform it into a meaningful format, and then return it as standard output. LINUX has a number of filters.

Eg : cat, head, tail, grep

The grep command

The grep command searches a file for a particular pattern of characters, and displays all lines that contain that pattern. The pattern that is searched in the file is referred to as the regular expression (grep stands for Global Regular Expression Printer).

Syntax: grep [option]…. Pattern [files]…

Options: –i (ignores case for matching)

–c (prints only a count of the lines matches a pattern)

Eg: grep “sa” class.txt

Additional Commands

The touch command

The touch command updates the access and modification times of each file to the current system time. If you specify a file that does not already exist, touch creates an empty file with that name.

$ touch filename

The uname command

Uname is a command-line utility that prints basic information about the operating system name and system hardware

Syntax: uname [option]

Eg:

uname -s : It print kernel name

uname -v : It print version

uname -m :It prints machine hardware name

uname -r : It print kernel release

The Sort command

This command sorts the contents of the file either alphabetically or numerically, in forward or reverse order.

Syntax : sort <options> <filename>

- r – Sorts the file contents in descending order.

- n – Sorts the file according to character in column ‘n’.

Eg: sort class.txt

sort –r class.txt

The wc command

The wc(word count) command by default counts the number of lines, words and characters in text.

Syntax: wc filename

Eg: wc class.txt

The fdisk command

The fdisk is the tool for getting partition information, adding and removing partitions. The fdisk tool requires super user privileges.

$ fdisk –l : list all the partitions of the hard drive.

The Netstat command

netstat is the command used to check the network statistics of the system. It will list the current network connections, routing table information, interface statistics etc

Eg : $ netstat

The apt-get command

The apt-get utility is a powerful and free package management command line program that is used to work with Ubuntu’s APT (Advanced Packaging Tool) library to perform installation of new software packages, removing existing software packages, upgrading of existing software packages and even used to upgrading the entire operating system.

Syntax: apt-get install package name

Eg: apt-get install netcat

The du command

du command determines the disk usage of a file. If the argument given to it is a directory, then it will list disk usage of all the files and directories recursively under that directory

Syntax : du file name or Directory name

Eg:$ du /etc/passwd

The df command

df reports file system usage.

Eg: $df

Process

An instance of a running program is called a process. Every time you run a shell command, a program is run and a process is created for it. Each process in LINUX has a process id (PID) and it is associated with a particular user and group account.

Shell Scripting

A shell script is a computer program designed to be run by the Unix/LINUX shell. Typical operations performed by shell scripts include file manipulation, program execution and printing text. (Fig 3)

#!/bin/bash

Add two numeric value

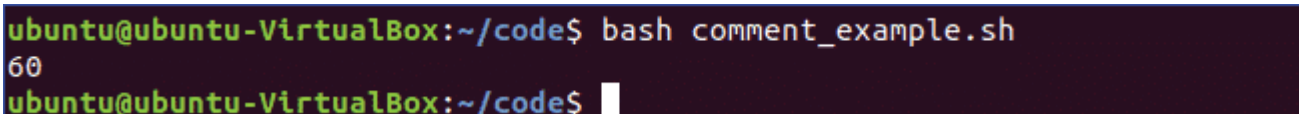
((sum=25+35))

#Print the result

echo $sum

Run the file with bash command.

Fig 3



Command		Description
•	apropos whatis	Show commands pertinent to string. See also threadsafe
•	man -t ascii | ps2pdf - > ascii.pdf	make a pdf of a manual page
	which command	Show full path name of command
	time command	See how long a command takes
•	time cat	Start stopwatch. Ctrl-d to stop. See also sw
dir navigation		
•	cd -	Go to previous directory
•	cd	Go to $HOME directory
	(cd dir && command)	Go to dir, execute command and return to current dir
•	pushd **.**	Put current dir on stack so you can **popd** back to it
file searching		
•	alias l='ls -l --color=auto'	quick dir listing. See also l
•	ls -lrt	List files by date. See also newest and find_mm_yyyy
•	ls /usr/bin | pr -T9 -W$COLUMNS	Print in 9 columns to width of terminal
	find -name '*.[ch]' | xargs grep -E 'expr'	Search 'expr' in this dir and below. See also findrepo
	find -type f -print0 | xargs -r0 grep -F 'example'	Search all regular files for 'example' in this dir and below
	find -maxdepth 1 -type f | xargs grep -F 'example'	Search all regular files for 'example' in this dir
	find -maxdepth 1 -type d | while read dir; do echo $dir; echo cmd2; done	Process each item with multiple commands (in while loop)
•	find -type f ! -perm -444	Find files not readable by all (useful for web site)
•	find -type d ! -perm -111	Find dirs not accessible by all (useful for web site)
•	locate -r 'file[^/]*\.txt'	Search cached index for names. This re is like glob *file*.txt
•	look reference	Quickly search (sorted) dictionary for prefix
•	grep --color reference /usr/share/dict/words	Highlight occurances of regular expression in dictionary
archives and compression		
	gpg -c file	Encrypt file
	gpg file.gpg	Decrypt file
	tar -c dir/ | bzip2 > dir.tar.bz2	Make compressed archive of dir/
	bzip2 -dc dir.tar.bz2 | tar -x	Extract archive (use gzip instead of bzip2 for tar.gz files)
	tar -c dir/ | gzip | gpg -c | ssh user@remote 'dd of=dir.tar.gz.gpg'	Make encrypted archive of dir/ on remote machine

	find dir/ -name '*.txt' | xargs cp -a --target-directory=dir_txt/ --parents	Make copy of subset of dir/ and below
	(tar -c /dir/to/copy) | (cd /where/to/ && tar -x -p)	Copy (with permissions) copy/ dir to /where/to/ dir
	(cd /dir/to/copy && tar -c **.**) | (cd /where/to/ && tar -x -p)	Copy (with permissions) contents of copy/ dir to /where/to/
	(tar -c /dir/to/copy) | ssh -C user@remote 'cd /where/to/ && tar -x -p'	Copy (with permissions) copy/ dir to remote:/where/to/ dir
	dd bs=1M if=/dev/sda | gzip | ssh user@remote 'dd of=sda.gz'	Backup harddisk to remote machine
rsync (Network efficient file copier: Use the --dry-run option for testing)		
	rsync -P rsync://rsync.server.com/path/to/file file	Only get diffs. Do multiple times for troublesome downloads
	rsync --bwlimit=1000 fromfile tofile	Locally copy with rate limit. It's like nice for I/O
	rsync -az -e ssh --delete ~/public_html/ remote.com:'~/public_html'	Mirror web site (using compression and encryption)
	rsync -auz -e ssh remote:/dir/ **.** && rsync -auz -e ssh **.** remote:/dir/	Synchronize current directory with remote one
ssh (Secure SHell)		
	ssh $USER@$HOST command	Run command on $HOST as $USER (default command=shell)
•	ssh -f -Y $USER@$HOSTNAME xeyes	Run GUI command on $HOSTNAME as $USER
	scp -p -r $USER@$HOST: file dir/	Copy with permissions to $USER's home directory on $HOST
	scp -c arcfour $USER@$LANHOST: bigfile	Use faster crypto for local LAN. This might saturate GigE
	ssh -g -L 8080:localhost:80 root@$HOST	Forward connections to $HOSTNAME:8080 out to $HOST:80
	ssh -R 1434:imap:143 root@$HOST	Forward connections from $HOST:1434 in to imap:143
	ssh-copy-id $USER@$HOST	Install public key for $USER@$HOST for password-less log in
networking (Note ifconfig, route, mii-tool, nslookup commands are obsolete)		
	ethtool eth0	Show status of ethernet interface eth0
	ethtool --change eth0 autoneg off speed 100 duplex full	Manually set ethernet interface speed
	iw dev wlan0 link	Show link status of wireless interface wlan0
	iw dev wlan0 set bitrates legacy-2.4 1	Manually set wireless interface speed
•	iw dev wlan0 scan	List wireless networks in range
•	ip link show	List network interfaces
	ip link set dev eth0 name wan	Rename interface eth0 to wan
	ip link set dev eth0 up	Bring interface eth0 up (or down)
•	ip addr show	List addresses for interfaces

	ip addr add 1.2.3.4/24 brd + dev eth0	Add (or del) ip and mask (255.255.255.0)
•	ip route show	List routing table
	ip route add default via 1.2.3.254	Set default gateway to 1.2.3.254
•	ss -tupl	List internet services on a system
•	ss -tup	List active connections to/from system
•	host pixelbeat.org	Lookup DNS ip address for name or vice versa
•	hostname -i	Lookup local ip address (equivalent to host `hostname`)
•	whois pixelbeat.org	Lookup whois info for hostname or ip address
windows networking (Note samba is the package that provides all this windows specific networking support)		
•	smbtree	Find windows machines. See also findsmb
	nmblookup -A 1.2.3.4	Find the windows (netbios) name associated with ip address
	smbclient -L windows_box	List shares on windows machine or samba server
	mount -t smbfs -o fmask=666,guest //windows_box/share /mnt/share	Mount a windows share
	echo 'message' | smbclient -M windows_box	Send popup to windows machine (off by default in XP sp2)
text manipulation (Note sed uses stdin and stdout. Newer versions support inplace editing with the -i option)		
	sed 's/string1/string2/g'	Replace string1 with string2
	sed 's/\(.*\)1/\12/g'	Modify anystring1 to anystring2
	sed '/^ *#/d; /^ *$/d'	Remove comments and blank lines
	sed ':a; /\\$/N; s/\\\n//; ta'	Concatenate lines with trailing \
	sed 's/[\t]*$//'	Remove trailing spaces from lines
	sed 's/\([`"$\]\)/\\\1/g'	Escape shell metacharacters active within double quotes
•	seq 10 | sed "s/^/ /; s/ *\(.\{7,\}\)/\1/"	Right align numbers
•	seq 10 | sed p | paste - -	Duplicate a column
	sed -n '1000{p;q}'	Print 1000th line
	sed -n '10,20p;20q'	Print lines 10 to 20
	sed -n 's/.*<title>\(.*\)<\/title>.*/\1/ip;T;q'	Extract title from HTML web page
	sed -i 42d ~/.ssh/known_hosts	Delete a particular line
	sort -t. -k1,1n -k2,2n -k3,3n -k4,4n	Sort IPV4 ip addresses
•	echo 'Test' | tr '[:lower:]' '[:upper:]'	Case conversion
•	tr -dc '[:print:]' < /dev/urandom	Filter non printable characters
•	tr -s '[:blank:]' '\t' </proc/diskstats | cut -f4	cut fields separated by blanks
•	history | wc -l	Count lines
•	seq 10 | paste -s -d ' '	Concatenate and separate line items to a

set operations (Note you can export LANG=C for speed. Also these assume no duplicate lines within a file)		
	sort file1 file2 | uniq	Union of unsorted files
	sort file1 file2 | uniq -d	Intersection of unsorted files
	sort file1 file1 file2 | uniq -u	Difference of unsorted files
	sort file1 file2 | uniq -u	Symmetric Difference of unsorted files
	join -t'\0' -a1 -a2 file1 file2	Union of sorted files
	join -t'\0' file1 file2	Intersection of sorted files
	join -t'\0' -v2 file1 file2	Difference of sorted files
	join -t'\0' -v1 -v2 file1 file2	Symmetric Difference of sorted files
math		
•	echo '(1 + sqrt(5))/2' | bc -l	Quick math (Calculate φ). See also bc
•	seq -f '4/%g' 1 2 99999 | paste -sd-+ | bc -l	Calculate π the unix way
•	echo 'pad=20; min=64; (100*10^6)/((pad+min)*8)' | bc	More complex (int) e.g. This shows max FastE packet rate
•	echo 'pad=20; min=64; print (100E6)/((pad+min)*8)' | python	Python handles scientific notation
•	echo 'pad=20; plot [64:1518] (100*10**6)/((pad+x)*8)' | gnuplot -persist	Plot FastE packet rate vs packet size
•	echo 'obase=16; ibase=10; 64206' | bc	Base conversion (decimal to hexadecimal)
•	echo $((0x2dec))	Base conversion (hex to dec) ((shell arithmetic expansion))
•	units -t '100m/9.58s' 'miles/hour'	Unit conversion (metric to imperial)
•	units -t '500GB' 'GiB'	Unit conversion (SI to IEC prefixes)
•	units -t '1 googol'	Definition lookup
•	seq 100 | paste -s -d+ | bc	Add a column of numbers. See also add and funcpy
calendar		
•	cal -3	Display a calendar
•	cal 9 1752	Display a calendar for a particular month year
•	date -d fri	What date is it this friday. See also day
•	[$(date -d '12:00 today +1 day' +%d) = '01'] || exit	exit a script unless it's the last day of the month
•	date --date='25 Dec' +%A	What day does xmas fall on, this year
•	date --date='@2147483647'	Convert seconds since the epoch (1970-01-01 UTC) to date
•	TZ='America/Los_Angeles' date	What time is it on west coast of US (use tzselect to find TZ)
•	date --date='TZ="America/Los_Angeles" 09:00 next Fri'	What's the local time for 9AM next Friday on west coast US
locales		
•	printf "%'d\n" 1234	Print number with thousands grouping appropriate to locale

•	BLOCK_SIZE=\'1 ls -l	Use locale thousands grouping in ls. See also l
•	echo "I live in `locale territory`"	Extract info from locale database
•	LANG=en_IE.utf8 locale int_prefix	Lookup locale info for specific country. See also ccodes
•	locale -kc $(locale | sed -n 's/\(LC_.\{4,\}\)=.*/\1/p') | less	List fields available in locale database
recode (Obsoletes iconv, dos2unix, unix2dos)		
•	recode -l | less	Show available conversions (aliases on each line)
	recode windows-1252.. file_to_change.txt	Windows "ansi" to local charset (auto does CRLF conversion)
	recode utf-8/CRLF.. file_to_change.txt	Windows utf8 to local charset
	recode iso-8859-15..utf8 file_to_change.txt	Latin9 (western europe) to utf8
	recode ../b64 < file.txt > file.b64	Base64 encode
	recode /qp.. < file.qp > file.txt	Quoted printable decode
	recode ..HTML < file.txt > file.html	Text to HTML
•	recode -lf windows-1252 | grep euro	Lookup table of characters
•	echo -n 0x80 | recode latin-9/x1..dump	Show what a code represents in latin-9 charmap
•	echo -n 0x20AC | recode ucs-2/x2..latin-9/x	Show latin-9 encoding
•	echo -n 0x20AC | recode ucs-2/x2..utf-8/x	Show utf-8 encoding
CDs		
	gzip < /dev/cdrom > cdrom.iso.gz	Save copy of data cdrom
	mkisofs -V LABEL -r dir | gzip > cdrom.iso.gz	Create cdrom image from contents of dir
	mount -o loop cdrom.iso /mnt/dir	Mount the cdrom image at /mnt/dir (read only)
	wodim dev=/dev/cdrom blank=fast	Clear a CDRW
	gzip -dc cdrom.iso.gz | wodim -tao dev=/dev/cdrom -v -data -	Burn cdrom image (use --prcap to confirm dev)
	cdparanoia -B	Rip audio tracks from CD to wav files in current dir
	wodim -v dev=/dev/cdrom -audio -pad *.wav	Make audio CD from all wavs in current dir (see also cdrdao)
	oggenc --tracknum=$track track.cdda.wav -o track.ogg	Make ogg file from wav file
disk space		
•	ls -lSr	Show files by size, biggest last
•	du -s * | sort -k1,1rn | head	Show top disk users in current dir. See also dutop
•	du -hs /home/* | sort -k1,1h	Sort paths by easy to interpret disk usage
•	df -h	Show free space on mounted filesystems
•	df -i	Show free inodes on mounted filesystems
•	fdisk -l	Show disks partitions sizes and types (run as root)

•	rpm -q -a --qf '%10{SIZE}\t%{NAME}\n' | sort -k1,1n	List all packages by installed size (Bytes) on rpm distros
•	dpkg-query -W -f='${Installed-Size;10}\t${Package}\n' | sort -k1,1n	List all packages by installed size (KBytes) on deb distros
•	dd bs=1 seek=2TB if=/dev/null of=ext3.test	Create a large test file (taking no space). See also truncate
•	> file	truncate data of file or create an empty file
monitoring/debugging		
•	tail -f /var/log/messages	Monitor messages in a log file
•	strace -c ls >/dev/null	Summarise/profile system calls made by command
•	strace -f -e open ls >/dev/null	List system calls made by command
•	strace -f -e trace=write -e write=1,2 ls >/dev/null	Monitor what's written to stdout and stderr
•	ltrace -f -e getenv ls >/dev/null	List library calls made by command
•	lsof -p $$	List paths that process id has open
•	lsof ~	List processes that have specified path open
•	tcpdump not port 22	Show network traffic except ssh. See also tcpdump_not_me
•	ps -e -o pid,args --forest	List processes in a hierarchy
•	ps -e -o pcpu,cpu,nice,state,cputime,args --sort pcpu | sed '/^ 0.0 /d'	List processes by % cpu usage
•	ps -e -orss=,args= | sort -b -k1,1n | pr -TW$COLUMNS	List processes by mem (KB) usage. See also ps_mem.py
•	ps -C firefox-bin -L -o pid,tid,pcpu,state	List all threads for a particular process
•	ps -p 1,$$ -o etime=	List elapsed wall time for particular process IDs
•	watch -n.1 pstree -Uacp $$	Display a changing process subtree
•	last reboot	Show system reboot history
•	free -m	Show amount of (remaining) RAM (-m displays in MB)
•	watch -n.1 'cat /proc/interrupts'	Watch changeable data continuously
•	udevadm monitor	Monitor udev events to help configure rules
system information		
•	uname -a	Show kernel version and system architecture
•	head -n1 /etc/issue	Show name and version of distribution
•	cat /proc/partitions	Show all partitions registered on the system
•	grep MemTotal /proc/meminfo	Show RAM total seen by the system
•	grep "model name" /proc/cpuinfo	Show CPU(s) info
•	lspci -tv	Show PCI info

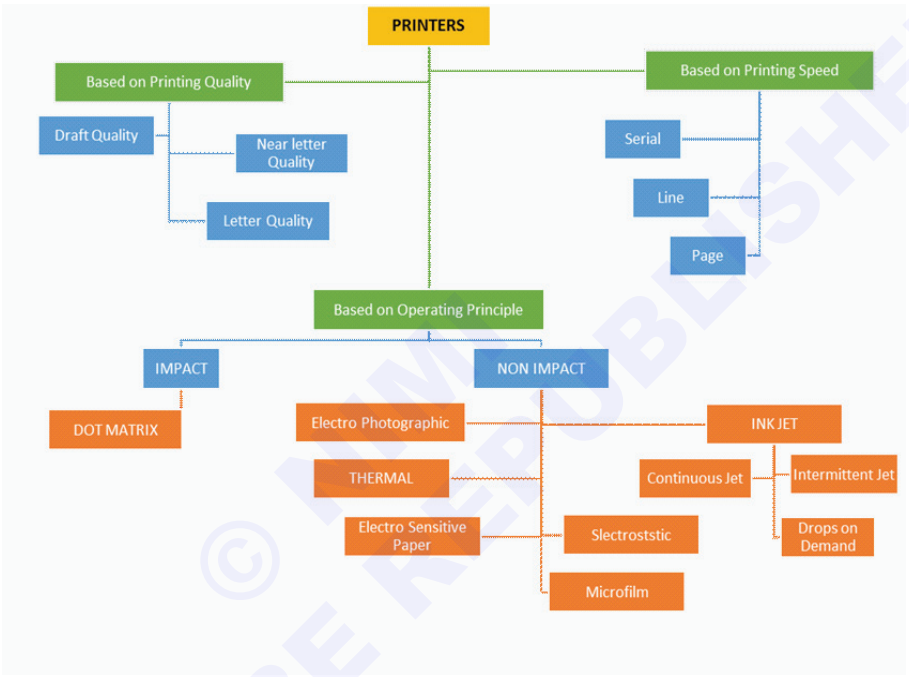
•	lsusb -tv	Show USB info
•	mount | column -t	List mounted filesystems on the system (and align output)
•	grep -F capacity: /proc/acpi/battery/BAT0/info	Show state of cells in laptop battery
#	dmidecode -q | less	Display SMBIOS/DMI information
#	smartctl -A /dev/sda | grep Power_On_Hours	How long has this disk (system) been powered on in total
#	hdparm -i /dev/sda	Show info about disk sda
#	hdparm -tT /dev/sda	Do a read speed test on disk sda
#	badblocks -s /dev/sda	Test for unreadable blocks on disk sda
interactive		
•	readline	Line editor used by bash, python, bc, gnuplot, ...
•	screen	Virtual terminals with detach capability, ...
•	mc	Powerful file manager that can browse rpm, tar, ftp, ssh, ...
•	gnuplot	Interactive/scriptable graphing
•	links	Web browser
•	xdg-open **.**	open a file or url with the registered desktop application

Printers - Classification

Objectives: At the end of this lesson you shall be able to
- **define printer**
- **types of printers**
- **explain the characteristics of printer**
- **working principle of printers.**

A printer is an electromechanical device which converts the text and graphical documents from electronic form to the physical form. A wide range of printers are available with a variety of features ranging from printing black and white text documents to high quality colour graphic images. Printers are categorized as follows (Fig 1)

Fig 1



Dot matrix printer: (Fig 2)

Fig 2

Dot matrix printing or impact matrix printing is a type of computer printing which uses a print head that moves back and forth, or in an up and down motion, on the page and prints by striking an ink-soaked cloth ribbon against the paper.

Each dot is produced by a tiny metal rod, also called a “wire” or “pin”, which is driven forward by the power of a tiny electromagnet or solenoid, either directly or through small levers. Facing the ribbon and the paper is a small guide plate pierced with holes to serve as guides for the pins. The portion of the printer containing the pins is called the print head. It generally prints one line of text at a time.

Serial dot matrix printers use a horizontally moving print head. The print head is a single vertical column of seven or more pins approximately the height of a character box. The pins are arranged in up to four vertically or/ and horizontally slightly displaced columns in order to increase the dot density and print speed through interleaving without causing the pins to jam. Thereby, up to 48 pins can be used to form the characters of a

line while the print head moves horizontally. The printing speed of serial dot matrix printers with moving heads varies from 50 to 550 cps.

Line dot matrix printers uses a fixed print head almost as wide as the paper path utilizing a horizontal line of thousands of pins for printing. Sometimes two horizontally slightly displaced rows are used to improve the effective dot density through interleaving. These printers are used for the professional heavy-duty high speed printing. It prints a whole line at once while the paper moves forward below the print head. Line matrix printers are capable of printing much more than 1000 cps, resulting in a throughput of up to 800 pages/hour.

Because the printing involves mechanical pressure, both of these types of printers can create carbon copies and carbonless copies. These machines are highly durable.

Ink-jet printer (Fig 3)

Fig 3

Ink jet printers form images and characters by spraying fine drops of ink on the paper. Ink-jet printers produce high-quality text and graphics. The most common type of inkjet printer is the drop-on -demand print head. Drop-on-demand printing means that ink is ejected out of the nozzles as needed. Characters are formed by spraying the ink in a series of dots, similar to the dot matrix printer.

At the output of each nozzle is a small piezoelectric crystal that vibrates when an electric signal is applied to it. The piezoelectric crystals act as small pumps to squeeze the ink out. When a dot is needed, the control circuits send a driver signal to the crystal, which causes it to vibrate, squeezing the nozzle tube and forcing a drop of ink on to the paper. Some ink jet printers use the bubble jet printing process. In this process, the piezoelectric crystals are replaced with small heaters. When a drop of ink is needed, a pulse applied to the heaters causes an air bubble to form in the ink nozzle. This rapidly expanding air bubble forces a drop of ink out of the nozzle and on to the paper. When the drive pulse is removed, the heaters cool almost instantly, creating a vacuum in the nozzle, which draws more ink from the reservoir. Ink jet printers produce letter quality print. They are quiet, fast, and flexible. Some colour printer manufacturers prefer the inkjet method for printing. To print colour, three print heads are activated simultaneously. The amount of each primary colour sprayed on the paper combines with the others to form all the colours of the spectrum.

Laser printer (Fig 4)

Fig 4

Uses the same technology as copy machines. A laser printer is mainly made up of an electrostatically charge photosensitive drum that attracts the ink in order to make a shape that will be deposited on the sheet of paper.

A primary charge roller gives the sheets of paper a positive charge. The laser gives a positive charge to certain spots on the drum with a pivoting mirror. Then, negatively charged ink in powder form (toner) is deposited on the parts of the drum that were previously charged by the laser.

By turning, the drum deposits the ink on the paper. A fusing mechanism finally attaches the ink to the paper. Laser printers produce very high quality text and graphics.

Printer characteristics:

Quality of type: The output produced by printers is said to be either letter quality (as good as a typewriter), near letter quality, or draft quality. Only daisy-wheel, ink-jet, and laser printers produce letter-quality type. Some dot-matrix printers claim letter-quality print, but if you look closely, you can see the difference.

Print speed: The speed of the printer is expressed in characters per second (cps) or pages per minute (ppm). Print speed generally represents the printer's ability to print a large number of pages per minute. Daisy-wheel printers tend to be the slowest, printing about 30 cps. Line printers are fastest up to 3,000 lines per minute. Dot-matrix printers can print up to 500 cps, and laser printers range from about 4 to 20 text pages per minute.

Graphics: Some printers such as daisy-wheel and line printers can print only text. Other printers can print both text and graphics.

Resolution: Expressed in dots per inch resolution means the sharpness of printed text. More dots per square inch the printer is able to produce results in a better quality of printed output. A laser printer is capable of printing 600 by 600 DPI or 360000 dots per square inch. Sometimes

the resolution is different for a monochrome, colour or photo print-out.

Fonts: Some printers, notably dot-matrix printers, are limited to one or a few fonts. In contrast, laser and ink-jet printers are capable of printing an almost unlimited variety of fonts. Daisy-wheel printers can also print different fonts, but you need to change the daisy wheel, making it difficult to mix fonts in the same document.

Printable area: Different printers have different printable areas. The printable area also depends on the paper size and the degree of rotation specified for the page layout or overlay used.

On board memory: Printer memory is used to store print jobs while the computer continues to work. A large buffer or memory in a printer allows you to continue your work without having to wait for something to print. Some printers also contain memory hardware. The higher the amount of memory, the longer the printer queue can be.

Warm-up time: It is the waiting time necessary before the first print-out. A printer cannot print when it is “cold”. A certain temperature must be reached for the printer to run optimally.

Paper format: It is the size of paper the printer can handle. Printers are able to accept different sized documents, generally in A4 format (21 x 29.7 cm) or less frequently A3 (29.7 x 42 cm). Some printers allow you to print on other types of media, such as CDs or DVDs.

Paper feed: It is the method of loading paper into the printer, characterising the way in which blank paper is stored.

Cartridges: Cartridges are of different types such as Ribbon cartridge, Toner cartridge and Ink cartridges.

Printing cost: It is interesting to examine the printing cost per sheet. The size of the ink drop is especially important. The smaller the drop of ink, the lower the printing cost will be and the better the image quality will be. Some printers produce drops that are 1 or 2 Pico litres.

Interface: how the printer is connected to the computer. The main interfaces are:

RS-232 Serial Interface

Centronics Parallel Interface

USB Interface

Network: This type of interface allows several computers to share one printer. There are also Wi-Fi printers that are available through a wireless network.

Control panel in printers

Every printer has a control panel some where on its body. Some printers have LCD control panels with touch screens that display text, or preview and select photos for printing, whereas others have control panels with buttons. If the printer does not have a control panel, then it is controlled through a software control panel in the OS. Definitions for some of the control panel buttons are given below. All-in-one printers have additional buttons on the control panel.

On-Line or Select: The purpose of On-Line or Select is to tell the printer whether to ignore the computer. When the printer is offline or the button is deselected, the computer cannot print.

When the printer is offline the printer is still on, which helps to do things that cannot be done when the printer is printing.

Form Feed: The Form Feed button ejects a page of paper from the printer. Form Feed button is used to eject the rest of that page or can be used to spit a blank page.

Line Feed: A line feed advances the paper one line. Some printers have a button labelled LF that executes a line feed when pressed, however, the printer must be in off-line mode to execute a line feed.

Pause: Pause button is used to temporarily stop the printing.

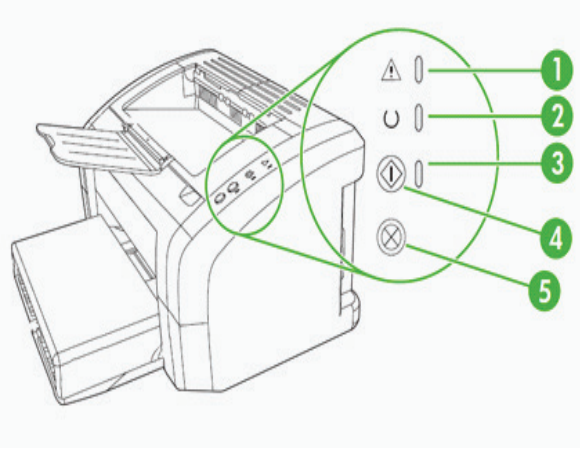
Font: This button is used to select one of the fonts available in the printer.

Tear Off: Press this button to move continuous paper to the tear-off position. Press it again to move the next page to the top-of-form position.

Condensed: Press this button to print condensed characters. Press it again to return to normal character printing.

Front panel controls of laser printer (Fig 5)

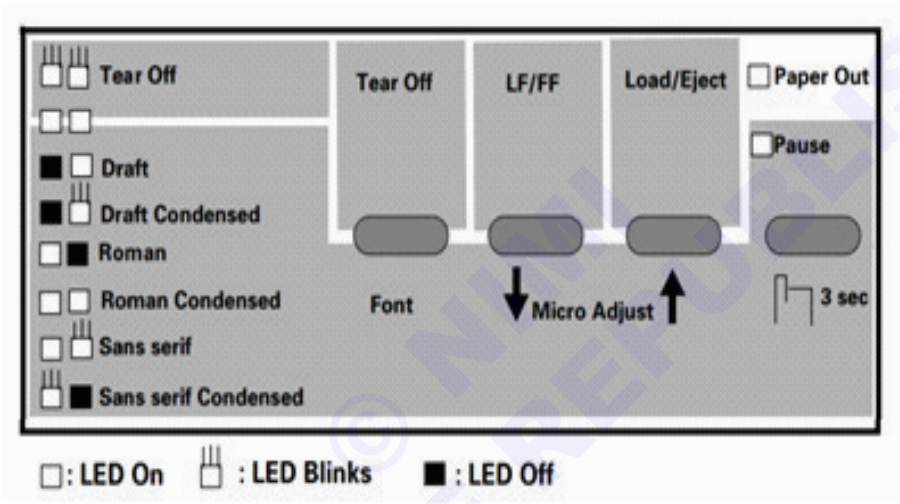
Fig 5



Marker	Switch / Indicator	Function
1	ATTENTION light	Indicates that the print-cartridge door is open, print cartridge is missing, or other errors.
2	READY Light	Indicates that the printer is ready to print.
3	GO light	To print a demo page, or to continue printing while in manual-feed mode, press and release the GO button.
4	GO button	To print a configuration page, press and hold the GO button for between 5 and 10 seconds, until the ATTENTION and READY lights flash. To run a cycle to clean the paper path by using a transparency, press and hold the GO button for at least 10 seconds until the ATTENTION and READY lights the remain on.
5	CANCEL JOB button	When the printer is processing data, press the CANCEL JOB button to cancel the print job.

Front panel controls of Inkjet printer (Fig 6)

Fig 6



Function of switches in the front panel

Switch	Function
Pause	• Alternates printing and non-printing status. • Enables Micro Adjustment function and Font selection, holding it down for 3 seconds.
Load/Eject	• Loads or ejects paper. • Executes micro feed forward, when this function is enabled.
LF/FF	• Executes line feed, pressing it shortly. • Executes form feed, holding it down for a few seconds. • Executes micro feed backward, when this function is enabled.
Tear Off	• Advances continuous paper to the Tear-off position. • Select font, when this function is enabled.

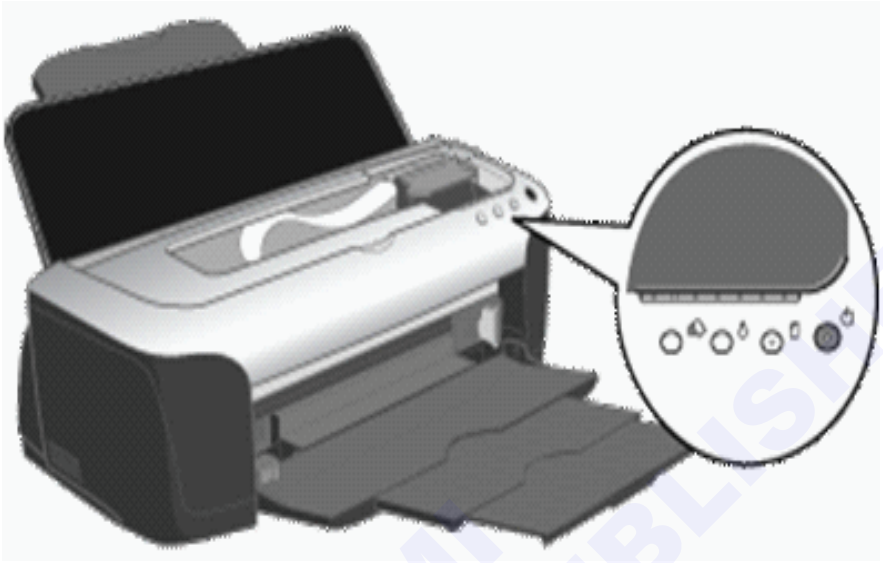
Operation at power On

Load/Eject	NLQ self-test.
LF/FF	Draft self-test.
Tear Off	Default setting.

Load/Eject & LF/FF	Data dump.
Load/Eject & LF/FF & Pause	Clear EEPROM.
Tear Off & Load/Eject & LF/FF	Clear EEPROM for Diving Line count for ribbon change timing.
Pause	Bi-d adjustment.

Front panel controls of Inkjet printer (Fig 7)

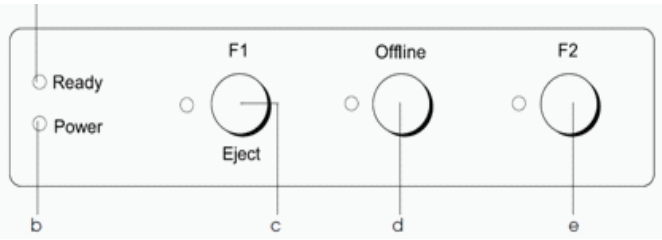
Fig 7



Front panel controls of pass book printer (Fig 8)

Switch	Function
Power	• Turns the printer on and off. • Clears the printer's memory if pressed twice while the power is on. • To turn off the printer, hold down the power button until the light goes out.
Paper	• Loads or ejects paper. • Resumes printing if pressed after a paper out error or double feed error.
Ink	• Moves the print head to the ink cartridge replacement position. • Returns the print head to its home position after ink cartridge replacement. • Performs print head cleaning if held down for three seconds when the ink out light is off.

Fig 8



Marker	Switch / Indicator	Function
a	Ready Light Yellow	• ON when the printer is ready to receive or already receiving data. • Flashes when a Error has occurred during printing process.
b	Power Light Green	• ON for a few seconds when the Printer is turned ON. • ON when the Printer is paused.
c	F1 / Eject Button	• Executes functions which are assigned to the F1 / Eject when the Printer is in the PR2 Mode. • Ejects paper when the Printer is in Esc / P or IBM PPDS(Personal Printer Data Stream) Mode.
d	Offline Button	• Alternates Printer activity between online and offline. • In default settings mode this button is used to select menu.
e	F2 Button	• Executes functions which are assigned to the F2 button when the printer is in PR2 Mode.

Printer Ports

Ports

It's important to use the best printer port possible when setting up a printer, especially if you use your printer heavily. Each printer port delivers different speeds, and your computer may only be able to use certain ports. Also, some ports enable faster printer setup and recognition. Ideally, you want the fastest speed possible for your printer.

Software Ports

Software ports are ports on a computer that act as the middleman between the computer and an external device. They act as keys that printers use to interact with computers. There are 65,535 different ports a computer can use, and of that amount the most common printing ports are 9100 and 6001. Other ports can be used as well, depending on the hardware, manufacturer and whether or not ports are already in use.

Hardware Printer Port Types

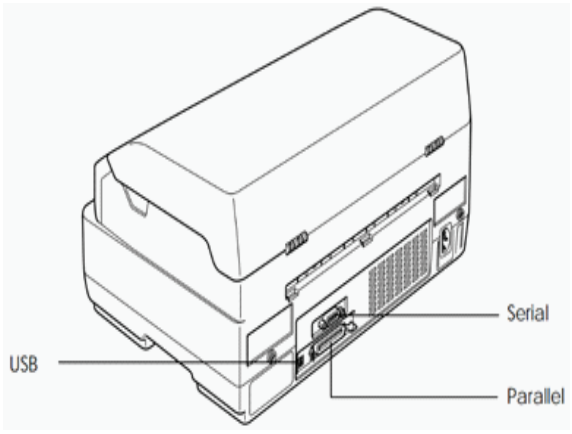
Many computers come with a parallel printing port, also known as an LPT1 port. The parallel port is a 36-pin port that older printers use to connect to computers, but the connection is quite slow at 2 megabits per second. Serial ports have nine pins in them and also work with printers but run at a much slower 115 kilobits per second. More modern printers typically connect to a PC using a USB port, typically located in the back of the computer. For small business users, USB connections are the fastest connections for a computer and printer, providing data transfer rates of up to 4.8 gigabits per second. (Fig 9)

The USB Ports Don't Detect the Printer after an Install Considerations most computers come with one parallel or LPT1 port because that's the maximum most motherboards can take. The same goes for serial connections. This limits the number of printers you can connect to one computer. Parallel and serial connections are usually not hot-swappable, meaning they won't work unless you shut down the computer to plug them in, which could add downtime to your business. However, you can plug in a USB device while the computer is on and Windows will recognize it. There are usually six to eight USB ports on a computer, and with USB hubs, up to 128 different printers or other devices can be hooked up to one computer. While it may be impractical to hook up 128 printers, you can still use any USB device while your printer is connected.

Wireless Connections

Modern printers include a Wi-Fi feature that enables them link to computers via a wireless network. They must still use the same software ports as if they were directly connected to a PC, but they can be placed almost anywhere within the radius of a wireless router. This also enables you to print from a laptop with Wi-Fi or an iPad, if the printer is compatible with Air Print. Note that many Wi-Fi printers still require a physical connection to the computer while the drivers are being installed.

Fig 9



Types of printer ports

1 **Serial (RS-232):** Serial ports are another legacy port, rarely used for printers except in certain niche applications. Cables, connectors, and required wiring vary widely. Several communication parameters must be known to communicate with a serial printer. The most important are baud rate and parity. Values vary, but typical serial printers often use a baud rate of 9600 and no parity.

2 **DB-25 parallel port:** There are three different types of parallel ports found in PCs.

Unidirectional - The unidirectional port is the original port found on PCs.

Bidirectional - The bi-directional port offers data transfer in both directions on the same lines.

Fast Parallel - The fast parallel port not only offers Bidirectional data transfer but also runs at a much faster data rate.

The bidirectional port offers data transfer in both directions on the same lines, and both the fast parallel and the bidirectional port can run in any of the three data transfer methods.

3 **USB port:** USB printers can be connected to any available USB port on the computer.

4 **Network:** Network printers are connected directly to the local computer network. The DNS hostname of the printer must be known. If the printer is assigned a dynamic address by DHCP, DNS should be dynamically updated so that the host name always has the correct IP address. Network printers are often given static IP addresses to avoid this problem.

Printer cables and connectors

Printer cable carries data between a computer and a printer. Most printers connect to the following ports on the PC

- DB-25 parallel port
- USB port

Parallel printer cable

The parallel port socket in the computer uses 25 pins. On most peripherals like printers, the 36 pins Centronics version is used. The centronics socket is named after the company that introduced the first dot matrix printer in 1970.

Printers with only parallel port can be connected to USB port using USB adapters also Known as Parallel-to-USB cable, or use a PCI parallel printer port card. The maximum data transfer rate of parallel port is 150 KBps.

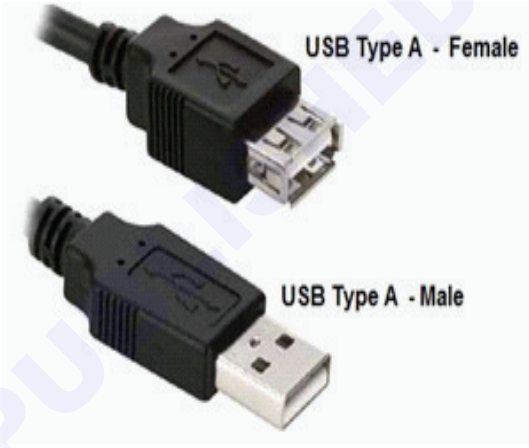
USB printer cable

The USB, or universal serial bus has replaced the RS232 and parallel communications in a lot of situations. USB is now the most used interface to connect devices like printer, mice and scanners to personal computers. Using a USB connector for printer increases the speed of the printing process, especially if the printer is handling printing jobs from multiple computers. There are several types of USB connectors, each capable of delivering the same data rate. The data transfer rate of an USB cable goes up to 480 Mbps.

Type A

The Type A USB connector is used to connect the USB Type A connection found in laptops and desktops to the same type of Type A plug in the printer. This is a rarely-used printer connection as Type A connectors are normally created only as a host connector on PCs and used to upstream information to an attached device. The Type A connector is shaped like a flat rectangle. (Fig 10)

Fig 10



Type B

The USB Type B is the most commonly found connector. Like the Type A, the end that connects to the PC uses a USB 4-pin connector plug. The other end however, uses a smaller Type B plug to connect into a Type B jack located on the printer. The Type B plug is of a squarish shape, and smaller in width than the Type A end. Two of the inside corners of the Type B connector have notches in them to aid in cable orientation when plugging the cable into the USB connector. The outside of the plug also has two beveled corners to help in orientation. (Fig 11)

Fig 11

Mini Type B

The Mini Type B cables are made for portable electronic devices. The cables connecting to Mini Type-B are generally made with the Type A connection on one end to connect to the PC and the smaller Mini Type-B with 5-pin connection on the other end. When used to connect a portable device to the printer, an adapter may be needed to convert the Type A end to a Type B for plugging the device directly into your printer. The Mini Type-B connector is usually found in smaller devices like cameras. (Fig 12)

Fig 12

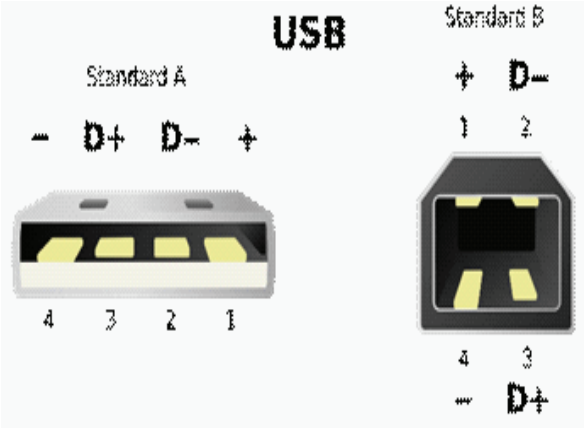
Mini Type B 4-pin

The Mini Type-B 4-pin has the same cable configuration as the Mini Type-B. The only difference is that it uses four pins instead of the five in use by the Mini Type-B. Connecting this cable to your printer may require an adapter for the Type A end, as with the Mini-B, to convert the Type A to a Type B for connection to your printer. Adapters are needed only if a Type A port on the printer is unavailable. (Fig 13)

Fig 13

In the standard USB A and B connectors, four pins are defined. Two pins are used for power and two pins are used for data transmission. The pins used for the power connection pin 1 and 4 are slightly longer as shown in Fig 14.

Fig 14



This is done to first connect the power supply when connecting a USB device, and then establish the data connection, thereby the chance that the driver or receiver ports of the data connection receive awkward and possible dangerous voltages is lowered substantially.

Pin Number	Cable Colour	Name	Function
1	Red	VCC	+5 V DC
2	White	D-	Data -
3	Green	D+	Data +
4	Black	Gnd	Ground

Network printer

Printers can be connected to a network using NIC and connection (typically RJ-45) by assigning an IP address either manually or automatically assigned from DHCP. Printers can also be connected to the print server.

One of the most common sources of printing problems is the printer cable.

Printer has a data buffer that receives the data from the computer and supplies it to the printer at a rate that the printer can accept. The signals from the printer to the parallel port turn on and off this flow of data. In a Centronics printer cable each of the 25 conductors on the printer cable is important to the proper operation of the printer. A bad cable can produce all sorts of strange printing problems.

Normal wear and tear can damage one or more of the wires or pins in the connectors. The Centronics connector is more vulnerable to damage than the D-type connector. A bad cable will often show no sign of damage. The fastest way to troubleshoot a cable with no obvious defects is to substitute a known good cable and see if the problem is solved. Or, connect the cable on a system that is having no problems and check whether the cable still has defects. The cable can also be tested using a PC Cable Tester or universal cable tester.

Checking USB printer cable

Delete the installed printer from the system. After deleting the printer unplug the USB printer cable from the system and plug it again. If the cable is good, the found new hardware wizard will show up and search for new hardware. The printer will be recognized and installed. If the Hardware wizard does not find the printer there is a chance for the cable to be at fault. Check the same with a different cable if available.

PC cable tester

It is a standalone portable test device designed to provide the user with a wire map of standard PC data cables. The LED display provided in the equipment clearly determines wiring status by providing a point to point pin out of actual wiring configuration. It is used to diagnose the existence of shorted wires, open wires and crossed wires a typical cable tester available in the market which is used to test the following cables and modular plugs such as LAN, telephone, Serial, coaxial, USB, VGA, Mini-USB, S-video, FireWire, and Printer cables in Auto scan and manual scan modes.

It provides a simple check and wiring configuration for DB9, DB15,DB15 HD, DB 25, Centronics 36, Mini DIN 6 PS/2, Mini DIN 4 S-video, 4-pin & 6-pin

1394 FireWire, USB, Mini USB, RJ11 and shielded and unshielded RJ45 telephone plugs.

In addition, RG58 or 59 BNC can be checked with a simple PASS or FAIL test with full diagnostic evaluation displayed if the cable fails.

Connect the cable to be tested to the corresponding connectors on the left- and right-hand sides of the tester.

The wiring configurations of some of the cables when tested in a cable tester are given below.

Printer Installation

To use a printer with a computer, the printer software which is a printer driver should be installed in the system and should make some settings to tell the computer how to find the printer and what to print. The drivers for the printer will be included in the CD / DVD that comes along with the printer or can be downloaded from the manufacturer's website. Some printers require that the software should be installed before connecting it, but other printers can be connected immediately. If the printer is a Plug and Play device, then connect it and power it on; Windows will installs what it needs automatically.

Connecting the printer to the computer and installing

Connect the printer to the computer either using a USB cable, parallel port cable, or SCSI cable and then connect the power plug to a power outlet. Insert the disk that came with the device and follow the on-screen instructions.

Choose Start -> Devices and Printers.

If you have a wireless printer, choose Start -> Devices and Printers and click the Add a Printer link in the window that appears. Choose the Add a Network, Wireless, or Bluetooth Printer option and follow the instructions.

In the Add Printer dialog box, click the Add a Local Printer option and click Next. The Add Printer dialog box appears.

The choose a printer port dialog box appears.

There are two options

If the manufacturer's disc is available, insert it in the appropriate CD drive now and click the Have Disk button. Click Next.

If the manufacturer's disc is not available, click the Windows Update button to see a list of printer drivers that can be downloaded from the Microsoft Web site. Click Next.

In the resulting Type a Printer Name dialog box, enter a printer name. Click Next.

Click Finish to complete the Add Printer Wizard.

Installing a wireless printer

Before starting installation of wireless printer the name or Service Set Identifier (SSID)of the network, and the password of the network should be known. A Service Set Identifier (SSID) is a sequence of characters that uniquely names a wireless local area network.

Place the printer temporarily near a PC that's already part of your network, so that it can be attached physically for software installation.

After installing the software of the printer place the printer within range of the wireless router or repeater. Any large metal objects, including building elements such as girders and even screen doors or windows, will interfere with the wireless signal. Even too many closed doors or walls will degrade the signal. If your wireless signal is weak or intermittent, move the printer closer to the wireless router and avoid obstructions.

In printers with LCD control panels configuration wireless configuration can be done directly from them. The printer will detect networks within range; then select the network and enter the password.

In printers without LCD screens configuring the wireless can be done using a Web browser.

Printer self test

Different tests are done in printers to identify and isolate the problems occurring in printers. Some test prints give the configuration details of the printers.

Self-test / Printer configuration test

A printer self-test is a test page which prints out when a series of buttons on the printer is pressed or a software is used to print a test page. When the self-test is run, the printer gives a page demonstrating the printer's ability to work. A self-test contains technical information about the

printer such as the printer's name, the amount of memory the printer has, and status log information which can be used to look up problem codes and its print settings. A self-test page also shows sample output from edge to edge of the machine's printable area. A Windows test page contains technical information about the printer like the software driver used by the printer, which version of the printer driver it is using, and where help or configuration files are located for the printer.

Printer configuration page tests the formatter of the printer. Printer configuration page can be printed by accessing the menu and information menu and then selecting Print Configuration. The configuration page gives the following information.

Printer Information

Lists the serial number, IP addresses, page counts, and other information for the printer.

Event log

Lists the number of entries in the event log, the maximum number of entries viewable, and the last three entries.

Installed personalities and options

Lists all printer languages that are installed (such as PCL - Printer Controlled Language and PS-Post Script) and lists options that are installed in each DIMM slot and EIO slot.

Memory

Lists printer memory, PCL driver work space (DWS), and I/O buffering and resource saving information.

Self-Tests in Dot matrix printer

Printers self-test is one of the facilities in built in a dot matrix printer. Self-test print is done without using a computer as an intermediary device.

Self-test helps to determine whether there is damage to the printer. In Dot matrix Printer Self-test is carried out by turning ON the printer while holding down a button or combination of buttons. Self-tests for different printers from different manufacturers are different. Same key combination will give different print output in different printers. Printer manufacturer's documentation gives the details of keys to be used for Self-test Fig 15 Shows a draft print test page.

Fig 15

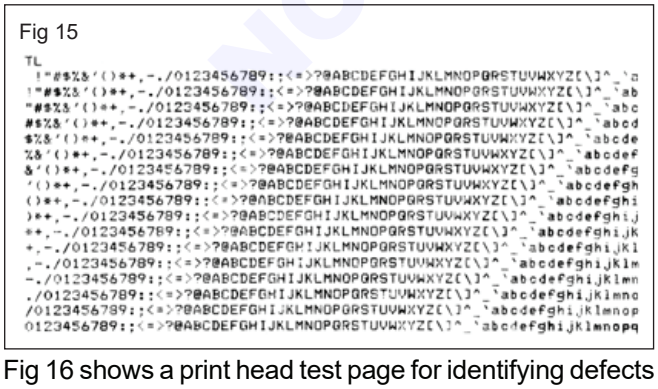
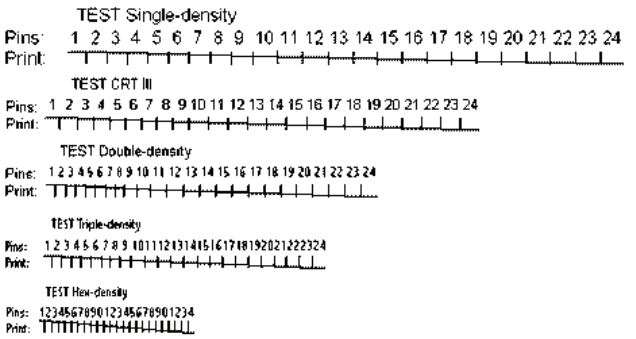


Fig 16 shows a print head test page for identifying defects in print heads

Fig 16



Self-Tests in Ink JET Printers

The test page in ink jet printers gives information such as device information (such as the product name, model number, serial number, and firmware version number), the accessories that are installed (such as the duplex unit), and the number of pages printed from the trays and accessories. It also Shows the estimated ink levels and the part numbers and expiration dates of the ink cartridges, and the status of the print head health and the part numbers, Using Test pages faults in cartridges and print heads can be easily isolated. Not all printers have self-tests. However, many have tests that are run by the drivers. Printing test pages uses a lot of ink.

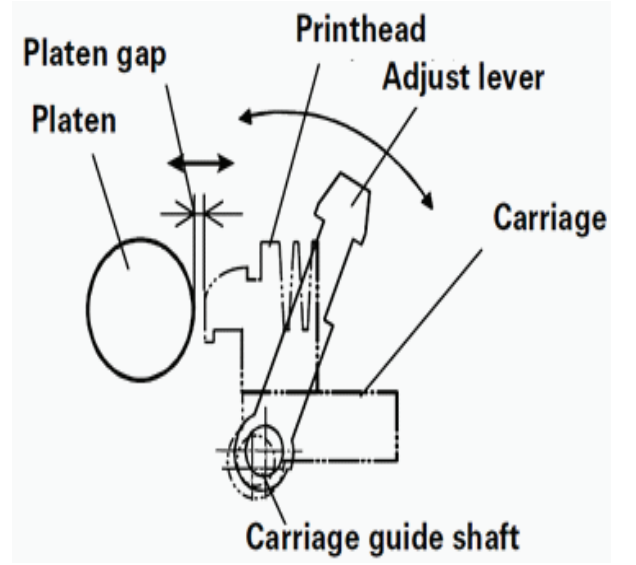
Sensors

Different types of sensors are used in Dot Matrix Printers to sense different parameters. The sensors used varies with the manufacturer and the type and model of the printer. Some of the sensors commonly used in Dot Matrix Printers are

Platen gap sensor

Platen gap is the gap between platen roller and print head as shown in Fig 17.

Fig 17



The Platen gap lever changes the distance between the print head and the platen. This helps the printer to print on thick paper. When printing on multi part paper, Platen gap lever is set on position 1. The lever activates a mechanical contact switch called platen gap sensor and causes the carriage to move at a slower speed. Thus preventing the printer head pins from getting struck up in the paper and breaking off.

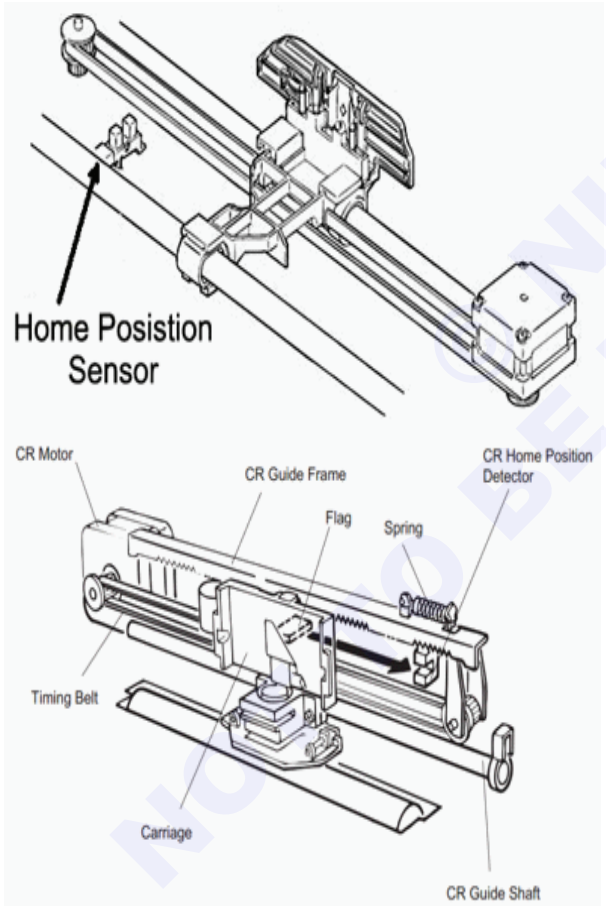
Carriage home position sensor

It helps to determine when the carriage is at home position, i.e. to the left side of the printer. The sensor remains open when the carriage is at home position and closed when away from home position. The sensor may be a mechanical switch or using a photo coupler. In a Photo coupler the sensor is activated when the light emitted from the photo coupler is interrupted. (Fig 18)

Front and rear PE sensors (use a photo interrupter)

Top PE sensor (to detect the TOF position, uses a photo interrupter)

Fig 18



Paper jam sensor (uses a magnetic transistor)

Tractor select sensor (uses a micro mechanical switch)

Pull tractor sensor (uses a micro mechanical switch)

CR encoder sensor (uses a photo interrupter)

PG encoder sensor (uses a photo interrupter)

PG home sensor (uses a micro mechanical switch)

Ribbon jam sensor (uses a photo interrupter)

Cover open sensor (uses a micro mechanical switch)

Printhead temperature sensor (uses a thermistor)

Head fan temperature sensor (uses a thermistor)

Paper width sensor (uses a photo reflector)

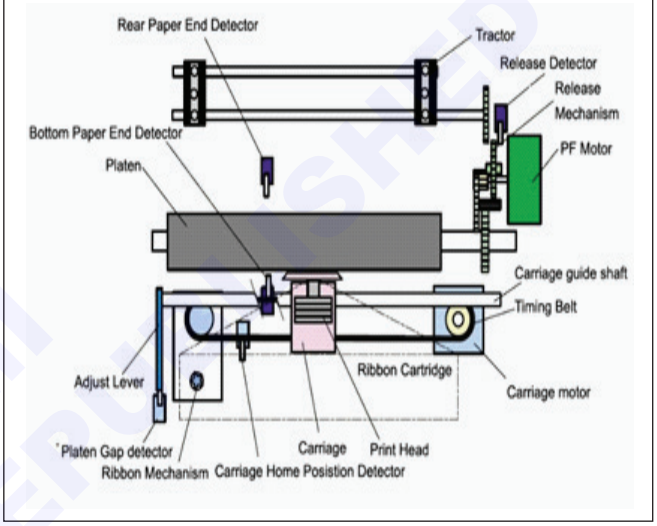
CR motor isolation resistance sensor (monitored by the analog port of the CPU)

PSB/PSE board power off sensor (signal interface)

Printing mechanism

Fig 19 shows the print mechanism of a typical Dot Matrix Printer.

Fig 19



Paper feed mechanism in DMP

Friction Feed: Friction-feed printer uses plastic or rubber rollers to squeeze a sheet of paper and pull it through the printer.

Tractor feed mechanism in DMP: Tractor-feed printers have two sprocketed wheels on either side of the printer that fit into holes in the paper. As the wheels revolve, the paper is pulled through the printer. Tractor feed is also called pin feed. Tractor-feed printers require special paper, whereas friction-feed printers can handle most types of cut-sheet paper, including envelopes. The tractors are narrow belts or cogs with prominent conical teeth or sprockets spaced to fit sprocket-holes in the paper. There is usually a tractor at either side of the paper.

Motor drive for the paper path is often a stepper motor. Some high speed printers have used DC encoder motors to achieve very high paper feed rates. (Fig 20)

Printhead mechanism: Fig shows the operation of a typical print head mechanism. The dot wire is attached to the actuating spring at point A. It is pulled back by magnetic force when power is applied and during standby. The magnetic force holds back the actuating spring. When current flows through the coil, a counter-magnetic field is induced in the coil. Then, the actuating spring ejects the dot wire forward against the ink ribbon, printing a dot on the paper. (Fig 21)

Fig 20

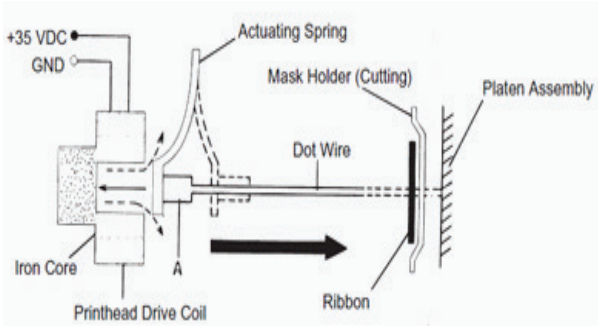
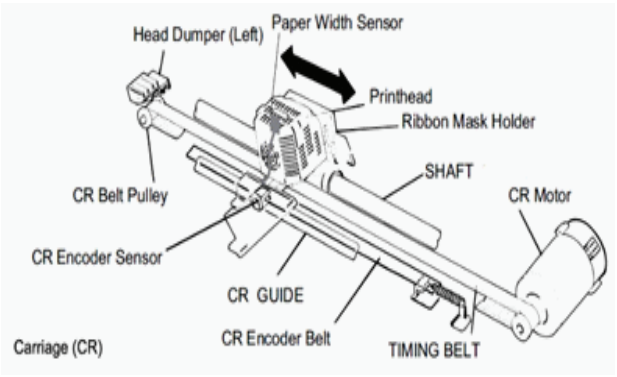


Fig 21



Carriage mechanism

The carriage mechanism moves the print head in the horizontal direction. The Carriage (CR) motor drives the carriage, with the print head on it.

The carriage needs to carry out its scanning action as rapidly as possible. The speed of pins in the head is the main limit on printer speed but the rate the carriage can travel is related. Clearly if the pin speed were doubled the carriage could travel twice as fast - doubling print speed. There is also some sort of balance between the number of pins packed into the head - which makes it heavy - and needing more power to drive it back and forth across the page. Continually accelerating a heavy print head one way and then the other does not seem a particularly efficient process and does require a fairly powerful motor. Other than the print head pins the carriage motor is usually the most stressed part of a printer system - and the most likely to give trouble.

Carriage rails normally provide support. The carriage normally grips one large rail, with a nearby smaller rail providing a bit of support. It may seem curious but carriage bearings rarely use rollers or ball bearings - these were tried on older designs but the need for a bit of elasticity in these bearings may have been a disadvantage. Almost all recent designs use either a brass / bronze or PTFE plastic sleeve on a steel rail. The carriage should slide very smoothly and easily. This is usually difficult to test because of course the carriage is usually connected to a drive belt and a motor - and they do not move particularly easily.

Carriage belts are toothed elastic material usually with a fibre or metal reinforcement. The belt loops across the width of the print-station with an idle wheel and tensioner at one side and the motor at the other. The motor has a toothed cog that meshes with the teeth in the belt. The carriage itself is locked to the belt at one point so when the motor moves the carriage is pulled in the appropriate direction. The most usual design is to have a motor at the right hand side, under the control panel. Older belts seem to be rubber and fabric, newer designs use fibre strings in an elastic compound.

Carriage belt tension needs to be right. If the belt tension is lose the user will see “margin drift” where typically successive lines of characters don’t all start in quite the same place. Bidirectional print shows the problem particularly strongly, successive print lines start in different positions. A printer with margin drift will print recognisable text but will be useless for graphics and bar codes.

The belt tension mechanism is usually a screw adjustment on the idle pulley at the left side of the printer.

Stepper Motors provide carriage drive on low cost printers. The microprocessor tells the motor to step forward or back and so far as possible it does so. A stepper motor typically has two coils and to move the motor the electronics alternately switches the current in the coils one direction then the other in a sequence. The drive circuitry is two circuits called bridges - four power transistors which switch on an off connecting the coils so that current flows in the correct direction.

Types of ink ribbons

Dot matrix printer ink ribbons

Dot matrix printers use either cloth or plastic ink ribbons, depending on the model of the printer.

Single-strike ribbons - Ribbons are only used in a single loop, thus creating consistent blackness throughout a document.

Multi-strike ribbons - You can use and reuse the ribbon but quality decreases over time. There are two types of printer ribbon: black and colored. Dot matrix printers used to be the main desktop printers in offices and businesses, until inkjet and laser printers were introduced. Today, dot matrix technology is still used in ATMs, cash registers, and other point-of-sale terminals.

Cash register and point of sale ink ribbons

Simple cash registers may contain small impact printers that use nylon ribbons for printing, but most modern, elaborate point of sale systems use small thermal transfer printers to print receipts, coupons, and other store-related items on special thermal paper for customers. Most of these systems use wax thermal ink ribbons, but some systems use a wax / resin combination ink ribbons for greater durability.

Thermal transfer printer ink ribbons

Thermal transfer printers use heat to, in essence, melt the ink and transfer it on to the printed medium. Durability needs can vary dramatically when it comes to items that are printed with thermal transfer printers, which is why there are three different types of ink that are made for these printers: wax thermal ink ribbons, wax/resin thermal ink ribbons, and resin thermal ink ribbons.

Wax thermal ink ribbons

Wax thermal ink ribbons are primarily used for printing on paper products. The wax ink adheres to both matte and semi-gloss finishes and is designed to last without smudging for years. However, the ink has to be kept dry, and it cannot be subjected to scratching or rubbing. Chemicals and oils can also easily destroy the ink, and this includes the oils from skin. This type of ink will last for years only if the item that has been printed with it is tucked away in a dry location and is rarely handled, which is why it is most commonly used for printed items that are only intended to last for a short period of time. This is the thermal printer ribbon that is best suited for paper printing. It can also be best suited for synthetic materials that require light direct contact only and those that do not create direct abrasion while printing.

Wax/Resin thermal ink ribbons

Wax / resin combination ink ribbons contain ink with greater durability and longer life spans than their pure wax counterparts do. Because of the resin content, these inks are more resistant to chemicals, smudges, and scratches than wax ink is, which makes these ink ribbons much more appropriate for printing items that could potentially be exposed to a good deal of human contact. Wax/resin inks are still vulnerable to water, however, and are not typically used on items that could be exposed to moisture. These ribbons can also be used for printing over synthetic materials.

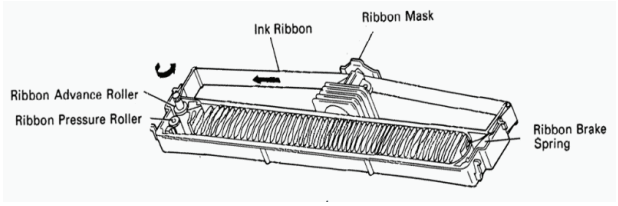
Resin thermal ink ribbons

Resin thermal ink ribbons produce the highest quality of the three types of thermal ink ribbons, as well as the most durable print of all of the types of thermal ink ribbons. These inks are extremely resistant to heat, chemicals, scratching, and many other environmental hazards. Thermal printer ribbons are primarily used in synthetic materials specifically those with a glossy finish. It can also be used when the printing process requires high chemical heat and direct abrasion.

Ribbon cartridge

The ribbon cartridge contains several mechanisms to ensure proper guidance of the ribbon. At the entrance slot, a pressure roller clamps the ribbon against the advance roller, enabling the advance roller to ”grab” the ribbon and draw it in. The ribbon brake spring, attached to the exit slot of the cartridge case, prevents slack in the ribbon and keeps its tension at a constant level. The ribbon mask prevents the ribbon from brushing against the paper. (Fig 22)

Fig 22



The ribbon enters on the left, goes through the gearwheels, which pulls on the ribbon and folds randomly into a large bundle. The calmer end goes past a plastic barrier with a stainless steel spring that provides some resistance to the ribbon pulling out of the cartridge, to keep the tension on the ribbon external to the cartridge. The whole ribbon is an endless loop that is advanced automatically by the printer periodically and can run around many times until such time there isn't enough ink on the ribbon and the printout becomes too faint. The top side of the cartridge also has a manual knob to control the ribbon take-up. The cartridge bottom has a slot for a shaft to drive the take-up spool automatically.

Refilling DMP Ribbon Cartridge

Ribbon Cartridge refills are available in the market. The refill consists of inked ribbon only. The used up fabric in the cartridge should be removed from the cartridge and the new refill can be placed in the empty cartridge. Place the loop of ribbon carefully through the gear at the left end and through the spring at the right end. Take care that the loop is not inter twined. Tighten the loose ribbon end using knob on the top. The refilled cartridge should be tested with a test print.

DMP head mechanism

The printing mechanism is composed of head, ink ribbon and ribbon mask.

The print head consists of the parts listed below.

Wire Guide

Print Wires

Armature Assembly

Spacer

Permanent Magnet Assembly

Thermistor: used to monitor the printhead temperature

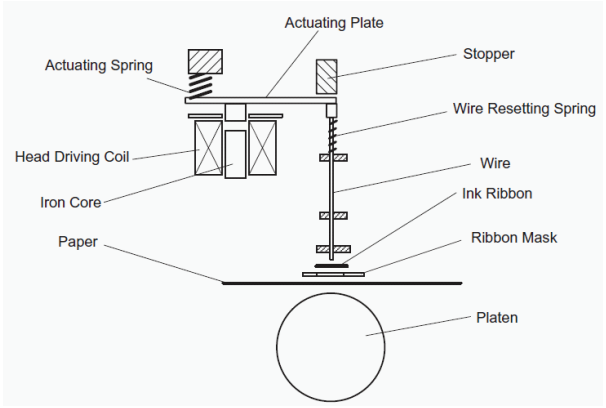
Printed Circuit board with Coils

The print head may be a 24-pin(12pins x 2) head or 9-pin (9 pins x 1) for impact dot matrix printing. The pins are steel wires which has its own drive coil. Fig 23 shows a typical print head mechanism in detail.

A drive signal, transmitted from the control circuit to the print head drive circuit, is converted in to proper print head driving voltage, which energizes the corresponding head coil. The energized coil then causes the iron core to become magnetized.

The magnetic force draws the actuating plate toward the core, and the dot wire, which is connected to the core, rushes toward the platen.

Fig 23

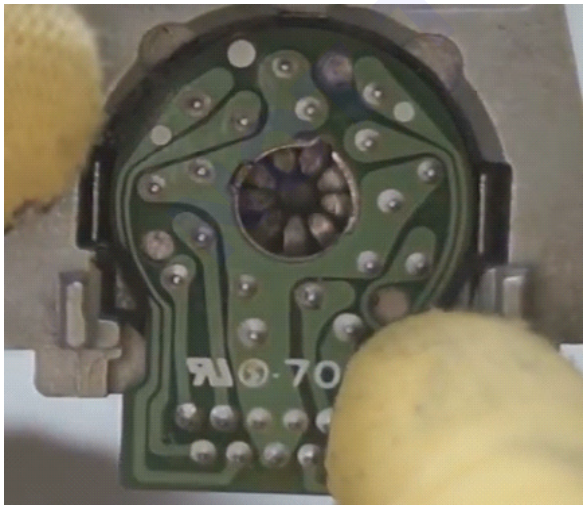


When the dot wire impacts the platen, pressing against the ribbon and paper, it prints a dot. When the driving voltage stops energizing the coil, the magnetic force vanishes from the iron core. The actuating plate returns to its original position and the dot wire also returns to its original position due to spring action.

Fig 24 Shows the actuating plates inside a disassembled 9 pin printer head

Since the print head heats up after a period of use, it is equipped with a thermistor to detect head temperature. The temperature detected by the thermistor is converted to an electric signal and fed back to the control circuit. In order to keep the same print quality, the drive mode of the print head is changed over according to the paper type and head temperature. This drive mode minimizes the degradation or damage to the dot wires in the printhead, which is caused by temperature rise of the print head from continuous printing, and also keeps print quality when the surrounding temperature is extremely low. Voltage changes reflecting changes in the thermistor's resistance are output to the CPU.

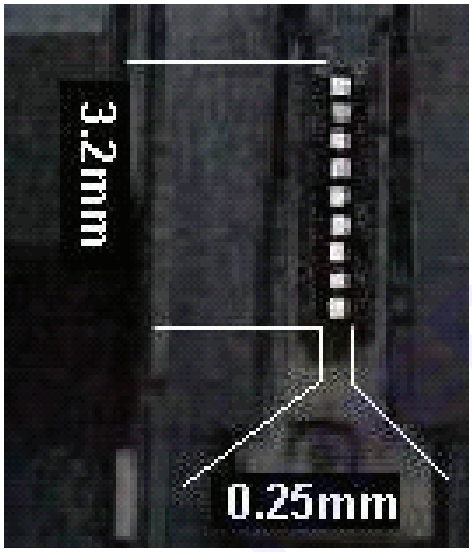
Fig 24



Types of Print Head

Based on the number of pins used in the printer head it is classified as 9 pin, 18, 24, 27 pin and 48 pin printer heads. Fig 25 shows the dimensions of a 9 pin head. A 0.25mm 9 pins head gives 100 dpi print.

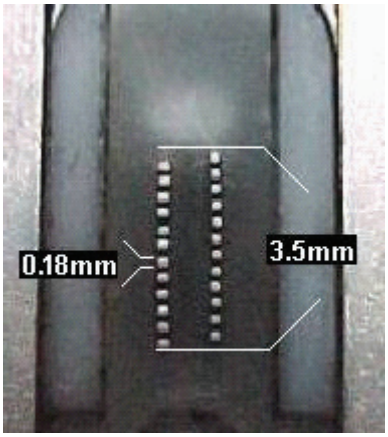
Fig 25



A 24 pin head has a 3.4mm strip and 01.8mm pins in two rows. It has been found that finer pins are more vulnerable to damage. Fig shows a 24 pin print head arranged in two columns. (Fig 26)

Some printers were made with "letter quality" 48 pin heads. These actually had two or more rows of pins in the head. Below 0.1 mm the metal of the pins was too light and weak to bending. Most 48 pin heads proved rather too weak.

Fig 26



Pixel Shape and Quality

Dot matrix pixel shape is normally circular.

Circular pins are the shape with least mechanical resistance to rapid movement and the best wear characteristic as well as being easiest to manufacture. Printers often have a "near letter quality"(NLQ) print mode that joins the dots by overprinting. NLQ print is slower but generally does look much better than draft mode.

The practical limit on dot-matrix technology is the speed of the pins.

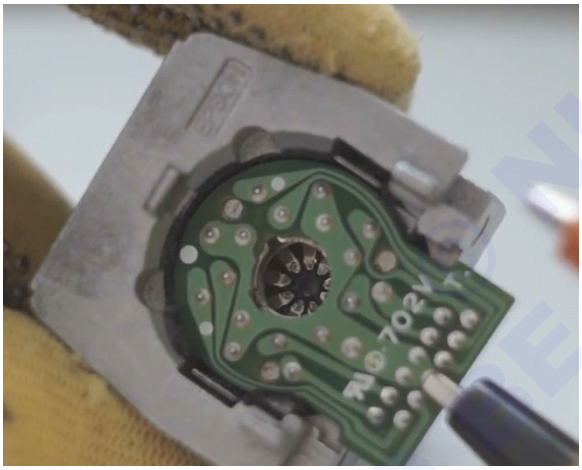
Dot matrix print head Problems

The most common print quality problem with dot matrix printers is a, “missing horizontal line of dots.” This is due to breaking off of pins and the remaining portion of the dot wire is too short to impact the paper.

There are, however, other reasons a pin may fail to strike the paper. Worn out head pins will also cause the print to be dull and faded out. It is also possible that the signal to fire the pin is not reaching the print head. If the ribbon cable connecting the print head to the main board is damaged, one or more of the signals to fire a pin will not reach the head. This can happen if the ribbon cable touches something while the carriage unit is moving back and forth. Therefore, the head cables should always be examined for any obvious flaws before concluding that the head has failed. To check the cable, unplug both ends of the cable and test continuity with a meter.

Apart from examining the head cables, the second basic step in diagnosing a dysfunctional dot head is measuring the resistance through the pin solenoids using an Ohm Meter. A 9-pin head has 9 individual solenoids and a 24-pin head has 24. (Fig 27)

Fig 27



Another reason for dysfunctional head is damaged head driver circuit. Measuring resistance through the head solenoids will help reveal a problem with the driver circuitry on the main/driver/logic board. A solenoid that measures very high or very low resistance relative to the value given in the printer manual, indicates there is a problem with the transistor responsible for firing it. If a new head is installed before servicing the defective driver circuitry, it will be quickly damage the new head in same manner as the old head.

Cleaning DMP Heads

Printouts with excess ink or ink smudges, faded characters and overall poor print quality may be related to the ribbon or dirty print head. To troubleshoot this issue, replace the ribbon and print a test page to see if the output improves. If not, then it’s likely that the print head should be cleaned.

Visually found debris in the head can be cleaned manually using a pair of tweezers. Ink deposits can be cleaned using a cotton swab dipped in Iso propyl Alcohol.

Functioning of DMP power supply

Printer SMPS consists of a EMI / RFI filter, a switching circuit and a feedback circuit. It also has a high frequency and high current protection circuitry. The SMPS supplies different voltages to the following sections

Logic card

CPU or Micro controller

PROM and RAM

CR motor and control logic

PF motor control Logic

Print head control logic

Interface logic

Control panel and Front panel

In the power supply circuit, the input AC power goes to the filter circuit, where the noise is removed by the filter circuit the diode bridge rectifier does full-wave rectification and the voltage is smoothed by the electrolytic capacitor. The voltage is fed to the gate port for switching FET Q1 through resistors. The switching regulator on the primary side uses Zero-cross ringing choke converter type (ZC-RCC)which contributes to the power supply circuit’s high stability, efficiency, portability and effectively generates +35VDC in the secondary side. Also, +35VDC generates +5VDCby the DC-DC converter(chopper IC).

The secondary circuit system of the power supply circuit includes the Power button. The Power button is located on the printer’s control panel and controls the power supply circuit.

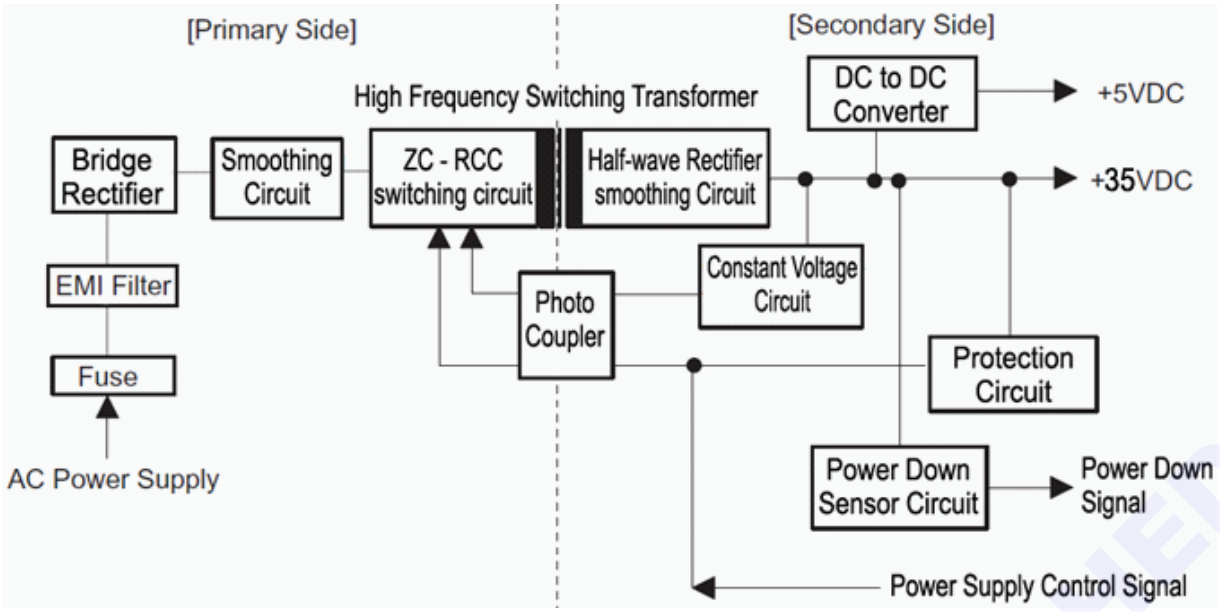
A +35 V line constant voltage control circuit and over-current/over-voltage protection circuits are provided to protect the printer and control circuits.

The power supply control signal (PSC) turns ON/OFF the switching FET through the photo coupler in the primary side. Therefore, input voltage is in the primary side when the AC cable is plugged in. When it is off, the current consumption is less than 1W.

The Power Supply Control (PSC) Signal turns on the power in the open state and turn off at the GND level. If the harness connecting with the operation panel is broken or disconnected and the PSC is in the open state, the power will be always on.

Fig 28 shows the block diagram of a typical Dot matrix SMPS power supply.

Fig 28



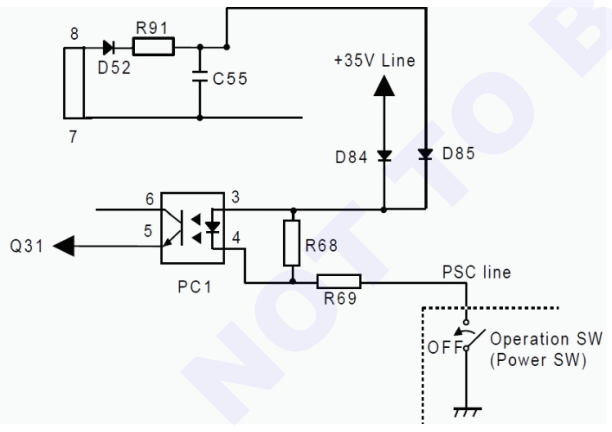
In the power supply shown in Fig 28. +5V powers the main board logic circuit, sensors and control panel LEDs, whereas +35 V powers the CR motor, PF Motor, Print head driver.

Power switch circuit

The power supply circuit is composed of an RCC (ringing choke converter) system and the power switch circuit in the secondary circuitry.

When printer power is off, the PSC line is connected to a ground line and the current is loaded from C55 to PC1. Consequently, Q32 and Q31 are turned on, and the switching FET is shut off. See Fig 29.

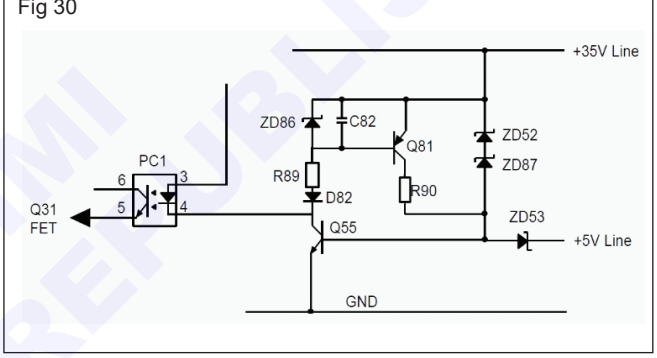
Fig 29



Over voltage protection circuit

When the output level of the +35V exceeds 42V or if the +5V exceeds 7.5V the switching FET in the primary side is switched off using the Zener diodes, Transistors and photo coupler in the circuit. Fig 30. shows a typical over voltage protection circuit.

Fig 30



The +35 VDC over voltage protection circuit operates when voltage exceeds 42V between ZD52 and ZD87 and shuts off the switching FET. The +5 VDC over voltage protection circuit operates when voltage exceeds 7.5 V between ZD53, and shuts off the switching FET. When either of these protection circuits operate, the protection cannot be removed without turning power off and on again.

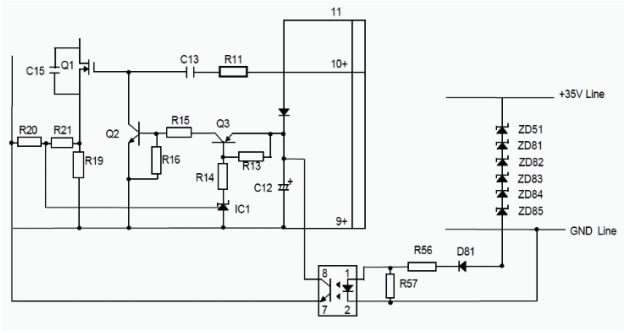
Constant voltage control circuit

The constant voltage control circuit operates to keep the 35 V line at 35 V ± 6 %. When the voltage between ZD51 and ZD85 becomes 32.7 V ± 2.75 %, PC1 turns on, and then Q2 also turns on. Consequently, switching FET Q1 shuts off. When the voltage between ZD51 and ZD85 becomes less than 32.7 ± 2.75 V, PC1 turns off, and then Q2 also turns off. Consequently, switching FET Q1 operates again. Repeating the above operation keeps the +35 V line at 35 V ± 6%. Fig 31. shows the constant voltage control circuit.

Line over load detection circuit

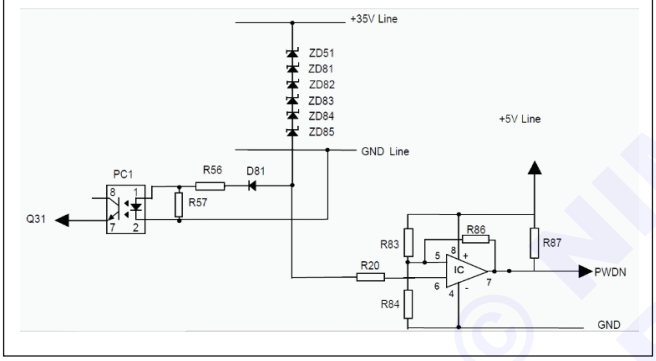
When the +35 V line is over loaded, it means that constant voltage control is not being maintained. In this condition, the forward current of PC1 drops to 0 A. Consequently, voltage Vf between PC1 and D81 also drops. (Fig 32)

Fig 31



In the circuit shown in Fig 45, when the Vf voltage drops below 1.3 V (+35 V line: 33.1 V), IC528 detects the overload and outputs the PWDN signal (+5 V: HIGH active) to port 20 of the CPU. When the CPU receives this PWDN signal, printing stops. When the +35 V line becomes normal again, the voltage between PC1 and D81 also becomes normal. When the Vf voltage goes above 1.6 V (+35 V line: 33.4 V), the PWDN signal is removed.

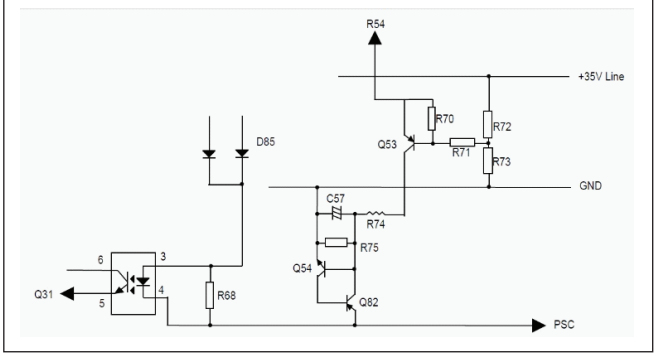
Fig 32



Over current protection circuit

When the +35 V line becomes less than 27 V, Q82 and Q54 turn on, and PC1 turns on. Consequently, Q32and Q31 turn off, and then switching FET Q1 shuts off. When the protection circuit operates, this protection can only be removed by turning the power off and on again. See Fig 33.

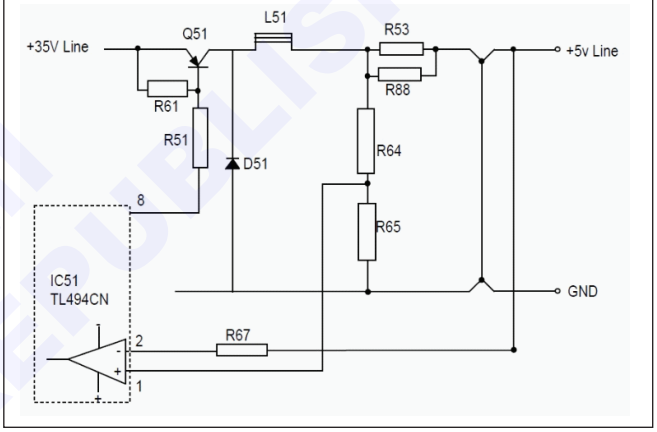
Fig 33



+5 V line over current control circuit is shown in Fig 34.

Port 2 of IC51 (TL494CN) monitors the +5 V line, and this protection circuit operates when the +5 V line goes below 4.75 V. When this circuit operates, port 8 signal output of the PWM pulse stops, and Q51 stops its switching operation. Consequently, the +5 V line stops generating.

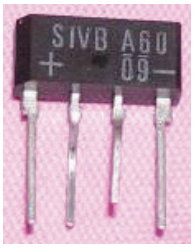
Fig 34

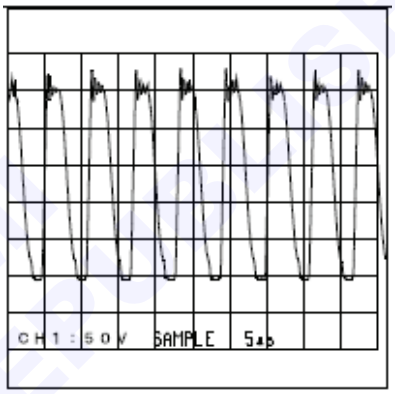
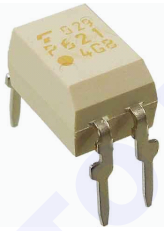
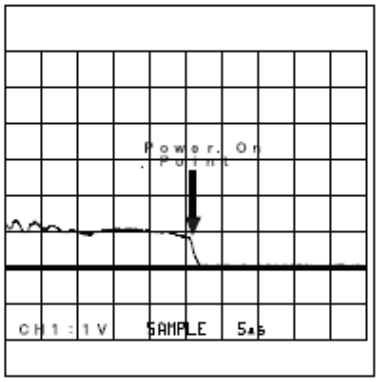


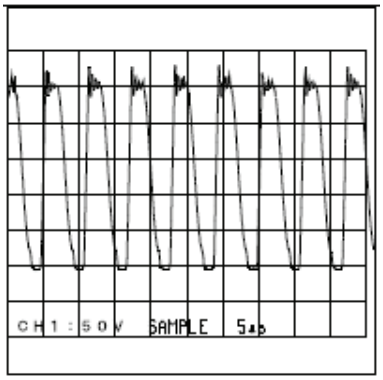
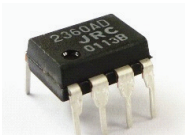
Power down detector

When the output voltage of +35V becomes low and unable to maintain stable voltage, the power down signal (PWDN) is output to the control circuit.

Fault finding power supply board

Problem	Cause	Testing point
The 35 V and 5 V lines are not output when the printer is powered on.	The diode bridge is defective. 	Measure the output DC voltage between the pins +ve and -ve terminal of the Diode Bridge.
	Rectifier/smoothing circuit is defective.	Check if Diode bridge is connected to AC line or not. Check all elements on the +ve side of the primary side such as Capacitors and Resistors. If there is short in Diode Bridge then, there is a possibility due to short circuit in the end of the circuit.

Problem	Cause	Testing point
	Rectifier/smoothing circuit is defective.	Check if Diode bridge is connected to AC line or not. Check all elements on the +ve side of the primary side such as Capacitors and Resistors. If there is short in Diode Bridge then there is a possibility due to short circuit in the end of the circuit.
	Line filter circuit is broken.	Check whether line filter and parallel capacitors are connected to the AC Line. Check the continuity of Line Filter coil.
	The transformer coil is open.	Measure the resistance of T1 transformer coils at pins.
	Switching FETQ1 (refer Fig 4) is defective.	Check that the resistance between the source and drain should be infinite. Check the voltage waveform between the source and drain of the switching FET, The switching operation is visible. 
	Opto Coupler is defective. 	Check the voltage waveform between pins 3 and 4 of the PC. 
	Q32 is dead.	Check that the resistance between the collector and emitter. It Should be infinite.
	Q31 is dead.	Check that the resistance between the source and drain. It Should be infinite.

The +5 V line is not output.	IC51 is dead.	Check the voltage waveform at pin 8 of IC51.
	Q51 is dead.	Check the voltage waveform between emitter and collector of Q51. 
	Smoothing Filter coil Short. L51 (see Fig 8.)	Check the resistance between both terminals of Filter Coil. Check whether the voltage of pin 6 is more than 1.3 V or not. If the voltage is more than 1.3 V, IC52 is dead.
The PWDN signal is constantly HIGH.	DC to DC Converter IC is defective. IC51 in Fig 8. 	

Functioning of DMP carriage assembly

The carriage movement mechanism consists of the carriage assembly, carriage (CR) motor, timing belt, driven pulley, home position (HP) sensor, etc. The CR motor drives the timing belt. The carriage assembly is connected to the timing belt, which is moved by the CR motor. Carriage mechanism and its functions are : -

Carriage: Mounts the print head.

CR motor: Drives carriage to the printing column direction. Usually printers use stepper motor for CR motor. Open loop control switches the phases according to the setting period and this mechanism enables the carriage to move until the appointed position.

Timing belt: Transfers the drive from the CR motor to the carriage.

Carriage guide shaft: Shifts the carriage parallel to the platen.

Home Position detector: Detects carriage home position. HP detector detects the signal right after when the CR motor switches the phase.

Fig 48 shows the carriage movement mechanism.

The printer detects the carriage home position with the HP sensor. This sensor is the basis for determining the carriage position. The HP sensor informs the CPU when the carriage is at the home position. The sensor is ON, when the carriage is pushed to the right or left. The striker on the carriage activates the sensor to indicate the carriage is at the home position, which toggles the sensor to OFF.

Paper feed assembly: Consists of paper feed motor (PF motor), paper feed gears, platen, rear paper end detector, bottom paper end detector and push tractor unit. Paper Feed Motor is a stepper motor. Open loop control switches the phases according to the setting period and this mechanism loads and carries paper to the appointed position and eject paper.

Motors

A dot-matrix printer generally has two motors. The vertical or line-feed motor drives the paper through the print-station, usually by driving a gear-chain and forms tractors. This motor needs to be capable of starting and stopping quickly to allow the position of a print-line to be determined quickly. The horizontal or carriage motor drives the print-head backwards and forwards within the print-station. This motor needs to be powerful because it has to accelerate and decelerate the print-head at either end of its travel.

In small printers the two motors are commonly both steppers. In large fast printers it is common to find the fast-moving carriage driven by a DC- Encoder motor.

DC encoder motors. The encoder motor is a conventional DC motor like that used in toys and other small devices. This has a permanent magnet stator locked in position. The stator creates a strong magnetic field within the motor. The armature is the shaft assembly in the middle of the motor, which is usually a stack or iron plates wound with coils - there are typically 3, 5, or many coils. When one or more coils are fed with current the armature creates its own magnetic field and moves to align itself with that of the stator. DC motors provide a powerful

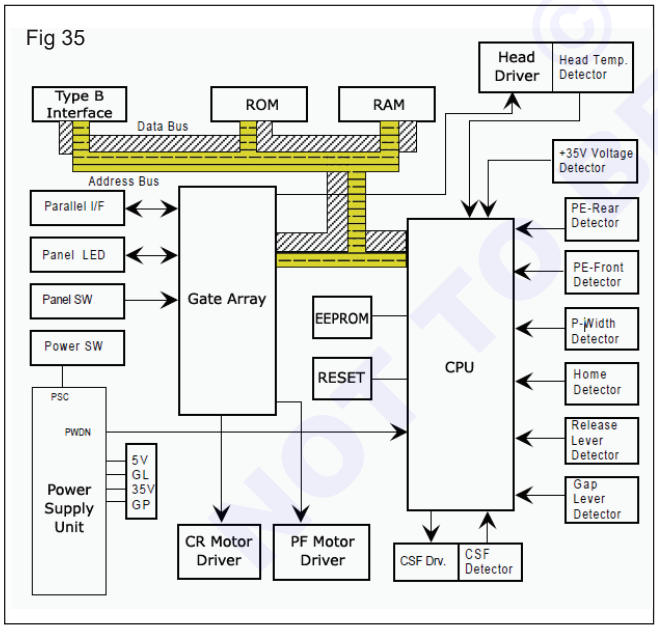
and responsive action in a relatively small package. In DC motors the response isn't precisely predictable so a control circuit does not know where the mechanism has got to. DC motor designs typically rely on an "encoder" to give feedback on position in some way. The encoder is typically a slotted disk with an opto-sensor on the back of the motor.

Stepper motors are "brushless" motor, usually with a strongly magnetised armature in the centre and two or three coils mounted around the outside. Each coil is activated in turn and the magnetic attraction or repulsion forces the armature round. Stepper motors don't have the brush and commutator mechanism to give continual motion, instead they rely on some external electronics to provide the alternate operation of the coils. One advantage of a stepping motor is that it only moves when the control electronics says to do so. When there is no current the magnet tends to resist movement, a phenomenon called "detent". Within certain limits a microprocessor control circuit can control where the mechanism has got to very precisely by just feeding successive pulses to the coils. The control circuit can know what the mechanism is doing without feedback.

Function of DMP control board

The control circuit oversees control of all the components in the printer and consists of a Main Board assembly and a panel board. The Dot Matrix printer's control circuit consists of a CPU a gate array, a PS-RAM, a bit PROM, CG (Standard Version) or CG (NLSP Version). (Fig 35) Shows the control circuit block diagram of a typical Dot Matrix printer.

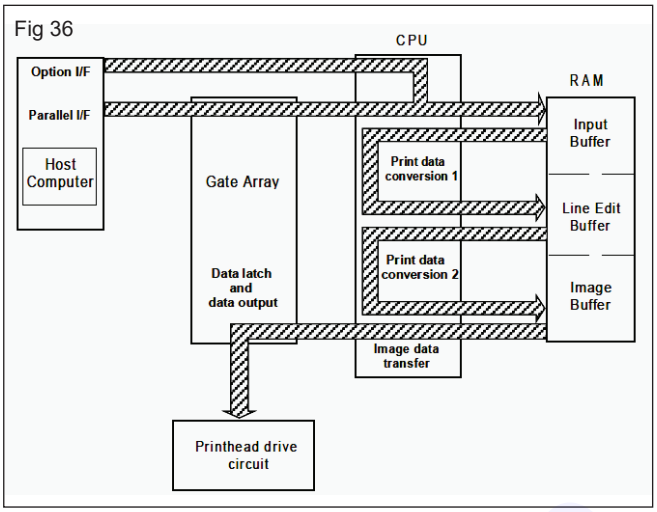
Fig 35



CPU

The CPU receives data from the host computer and sends it to the input buffer in RAM (under interrupt processing control). Extends the input data held in the buffer to create image data. Loads this image data to the image buffer in RAM. Transfers the image data to the print head driver circuit. (Fig 36)

Fig 36



Gate array

The gate array controls the functions below:

- Controls output data from the internal block
- Memory management
- Address latch of the address/data bus from the CPU
- Clock control unit
- Bit manipulation
- Interface control
- Expanded parallel port
- Print head control
- Motor control

EEPROM

An electrically writable and erasable ROM used to hold information such as the TOF position and bi-directional adjustment value. The EEPROM is non-volatile memory that stores information even if the printer power is off. The EEPROM is controlled by CPU ports. When the PWDN signal (power down) is detected, the CPU writes the necessary data to the EEPROM before the +5 V line drops to 4.75 V.

ROM

The ROM contains the program that runs the CPU and holds the character design (also called the character generator).

RAM

The RAM contains the CPU working area and the buffers.

CG

The Character Generator (CG) contains the bitmap fonts for each character table.

Carriage (CR) motor driver

The carriage motor driver circuit controls the CR motor. CR motor driver circuit detects and regulates the amount of current flowing in the carriage motor coil. The current flowing through the coil varies, depending on the speed of the CR motor. The CPU sets the amount of current and signals are sent via ports 32 to port 35.

PF motor driver

Driver circuit for the PF motor.

System reset circuit

Control circuits of CPU and Gate array ICs are initialized when a /RESET signal (LOW level) is output from port 1 (VOUT) of system reset IC. The system reset IC monitors the +5 V line on port 3, and resets under the following conditions:

1 When the power supply is turned on, a RESET signal is output. RESET is canceled when the +5 V line goes up to 4.2 V, and then100 ms passes.

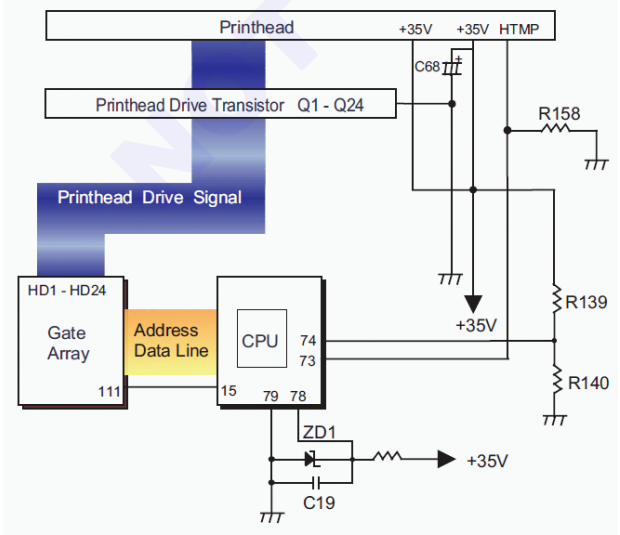
2 When the +5 V line goes below +4.2 V, a RESET signal is output. RESET is canceled when the +5 V line goes back up to 4.2 V and then 100 ms passes.

Print head driver circuit (Fig 37)

Print head drive begins with monitoring the 35 V line currently applied. This function enables the printer to change the period of time for applying current to the print head slightly depending on the condition. As a result, the printer can output image at a constant density.

When a high-duty job is in process, the temperature inside the print head will rise, and if the job is continued at a high temperature, it may damage the coil. Therefore, the Pin 73 (AN0) on the CPU monitors the temperature inside the print head. With this operation called protection operation for hot head, printing is stopped when the temperature reaches the standard level 1. As the temperature drops to the standard level 2, printing begins again at a lower speed, and then at a normal speed when the temperature lowers to the standard level 3.

Fig 37



Once the current flows into the head drive resistor, the coil for the corresponding pin is activated with the current. The current flown in to the coil is converted into energy used to rush the pin. Note there is possibility that some unused energy returns to the board, which may damage the head driver transistor. For this reason, a Zener diode is attached for each transistor to ground the current so the voltage over the standard level (15 V) does not directly return to the transistor.

The standard voltage for the A/D converter is made in ZD1 and input to CPU port 78. Based on this standard voltage, the A/D converter in the CPU operates. Port 74 monitors the +35 V line between R50 and R51 to determine the print head driver pulse width. Using the monitored voltage, the CPU converts the voltage to a digital value and decides the print head driver pulse width, and then transports the data to the gate array via CPU port 15. Based on the monitored voltage, the CPU decides the printing interval. Port 73 monitors the print head temperature to protect the print head. If the temperature exceeds 95° C (213° F), printing is stopped.

Sensor circuits

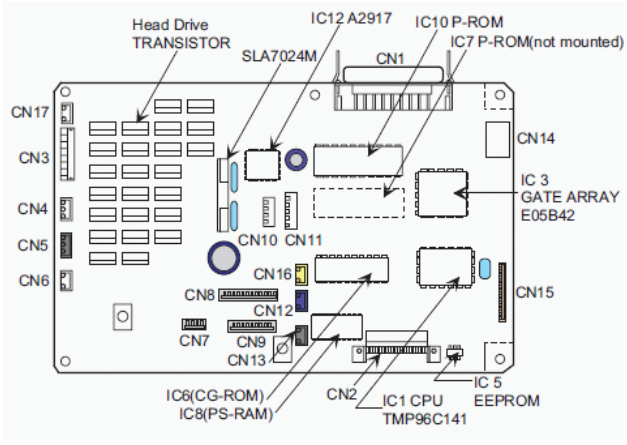
The CPU detects conditions of the following sensors: home position (HP) sensor, release sensors 1 and 2,platen gap (PG) sensor, rear and front paper end (PE) sensors, paper width (PW) sensor. Two types of sensors are used in this printer. Release sensors 1 and 2, the PG sensors, and the front PE sensor are momentary switches.

The HP sensor, rear PE sensor, and PW sensor are photo diode switches. The HP sensor detects CR home position when the photo diode rays are cut off by the printhead. The rear PE sensor detects that paper has been loaded when the photo diode rays are cut off by the sensor plate, which is included in the rear PE sensor. The PW sensor, used for paper width measurement and paper loading positioning, detects the paper edge by comparing the voltage it measures with a standard voltage that was measured during the power on sequence.

The +35 V line and head temperatures are monitored to set the pulse length of the head driver signal.

Fig 38 shows the block diagram of DMP main board.

Fig 38



Identifying problems in main board.

Problem	Possible causes
The printer does not operate at all.	Reset IC Is Defective
	Gate array IC Defective
	CPU IC defective
Carriage operation is abnormal.	CR Driver IC defective
	CPU IC defective
Paper feed is abnormal.	CPU IC defective
	Gate array IC Defective
	PF Driver IC defective
No data is printed.	CPU IC defective
A particular dot fails to print.	Gate array IC Defective
	One of the head drive transistors is defective

Laser printer

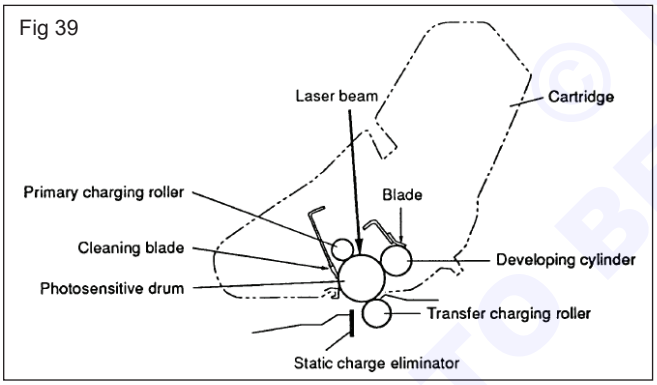
A laser printer is a type of electro photographic printer. Laser printers work with the combination of mechanical, electrical, and optical technologies.

The entire laser printing process can be explained using the following six steps

1 Cleaning

A wiping blade is used to clean the drum of any residual toner. Erase lamps light the surface of the drum to neutralize any electrical charge left on it. These erase lamps are usually in the top cover of the printer Fig 39 shows the cleaning blade construction.

Fig 39



2 Conditioning

The drum is conditioned by a roller that places a high uniform electrical charge of -600V on the surface of the drum. The roller is called the primary charging roller (PCR) or primary corona, which is charged by a high-voltage power supply assembly Fig 40 and Fig 41shows the developing cylinder and primary charging roller construction. Fig 40 and Fig 41 shows the developing cylinder and primary charging roller construction.

3 Image writing

A laser beam discharges a lower charge only to places where toner should be applied.

Fig 40

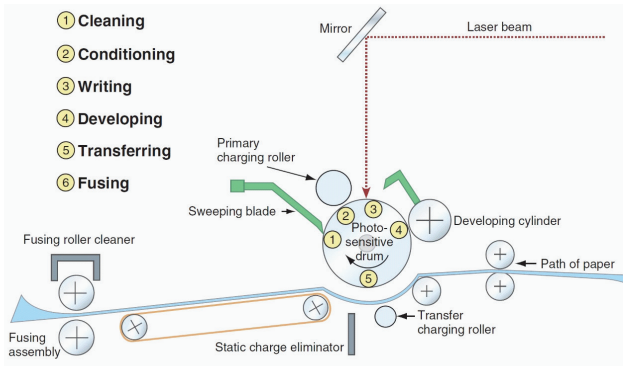
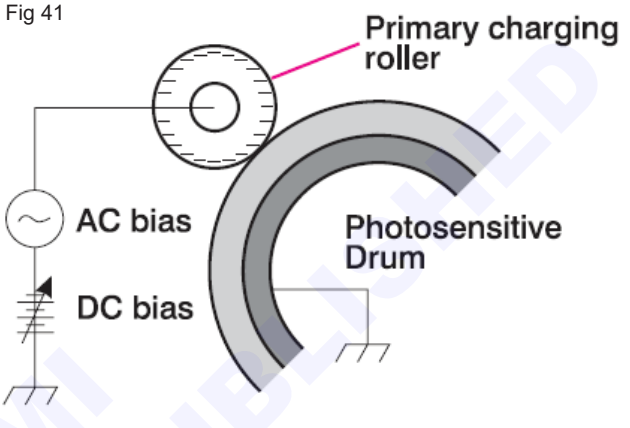
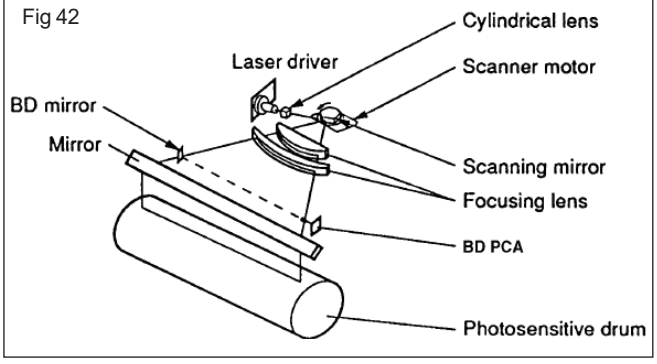


Fig 41



The uniform charge applied in the conditioning stage is discharged only where you want the printer to print. This is done by controlling motors and mirrors that direct the laser beam to scan across the drum until it completes the correct number of passes for each inch of the drum circumference. For example, for a 1200 Dots Per Inch (DPI) printer, the beam makes 1200 passes for every one inch of the drum circumference. The laser beam is turned on and off continually as it makes a single pass down the length of the drum, so that dots are written along the drum on every pass. (Fig 42)

Fig 42



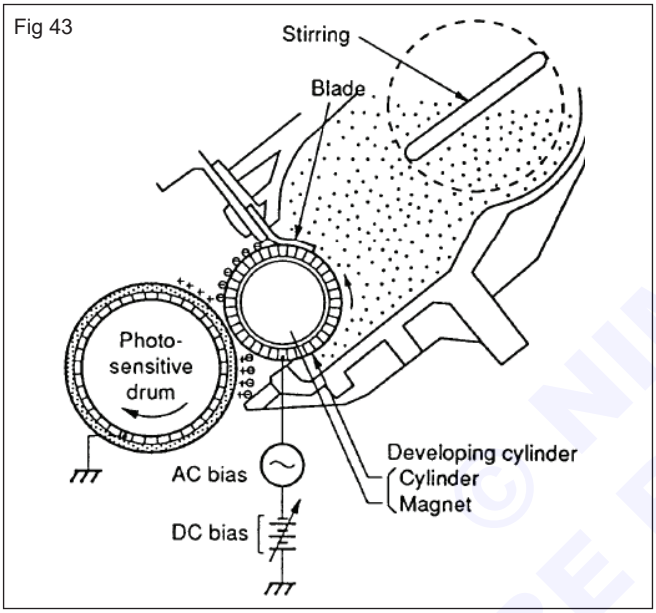
For a 1200-dpi printer, 1200 dots are written along the drum for every inch of linear pass. The 1200 dots per inch down this single pass, combined with 1200 passes per inch of drum circumference, accomplish the resolution of 1200 x 1200 dots per square inch of many desktop laser printers. The laser beam has written an image to the drum surface as a -100V charge. The -100V charge on this image area will be used in the developing stage to transmit toner to the drum surface. At the end of each sweep, the beam strikes the beam detect lens,

generating the Beam Detect (BD) signal. The BD signal is sent to the DC Controller, where it is converted to an electrical signal used to synchronize the output of data (VDO) for one sweep (scan line) and to diagnose problems with the laser diode or laser/scanner motor.

4 Developing

The developing cylinder applies toner to the surface of the drum. The toner is charged and sticks to the developing cylinder because of a magnet inside the cylinder. A control blade prevents too much toner from sticking to the cylinder surface. As the cylinder rotates very close to the drum, the toner is attracted to the part of the surface of the drum that has a -100V charge and repelled from the -600Vpart of the drum surface. The result is that toner sticks to the drum where the laser beam has hit and is repelled from the area where the laser beam has not hit. Fig 43 shows the image developing stage.

Fig 43



5 Transferring

In the transferring step as shown in Fig 44, a strong electrical charge draws the toner off the drum on to the paper. This is the first step that takes place outside the cartridge and the first step that involves the paper. The transfer charging roller puts a positive charge on the paper to pull the toner from the drum on to the paper. Then the static charge eliminator weakens the charges on both the paper and the drum so that the paper does not stick to the drum. The stiffness of the paper and the small radius of the drum also help the paper move away from the drum and toward the fusing assembly. Very thin paper can wrap around the drum.

6 Fusing

The fusing step uses heat and pressure to fuse the toner to the paper. Up to this point, the toner is merely sitting on the paper. The fusing rollers apply heat to the paper, which causes the toner to melt, and the rollers apply pressure to bond the melted toner into the paper. The temperature of the rollers is monitored by the printer. The fusing roller contains two quartz-halogen lamps that provide heat for the fusing process. Fusing temperature is monitored by the DC Controller PCA through a thermistor. The DC Controller maintains a temperature of about 190° C during print mode. If the fusing system over heats (about 230°C), then the Thermistor opens, interrupting power to the fusing heater, causing a FUSER ERROR to appear. If the fusing system exceeds the safe temperature, the thermal fuse opens, cutting off the power from the fuser. (Fig 45)

Fig 44

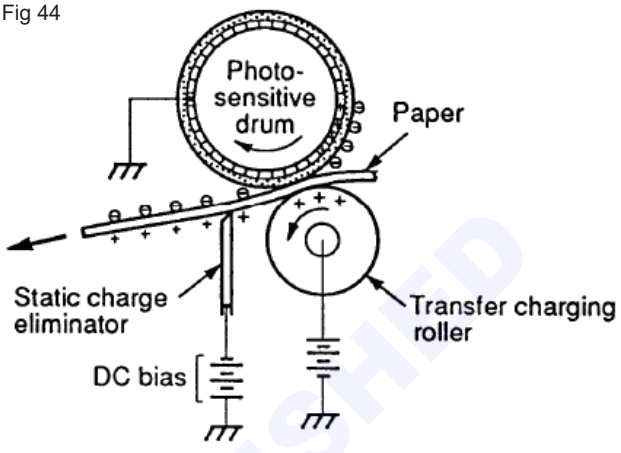
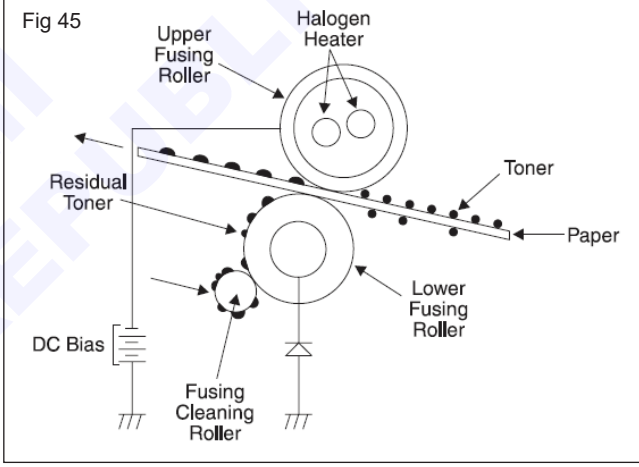


Fig 45



Parts of a Laser Printer

Fig 46 shows the cross section of a typical Laser Printer.

Multipurpose tray: Multipurpose tray is used to load Special media, such as OHTs, labels, and envelopes.

Cassette: The cassette is used to stack paper for uninterrupted printing. The capacity of the cassette varies from printer to printer and the size of the media also varies accordingly.

Separation pads: The paper is separated from any excessive sheets of paper by the separation pad and fed to the registration roller. Separation pad prevents multiple sheets from being fed to the registration roller. Fig. shows a typical separation pad used in laser printer.

Pick-up roller: Pick-up roller is used to pick-up the paper sheet by sheet from the multipurpose tray or cassette. The number of pick-up rollers depend upon the number of cassettes or trays present in the printer. The pick-up roller makes one rotation to pick up paper in the cassette or multipurpose tray. Any excessive sheets are

removed by the separation pad, and a sheet of paper is sent to the printer.

Registration shutter: Registration shutter removes the skew in the paper fed by the pickup roller.

Registration roller : The paper reaches the registration roller after its skew is corrected by hitting the registration shutter.

Toner cartridge: Toner cartridge consists of toner powder, OPC drum, Primary charge roller, developing cylinder or mag roller, Doctor Blade, wiper blade etc. Image formation takes place in the toner cartridge.

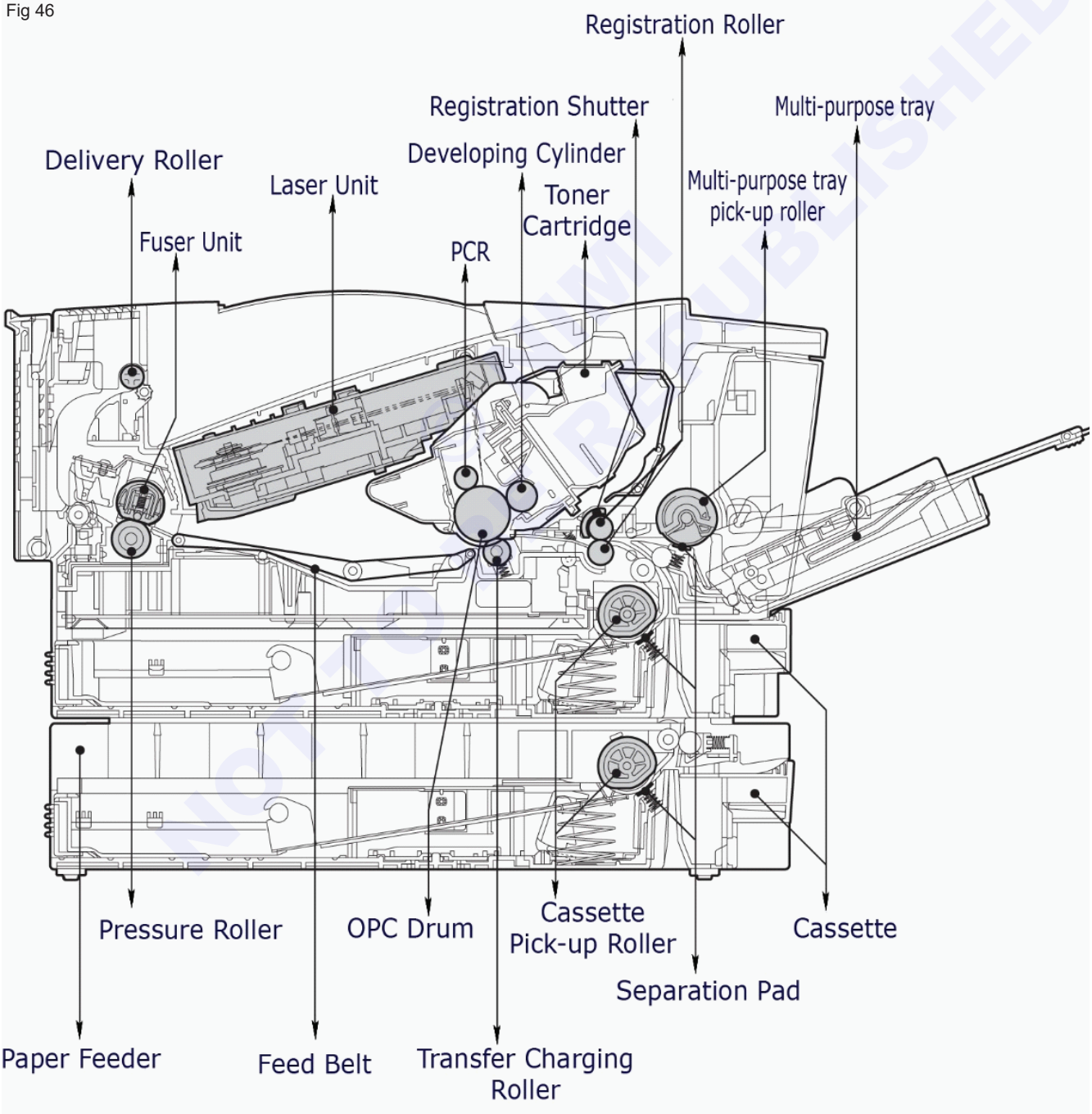
Transfer charging roller: It helps in transferring the image formed on the OPC drum to the paper. The paper travels in between the transfer charge roller and the OPC drum. In order to smoothen the Toner transfer from the OPC drum to the paper the Transfer charge roller is oppositely charged to the OPC drum.

Laser unit: The laser unit consists of the laser driver unit, scanning motor, scanning mirror, lens system, reflecting mirror and laser beam detector mirror. The Laser unit produces the laser beam responsible for writing the image on the OPC drum.

Feed belt: Helps in smooth motion of paper from the image formation stage to the fusing stage without the formed image getting distorted.

Fuser unit: The function of this unit is to permanently fix the toner image onto the paper. This is achieved using a temperature controlled heating unit.

Fig 46



Motors: The main motor gives the driving power to the printer mechanism.

Solenoids: Solenoids used in Laser printers are paper Feed solenoid, Duplexing unit solenoid. Paper feed solenoid transmits the driving power from the main motor to the paper feed roller through the paper feed clutch.

Clutch: Registration clutch, Paper input unit feed clutch, Tray 1 feed clutch are some of the clutches used in laser printers.

Sensors: Paper feed sensor, Paper level sensor, Paper out sensor, Fuser delivery sensor, Cassette select sensor and Output bin full sensor are some of the sensors used in laser printers.

A toner cartridge is used in the laser printing process. The toner cartridge has a rigid plastic housing that is replaceable, recyclable, and reusable. It consists of the following parts. (Fig 47)

1 Toner hopper with Toner powder

2 Stirring blade

3 Developer blade

4 Developer roller

5 PCR (Primary Charge Roller)

6 Organic photo conductive drum (OPC Drum)

7 Cleaning blade

8 Waste hopper

1 Toner hopper

Toner is stored in the hopper. Toner powder is a fine, dry mixture of plastic particles, carbon, and black or other coloring agents that make the actual image on the paper.

2 Stirring blade

As the cartridge rests between prints, the toner settles. The weight of the toner particles cause them to sink while the air is forced out, or rises. When printing, it's important to have air circulating so the toner moves freely. Cartridges include a set of stirring blades that keep the toner fluffed up and flowing freely inside the cartridges during all printing operations. After selecting print, the initially settled toner is stirred in the developing unit and pushed towards the developer roller as it is aerated and partially charged.

3 Developer blade (Doctor blade)

As toner accumulates on the developer roller, the toner passes under the developer blade which sheers a layer of toner off to a consistent height. During this process, a charge is generated on the toner before it transfers to the OPC drum. The toner charging occurs through the process of mixing in the hopper and being rubbed by the developer blade as the roller rotates. This process of charging the toner is called tribo-charging. Toner acts as a lubricant on the developer blade to prevent streaks, noise and other defects.

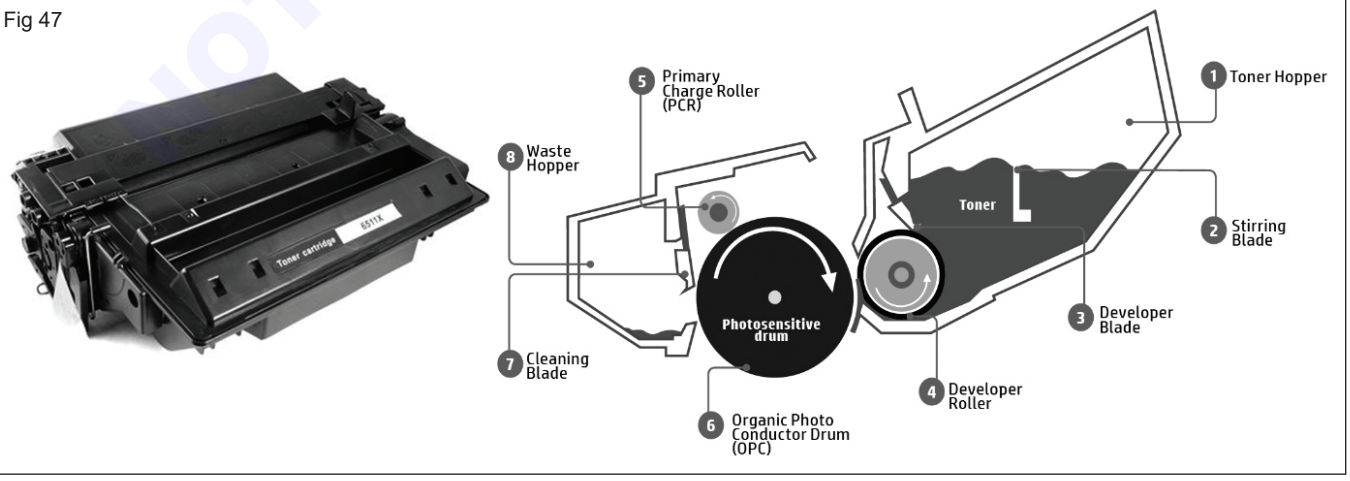
4 Developer roller (Mag roller or Mag sleeve)

Magnetic Roller consists of a metallic cylinder that rotates around a fixed magnetic core. It is usually referred to as the magnetic roller or "mag" roller. Mag Roller assists the transfer of toner from the reservoir onto selected areas of the OPC drum. This roller has a magnetic sleeve that attracts toner particles on to its surface and transfers them to the OPC. The amount of toner on the roller is controlled by the developer blade, which uses pressure to keep the amount of toner constant and causes a static charge to build on the toner. As the developer roller rotates, the toner is "pushed" toward the OPC. Thin seals are used along the roller and around the gears to prevent toner from leaking.

5 Primary charge roller (PCR)

PCR is a solid multi-layered rubber roller with a metal core which applies a uniform charge on the OPC drum to prepare the drum to receive a new image. It is located beside the OPC drum. During the printing process, a high voltage is applied across the PCR and it rotates against the drum there by coating the light sensitive surface with a negative electrostatic charge. With usage, the surface of the rubber roller can wear or be damaged by contaminants. Any damage to the PCR can result in subsequent damage to the surface of the OPC drum since the two surfaces rotate in contact with each other.

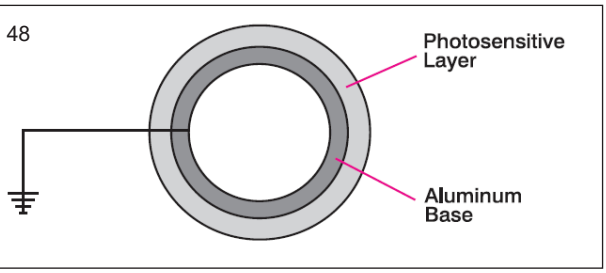
Fig 47



6 Organic photo conductor drum (OPC, or Imaging drum)

The OPC Drum is a thin walled aluminum cylinder coated with a layer of non-toxic, organic-photoconductive (OPC) material which becomes electrically conductive when exposed to light. The aluminum base of the photosensitive drum is electrically connected to ground potential. (Fig 48)

Fig 48



OPC drums help electrical conduction, meaning they serve as a receiver of the negative charge needed to transfer the toner to the paper. Each drum has three coating layers that serve different purposes and are all made from environmentally-friendly, biodegradable materials.

UCL (Undercoat Layer): This layer serves as a glue between the aluminum and inner-most layer.

CGL (Charge Generation Layer): This is a thin layer, 50 times thinner than an average piece of hair, that aids in the print speed and determines the color of the drum.

CTL (Charge Transport Layer): The outer, transparent layer of coating that allows the laser to strike through the CGL. This will define the acceptance of electrical charge and ultimately the life of the drum, as it is exposed to the elements, including paper, rollers and toner. OPC drums get easily too damaged. Do not touch it with your fingers or expose it to bright lights. Cleaning should be done only in a dimly lit, temperate area and do not use oils or other cleaning products. When the OPC drum starts to get worn, prints will be lighter. If it is damaged with a scratch, for instance, printed pages will start having black marks on them.

The laser strikes the OPC surface, creating an image one line at a time. The toner is then transferred from the surface of the OPC to the paper by the transfer roller. This process applies a positive charge to the underside of the paper which attracts the negatively charged toner from the OPC pulling the toner image onto the paper. The paper has the toner image electrostatically held in place and is now passed to the fusing unit, within the printer, where toner is permanently fixed to the paper by applying heat and pressure. OPCs are designed to work in combination with the printer's laser and other cartridge components (toner, developer roller, PCR, cleaning blade). Most drums will rotate 3 times to cover a single letter size page. This means that only 1/3 of the image can be placed on the drum at one time.

7 Cleaning blade (Wiper blade)

The wiper blade is a polyurethane strip that rides against the length of the drum and covers the waste bin. As the drum rotates with the 1/3 of a page image on it, and places the image on the paper, some of the toner is still left on the drum and must be cleaned off before the next 1/3 of the image can be placed on the drum. If it is not cleaned off, the first 1/3 of the image will be repeated in a ghost-like background of the second 1/3 of the image, and the second 1/3 of the image will also be repeated in a ghost-like background of the third 1/3 of the image. The wiper blade prevents this from happening. The edge of the wiper blade is precision sharp and smooth. The toner acts as a lubricant on the cleaning blade to prevent damaging the OPC and aids in thoroughly cleaning the inside of the cartridge. As the wiper blade scrapes the toner from the drum, it drops it into the waste bin. Because the toner in the waste bin has been charged, it can no longer be used.

8 Waste hopper

Toner particles left behind and other debris picked up during transfer are deposited in the waste hopper after they are scraped off by the cleaning blade.

Toner refilling is the practice of refilling empty laser printer toner cartridges with new toner powder. This enables the cartridge to be reused, saving the cost of a complete new cartridge and the impact of the waste and disposal of the old one.

Types of toner cartridges

Genuine or OEM

Genuine - also known as "original equipment manufacturer" (OEM) are cartridges sold by the printer manufacturers. Manufacturers offer certain guarantees when genuine brand toner are used in the printer. Genuine cartridges are more expensive than refills, compatibles or re-manufactured cartridges.

Compatible

Compatible - also known as "generic" or "alternative brand" are cartridges are manufactured from scratch, they are not used cartridges that have been refilled or re-manufactured. They are produced by third party companies and sold under different brand names. Often compatible cartridges may vary slightly in look, design and page yield to their genuine corresponding items due to certain patents that restrict the exact copying of designs. Although these generic cartridges may be less reliable, they may be a cost-effective alternative to the genuine article.

Remanufactured

Remanufacturing involves a process by which the toner in an OEM or compatible cartridge which has been used only once is refilled. Any worn out or defective parts are replaced and the cartridge is cleaned and then it is refilled with toner. The remanufacturing process differs from person to person, as well as the quality of toner that the cartridge is filled with. Re-manufactured toner cartridges can lead to leaking, printer malfunction, or even damaging the printer altogether.

Replacing a toner cartridge

Toner cartridges should be replaced when the existing Toner is not able to give good quality complete print outs. For replacing the Toner cartridge open the front cover of the printer and remove the existing cartridge gently using the handle provided. Exercise caution that no toner gets spilled inside the printer due to mishandling of the toner cartridge. Place the removed cartridge in a recycling bag. Remove the new cartridge from its package. To prevent damage to the print cartridge, minimize its exposure to direct light by covering it with a sheet of paper and hold the print cartridge at each end. Be careful not to touch the imaging drum on the bottom of the print cartridge. Smudges on the drum can cause print-quality problems. Pull the tab at the side of the cartridge until all the tape is removed from the cartridge. Put the tab in the print cartridge box to return for recycling. Gently rock the toner cartridge from front to back to distribute the toner evenly inside the cartridge. Insert the print cartridge in the device and close the print cartridge door. If toner gets on the clothing, wipe it off with a dry cloth and wash the clothing in cold water. Hot water sets toner into the fabric.

Troubleshooting defects in toner cartridges

1. **Back ground grey streaks:** Caused by a dirty PCR roller or worn out wiper blade.
2. **Light print:** dirty or worn out Magnetic roller or worn out doctor blade.
3. **Solid black pages:** Bad drum ground contact from the drum axle shaft to the contact gear inside the drum.
4. **Straight thin black lines down the page:** scratched Drum.
5. **Black dots repeating every 3":** Bad drum or something is struck up on the drum.
6. **Dark black horizontal lines:** Bad PCR connection.
7. **Tire tracks:** Worn out drum.
8. **Half the page prints and other half is blank:** Cartridge pin not fitted properly on one side or Tension spring not fitted properly.

Power supply

The power supply for a laser printer is divided in to two section, low voltage power supply and high voltage power supply. The AC and DC power supply circuits are contained in the Low Voltage Power Supply (LVPS). The high voltages required for image formation are generated by the High Voltage Power Supply (HVPS).

LVPS

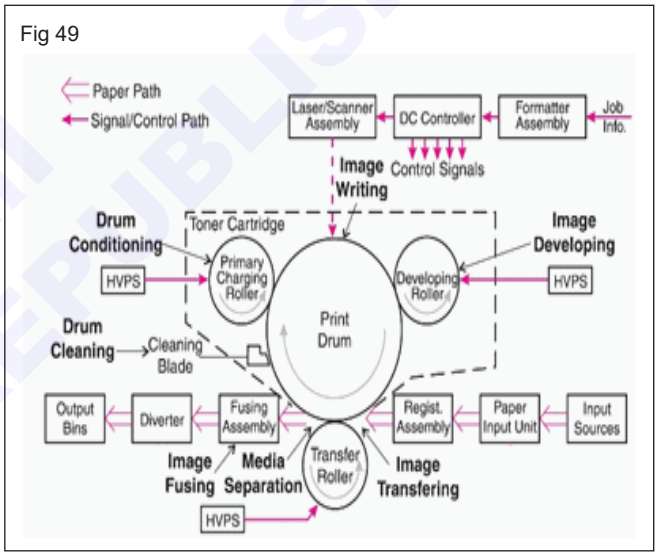
The AC power circuitry supplies AC voltage whenever the power cord is connected, and the power switch is on. A toner cartridge must be installed and the top access door must be closed before AC voltage is supplied to the DC power circuits or the fusing assembly. To prevent damage due to over current or over voltage, some printer LVPS has a resettable circuit breaker which shuts off AC input power to the LVPS in case of an AC over current condition. To reset, remove the LVPS and press in the circuit breaker button.

The blocks in a Low voltage power supply of a Laser Printer. The AC line voltage for the printer is applied through the main switch and supplied to the low-voltage power supply circuit through the fuse. The low-voltage power supply divides the AC voltage to +24 VDC, +5 VDC and +3.4 VDC and supplies them to the DC controller PCA. This circuit generates a zero-cross signal and supplies it to the DC controller PCA. +3.4 VDC is supplied to ICs on the DC controller PCA and the BD PCA. +5 VDC is supplied to the laser driver PCA and sensors. +24 VDC is supplied to the high-voltage power supply PCA to drive the main motor.

HVPS

High voltage is required in laser printing to create electrostatic charges. A typical printer is making pre-charge, developer bias AC bias and transfer voltages. A series of voltages are applied around the photoconductive drum. (Fig 49)

Fig 49



Pre-charge: Negative charge around 600V in the photoconductive OPC drum.

Illumination: The optical source (laser) discharges some areas. Most systems are write-black, the laser discharges areas that are to carry toner powder. In a write-white system the laser discharges areas that will not carry toner. The OPC now carries a "latent image" in varying static charges.

Developer: Around 600V negative charged toner powder.

Transfer: Positive charge to conductive rubber transfer roller carrying a positive charge. Static Eliminator - A charge is effected on the fuser rollers to prevent the toner shifting High voltage power supplies typically use a transistor inverter, a small transformer and often have a diode or capacitor ladder to follow.

The HVPS doesn't usually step up a mains voltage. Instead it tends to work from the 24 to 36 Volt DC supply used for motors. This provides a better regulated supply that can be turned on and off by simple transistor circuits

and that can run at a high frequency - perhaps a hundred kilohertz. The transistor starts a condition, creating a magnetic field in the transformer core. The rise of the field shuts the transistor down and the field collapses restarting the process. The other winding of the transformer core has many turns so the alternating field from this side is at a high voltage. This AC is rectified back to DC with a diode and capacitor.

Voltage multipliers are used to double or quadruple the output, allowing the transformer to be considerably smaller. The diodes charge the capacitors in parallel but they add up in series making the higher voltage. Colour laser printers can need three or four voltages for each colour.

Voltage measurement

To measure voltages which might exceed 600 a high voltage probe is needed. A typical handheld test meter has a maximum input voltage of 600 and anything greater is quite likely to damage the meter. A few meters have a maximum of 1,000 volts but laser printers typically produce more than that - up to 3,000 volts is quite normal and higher voltages perfectly possible. These voltages are much greater than test meters are intended for and could possibly break down the insulation of the meter risking the user's life Fig 50 shows the voltage measurement tool used in the printer.

Fig 50

High voltage probes are the way to pre-scale the voltage to fit a meter range. A high voltage probe is just a couple of resistors making a voltage divider to pre-scale the signal (say 95 mega ohms in series with a 1 mega ohm resistor to ground. Together with the meters typically 10 mega ohm resistance this gives a 100 to 1 pre-scaling. High voltage resistors need to be used - ordinary low voltage resistors could break down and arc, at the least damaging the meter and at worst proving fatal. Grounding of the test probe needs to be done properly. It's typically a crocodile clip.

The functions of a laser printer can be divided in to 6 blocks, the engine control system, laser exposure system, Image formation system, pickup and feed system, fixing and delivery system, external and control system.

Pickup and feed system

When the paper feed solenoid is turned on, the driving power from main motor(M1) is transmitted to the paper feed roller through the paper feed clutch(one way clutch), then, the paper feed roller rotates. At the same time, the push down cam also rotates, then, the tray lifting plate stands up. The paper in the tray is carried into the printer by the paper feed roller. Separation pad method is used in order to separate each paper and prevents of feeding the second paper together.

Paper empty sensor or Pre feed Sensor

Paper empty sensor is mounted at the upper parts of the multi paper feed tray and detects if there is any paper in the tray or not.

If there is a paper in the tray, actuator stands up and the sensor goes to OFF condition. Also, if there is no paper, actuator falls into the hole of tray, and the sensor goes to ON condition. The placement of sensors and switches in a typical laser printer.

Paper Width Sensor

The paper-width sensor senses the width of the media.

Paper-delivery sensor or Fuser Delivery Sensor

The paper-delivery sensor senses when media has successfully moved out of the fusing area.

Top-of-page sensor

The top-of-page sensor detects the leading and trailing edges of the media. It synchronizes the photosensitive drum and the top of the media.

1 Left width sensor,

2 Top of page sensor,

3 Right width sensor flags

Output-bin-full sensor

The output-bin-full sensor signals that the bin is full. Fig shows the output bin full activator flag in a typical laser printer.

Image-formation system

Laser printing requires the interaction of several different technologies, including electronics, optics, and electro photographics, to provide a printed page.

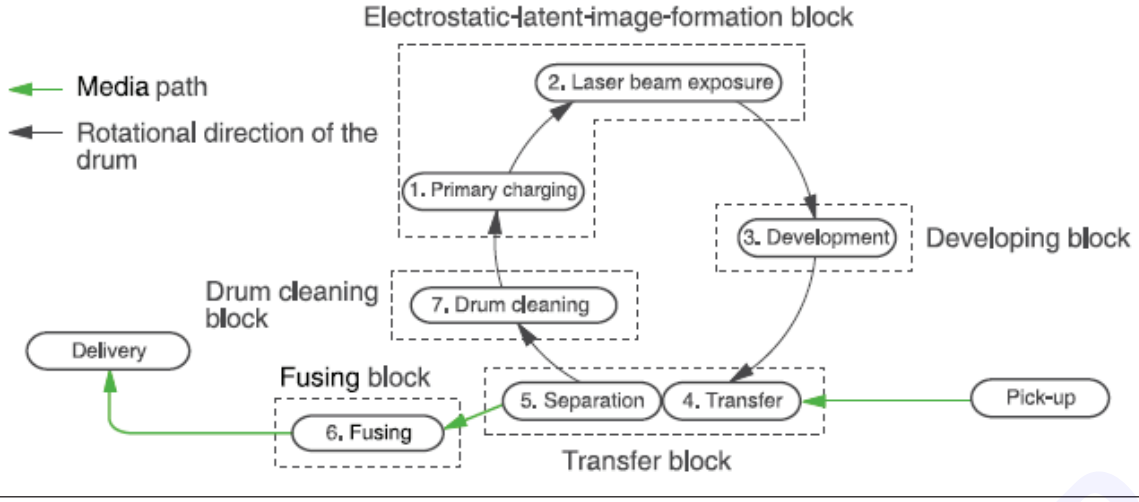
Each process functions independently and must be coordinated with the other device processes. Image

formation consists of the following five processes:

- Electrostatic latent-image formation
- Developing
- Transfer
- Fusing
- Drum cleaning

The five processes contain eight steps, which are shown in Fig 51.

Fig 51



Inkjet printer

Inkjet printers are composed of the following main sections.

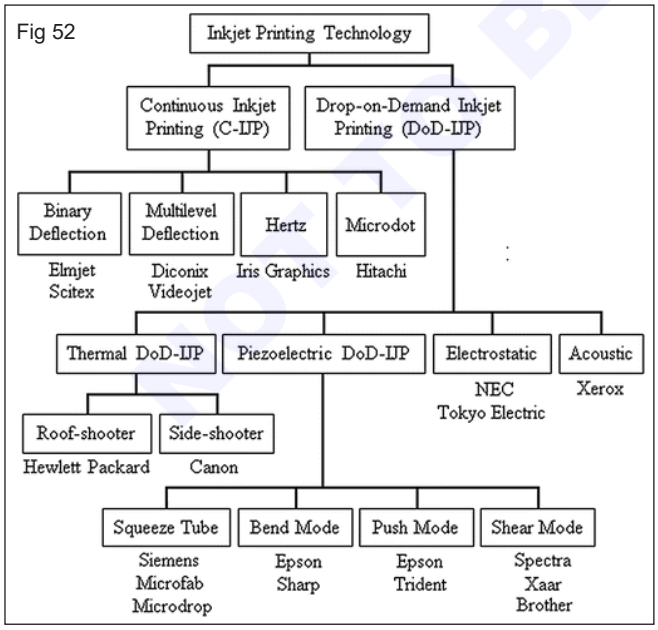
- Ink reservoir
- Ink circulation system
- Droplet generation and acceleration system
- Droplet guiding system.

Depending on the drop generation method, three types of inkjet printers are used:

- Continuous jet;
- Intermittent jet;
- Drops-on-demand.

Fig 52 shows the classification of Ink Jet Printing Technology and the technology adopted by different manufacturers.

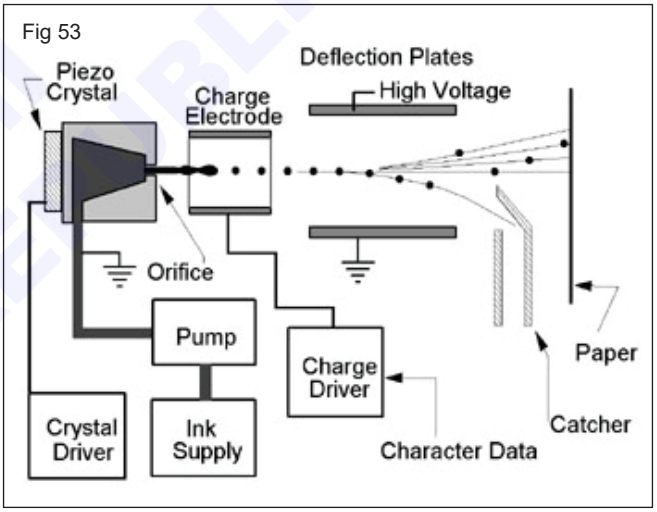
Fig 52



Continuous jet printer

The droplet generation head is continuously supplied with ink under pressure by a pump. Cone-shaped nozzles are used with diameters of the order of tenths of microns, usually made from ceramic materials resistant to wear and tear. (Fig 53)

Fig 53



Due to the superficial tension, the jet tends to separate into independent droplets. This process is forced by varying the pressure on the back of the nozzle with a piezoelectric crystal. Consequently, a mechanical vibration of the ink reservoir casing is produced; if this vibration is continuous, the droplets will be generated continuously.

In addition to this piezoelectric method of droplet generation, the thermal method can also be used.

In order to guide the droplets, they are charged electrostatically with electrodes placed in the area of droplet separation. Since the inkjet is electrically connected to ground, the droplets formed are charged with a polarity opposite to that of the positive electrode. After separation, the droplets maintain their charge.

The voltage of charging electrodes is controlled by the image generation block. The charge of a droplet should vary between limits largely enough to allow later deflection over the required distance. The maximum charge is limited by the need to avoid electrostatic rejection of neighboring droplets and droplet "explosion", which may occur if the electrostatic rejection forces inside the droplet exceed the superficial tension.

The ink used should be chemically stable and compatible with the materials used for building the printer; likewise, it should be conductive, non-toxic, and non-inflammable. To prevent the ink from drying in the nozzles, additives are mixed into the ink and filters are inserted into the ink circulation system.

Continuous jet printers allow to achieve high frequencies for droplet generation of over 100,000 droplets per second and high speeds of the inkjet. A good printing quality is achieved if the droplets have small size and the resolution is high. At a certain maximum generation frequency, in creasing the resolution will reduce the printing speed. Conversely, if the printing speed is increased by increasing the droplet generation frequency, the resolution will be decreased.

Color inkjet printer

In color inkjet printers, the speed of color printing is much slower than that of monochrome printing. This is because, mostly, there are no separate print heads for each of the primary colors, but a single print head for the color inks. Usually, color printers have a separate print head for the black ink. Monochrome printing is performed on a width of 56 dots, while color printing is per-formed on a width of 16 dots. Printing a line of color the same width as one in monochrome requires multiple passes.

To increase the range of pure colors that printers can generate, some manufacturers have designed six-color inkjet printers. These printers use two additional inks beyond the four common inks. Generally, the additional colors used are orange and violet. This results in a more realistic reproduction of photographs and less need to use other techniques for color ex-tension, such as dithering.

Printing quality for inkjet printers in general, and color printers in special, is deter-mined to a large extent by two elements: ink quality and paper quality. There are two types of ink that are used. The first type is slow-drying and it is used for monochrome printers. The second type is fast-drying and it is used for color printers. On these printers, since different inks are mixed, they need to dry as quickly as possible to avoid color alteration by merging of adjacent dots.

In general, the inks used for inkjet printers are based on pigments diluted in water, which may create some problems.

Generally, dye-based cyan, magenta and yellow inks are used, with small molecules (less than 50 nm). These have high brilliance and allow to achieve a large color range, but they are not enough water-resistant and fade-resistant in time. Inks based on pigments with larger molecules (between 50 and 100 nm) are more waterproof and fade-resistant, but they cannot deliver an enough range of colors and are not transparent. For that reason, currently these pigments are only used for the black ink.

Parts of an Ink Jet Printer

Print head assembly

- **Print head:** The core of an inkjet printer, the print head contains a series of nozzles that are used to spray drops of ink.
- **Ink cartridges:** Depending on the manufacturer and model of the printer, ink cartridges come in various combinations, such as separate black and color cartridges, color and black in a single cartridge or even a cartridge for each ink color. The cartridges of some inkjet printers include the print head itself.
- **Print head stepper motor:** A stepper motor moves the print head assembly (print head and ink cartridges) back and forth across the paper. Some printers have another stepper motor to park the print head assembly when the printer is not in use. Parking means that the print head assembly is restricted from accidentally moving, like a parking brake on a car.
- **Belt:** A belt is used to attach the print head assembly to the stepper motor.
- **Stabilizer bar:** The print head assembly uses a stabilizer bar to ensure that movement is precise and controlled.

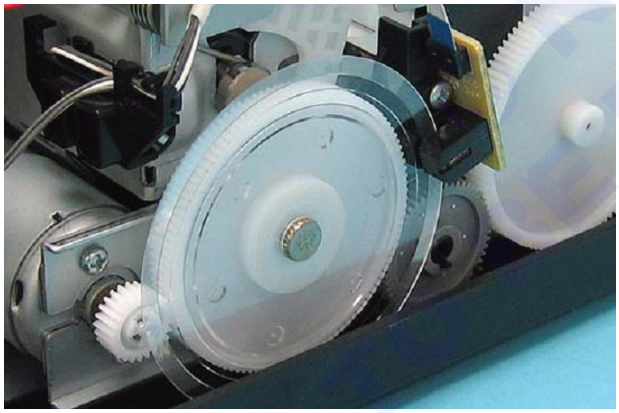
Paper feed assembly

- **Paper tray/feeder:** Most inkjet printers have a tray that you load the paper into. Some printers dispense with the standard tray for a feeder instead. The feeder typically snaps open at an angle on the back of the printer, allowing you to place paper in it. Feeders generally do not hold as much paper as a traditional paper tray.
- **Rollers:** A set of rollers pull the paper in from the tray or feeder and advance the paper when the print head assembly is ready for another pass.
- **Paper feed stepper motor:** This stepper motor powers the rollers to move the paper in the exact increment needed to ensure a continuous image is printed.
- **Power supply:** While earlier printers often had an external adapter, newer printers use a standard power supply that is incorporated into the printer itself.
- **Control circuitry:** Control circuitry in the printer controls all the mechanical aspects of operation, as well as decode the information sent to the printer from the computer.
- **Interface port(s):** Parallel port is still used in many printers, but newer printers use the USB port. A few printers connect using a serial port or small computer system interface (SCSI) port.

- Control Boards
- Logic Board
- Main Board
- Power Supply Board
- Sensors
- Cover Open Sensor
- Front / Rear Paper End Sensor
- Home position Sensor
- Cartridge Sensor
- Encoder Sensor

Encoder Strip / Disk: The purpose of the encoder strip is to help carriage assembly identify its position using a sensor located on the ink station. The Encoder sensor reads the small lines on the encoder strip and determines where it needs to print. Suppose if the encoder strip has 350 vertical lines in it, then the printer can always tell where the ink station is located, this is how the printer judges distances, 1 inch or 5 inches or the small spacing between letters etc. An Inkjet printer should always have a clean encoder strip for exact printing. After repeated usage ink will build up on the encoder strip over time causing the printer to misalign spacing along with potential printer failure. Fig 54 shows an Encoder disk used in inkjet printer.

Fig 54



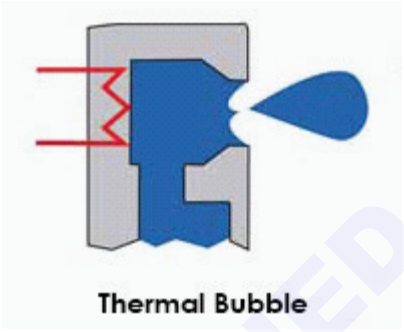
Ink cartridge

An ink cartridge or inkjet cartridge is a component of an inkjet printer that contains the ink that is deposited onto paper during printing. Each ink cartridge contains one or more ink reservoirs. Certain manufacturers also add electronic contacts and a chip that communicates with the printer. The print head and circuitry, which perform most of the work for the inkjet printer, are contained on the ink cartridge itself. There are many nozzles (jets) in the print head on the bottom of the cartridge. Each nozzle is smaller in diameter than a human hair. Under each nozzle is a heater (resistor) that heats the ink inside the cartridge. When the ink is heated, a bubble forms that bursts, shooting the ink through the jets onto the paper.

The resistors on most cartridges will continue to work until they burn out, about every sixth time the cartridge is recycled. This is the average, but not the rule. The reality is that up to 5 percent of all inkjet cartridges cannot be recycled even once, and some can be recycled many more than five times.

There are two main inkjet technologies currently found in inkjet printers: thermal bubble or bubble jet where tiny resistors create heat that vaporizes the ink to create a bubble. (Fig 55)

Fig 55



As the bubble expands, some of the ink is pushed out of a nozzle onto the paper and when the bubble collapses a vacuum is created which draws more ink into the print head from the cartridge.

A typical bubble jet print head has 300 to 600 miniscule nozzles all of which can fire a droplet simultaneously.

The printing depends on the smooth flow of ink, which can be stuck if the ink begins to dry at the print head, as can happen when an ink level becomes low. Dried ink can be cleaned from a cartridge print head used isopropyl alcohol or distilled water. Isopropyl alcohol will damage the printing head, melting the plastic at the connections and rubber gaskets. Distilled water and a lint-free cloth is best for cleaning print heads.

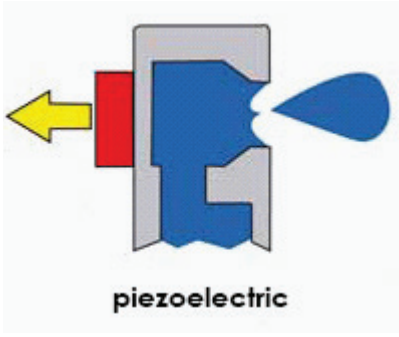
The ink also acts as a coolant to protect the metal-plate heating elements? when the ink supply becomes less, and printing is attempted, the heating elements in thermal cartridges often burn out, permanently damaging the print head. Cartridges should be refilled when the ink first begins to run low, to avoid overheating and damage to the print head.

In piezoelectric the Piezo crystals deform when an electric current is applied. They are found at the rear of the ink reservoir of the cartridge nozzles and each nozzle forces a tiny amount of ink out of the nozzle when the crystal receives a tiny electric charge that causes it to vibrate. There are two types of crystals used: those that elongate when subjected to electricity or bi-morphs which bend. Epson printers use this type of ink flow. (Fig 56)

Refilling inkjet printer cartridges

An inkjet refill kit is a set of tools and a certain amount of ink used to refill ink cartridges. The specific tools and the amount or type of ink depends on which cartridge the kit is designed for. Typically, a refill kit comes with a cartridge holder, bottles of ink and needles.

Fig 56



The refill process normally involves the following steps:

Injecting ink (Fig 57)

Fig 57

Depending on the type of cartridge being refilled, ink can either be injected through a hole on top of the cartridge, or directly into the ink chambers after the top has been opened up. The ink can be injected directly from a bottle (with a needle tip on it) or from a needle filled with ink. The ink must be slowly injected into the cartridge so as not to cause damage, or overfilling, or overflow to other-color ink reservoirs. For colors, a label on the cartridge might have three ordered color-dots to indicate the corresponding three ink colors of the reservoir chambers.

Installing and running: Once the cartridge is filled, the top is placed back on and the cartridge can be reinstalled in the printer. Some extra ink may flow from the cartridge print-head, which should be wiped or blotted with tissue paper. On some cartridges, the ink has a problem getting to the bottom of the cartridge, then it must be forced to the bottom either by suction through the jet plate or by putting pressure from the top with a syringe to expel the ink through the jet plate very gently. Fig 58 shows the Printer cleaning utilities on the refilled cartridge should be carried out in case any excess ink is left over from the refilling process.

Print-head cleaning: Sometimes the ink flow might be blocked by dried ink on the ink cartridge print-head. For color cartridges, typically one ink-color fails to flow due to dried ink. The dried ink can be cleaned using isopropyl alcohol (50% or higher) on a swab or folded paper towel rubbed gently three or four times across the print-head. Another method is to let the cartridge sit overnight in a shallow cup or glass of very warm clean distilled water. The water depth required is about .25 or .375"; remove and re-clean by wiping and blotting with tissue paper.

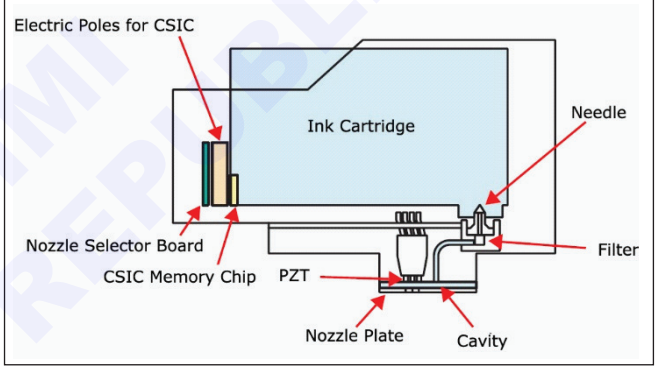
Fig 58

Inkjet printer is composed of the print head unit, paper feeding mechanism and carriage mechanism.

Inkjet printer head in epson printers

The print head mechanism consists of ink cartridges and print heads. Each print head is composed of PZT (Piezo Electric Element), nozzle surface, ink supply needle, nozzle selection circuit board, cartridge sensor, CSIC, and CSIC connection circuit. (Fig 59)

Fig 59



Ink cartridge

An ink cartridge stores ink to be supplied to the print head.

CSIC:

CSIC is a non-volatile memory EEPROM attached to each black and color ink cartridge. It keeps the following information:

1 Ink remaining level

2 Number of cleanings performed

3 Number of installation of the ink cartridge

4 Accumulated installation time of the cartridge

5 Model name of the printer in use

6 Ink cartridge production information print head

Piezo electric element (PZT)

The main board generates the drive waveform. Based on the drive waveform generated on the Main Board, the PZT selected by the nozzle selector IC on the

Print Head pushes the top of the ink cavity, which has ink stored, to eject the ink from each nozzle on the nozzle plate. Driven by the print signal from the control circuit board, it ejects ink from the nozzle plate.

Nozzle plate

The plate with nozzle holes on the Print Head surface is called Nozzle Plate. Ink pressured by the PZT is ejected from this plate.

Ink supply needle

Connects the ink cartridge and print head to run ink to the print head.

CSIC connection circuit

Connects the control circuit board and CSIC attached on the ink cartridge. One end of the harness is connected to the control board together with the print head cable.

Nozzle selection circuit board

This circuit, controlled by ASIC on the control circuit board, selects nozzles to be driven for printing. On the other hand, head drive voltage is produced on the controller circuit side.

Filter

There is a possibility of dirt or dust getting accumulated around the cartridge needle When the Ink Cartridge is installed, this dirt or dust around the cartridge needle is absorbed into the Print Head, which will cause nozzle clog and disturbance of ink flow, alignment failure and dot missing finally. To prevent this problem, a filter is set under the cartridge needle.

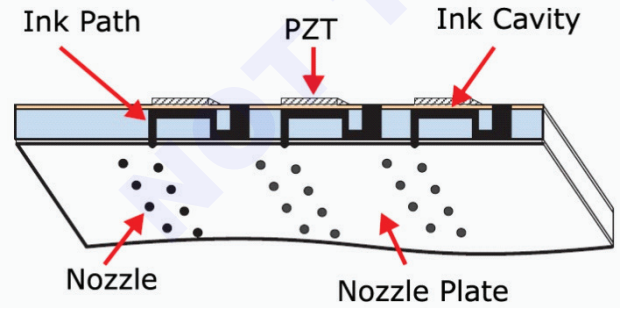
Ink cavity

The ink absorbed from the Ink Cartridge goes through the filter and then is stored temporarily in this tank called “ink cavity” until PZT is driven.

Printing process

Normal state: During normal state, no printing related signal is received from the main board. So no drive voltage is applied to the PZT and so the shape of the PZT does not change. Therefore the PZT does not push the ink cavity and the ink pressure inside the ink cavity is kept normal (Fig 60)

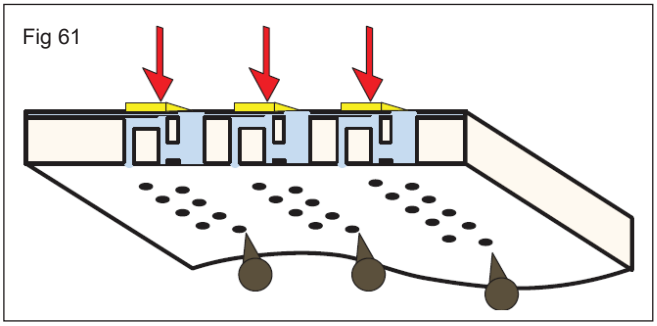
Fig 60



Ejecting state

When the print signal is output from Main Board, the nozzle selector IC located on the Print Head latches the data once by 1-byte unit. Based on the drive waveform generated on the Main Board, the PZT selected by the nozzle selector IC pushes the top of the ink cavity. The ink stored in the ink cavity is ejected from nozzles. (Fig 61)

Fig 61



Inkjet printer head in HP printers

HP cartridges uses thermal inkjet technology. Printer head is contained in the form of a disposable cartridge. Each cartridge has a small reservoir called as the firing chamber filled with a tiny measure of ink. This ink is heated with a thin-film resistor layered above the firing chamber. As the ink heats up, it expands to form a bubble. The bubble expands until it bursts, at which point the ink is forced through the nozzle located below the firing chamber and out onto the paper. This process is repeated up to 12,000 times per second, and creates residual heat in the resistor. A layer of silicon is placed above the resistor to cool it by transferring the residual heat away.

Cleaning print cartridges

Manual cleaning

If the printer is used in a dusty environment, a small amount of debris might accumulate inside the case. This debris can include dust, hair, or carpet or clothing fibers. When debris gets on the print cartridges and cradle, ink streaks and smudge smight appear on printed pages. Ink streaking is easily corrected by manually cleaning the cartridges and cradle.

For cleaning Distilled water and Cotton swabs or other soft, lint-free material that will not stick to the cartridges should only be used. Care should be taken so that ink does not get smeared in the hands or clothing. A removed print cartridge should not be left outside the printer for more than 30 minutes.

Do not wipe the nozzle plate. Touching the ink nozzles will result in clogs, ink failure, and bad electrical connections.

Automatic cleaning

Automatic cleaning of cartridges is done from the printer menu by the printer. Automatic cleaning can be done if the cartridge is not empty. If the printed page has missing lines or dots, or if they contain ink streaks, the print cartridge might be low on ink or might need to be cleaned. Unnecessary automatic cleaning wastes ink and shortens the life of the cartridge.

Certain printer manufacturers include a head cleaning utility along with the printer software.

In Epson printers the head cleaning is done by selecting “Head Cleaning” in the printer driver utility. The printer should be in stand by state before proceeding with head cleaning. The state of the printer can be verified using the Epson status monitor.

Working principle of Printer, Scanner and MFD

Objectives: At the end of this lesson you shall be able to
- **working principles of network scanner**
- **working principles of multifunction printer**
- **working principles of passbook printer**
- **working principles of high Speed printer**
- **working principles of line printer**
- **working principles of network printer**
- **working principles of print server.**

Image scanner

An image scanner is a device that optically scans images, printed text, handwriting, or an object, and converts it to a digital image. Some of the types of scanners are.

Drum scanner

Flat bed scanner

CCD based scanner

CIS based scanner

Film scanner

Roller scanner

3D scanner

Smart phone scanner using app

Drum scanner

Drum scanners use a technology called a photo multiplier tube (PMT). In PMT, the document to be scanned is mounted on a glass cylinder. At the center of the cylinder is a sensor that splits light bounced from the document, in to three beams. Each beam is sent through a color filter into a photo multiplier tube where the light is changed into an electrical signal.

Flat bed scanner

CCD - Charge Coupled Device scanner

The charge-coupled device (CCD) converts optical

images to electrical signals. A CCD usually has an array of cells to capture a light image by the photo-electric

effect. The CCD is a single chip photoelectric conversion device which consists of several thousand photo sensitive devices of each several microns square, for reading RGB image signals, with a built-in scanning circuit.

A 6-line CCD with two rows of staggered photo sensitive devices for RGB each. The 6-line CCD therefore can scan at 1200 dpi x 2 = 2400 dpi.

On a flat bed scanner using CCD technology, the light source, normally a cold cathode light, is reflected by the original, diverted by mirrors and gathered by a lens onto the sensor. This consists of light-capturing CCD elements. In some cases the CCD elements may also have a micro-lens in front of every photodiode to gather light more effectively. CCD technology allows a higher depth of field, higher scan speed and signal noise ratio and greater color accuracy.

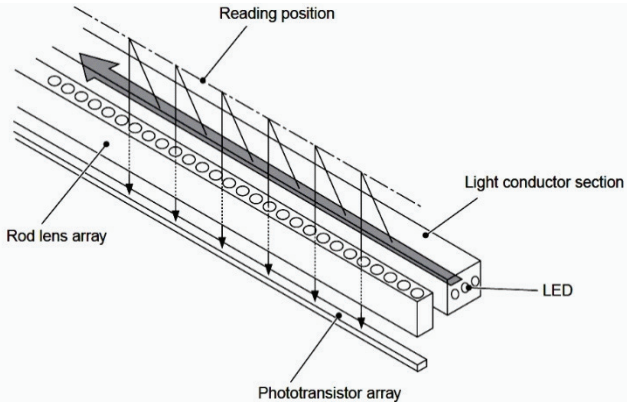
CIS - Contact Image Sensor scanner

In contact Image Sensor technology, the light from RGB (red, green, blue) LEDs called the light conductor

section are reflected by the original at the end of the glass part. Light is sent directly through an array of lenses to the image sensor which can be either CCD or CMOS.

When the LED is turned ON, the LED light is supplied to the light conductor section which exposes a document. That is, the LED light indirectly exposes a document through the light conductor section. This is called LED Indirect Exposure. The light reflected from the document is collected by the phototransistor array through the rod lens array and is read as an image signal. (Fig 1) shows the outline of contact image sensor.

Fig 1



Power consumption is less in CIS based Flat Bed Scanners.

Scanner functioning

The scanner functions are divided into

- Optical system
- Image processing system
- Control system.

Optical system

The optical system consists of the scanning lamp, lens and mirrors. When scanning a reflective document, the scanning lamp in the scanning unit exposes the document and focuses the reflected light from the document on the light-sensitive device via the lens and mirrors. A lamp is used to illuminate the document. The lamp in newer scanners is either a cold cathode fluorescent lamp (CCFL) or a xenon lamp, while older scanners used a standard fluorescent lamp. When the scanner is powered on, or the host computer sends a scan command, the Application-specific integrated circuit (ASIC) turns the scanning lamp lighting signal ON to light the scanning lamp.

The reflected light from the document is focused on the light-sensitive device via the mirrors and lens unit. A built-in timer to be set by the device driver is counted during lamp ON and turns the scanning lamp OFF when no scan command is sent for a certain period. (Fig 2)

Fig 2

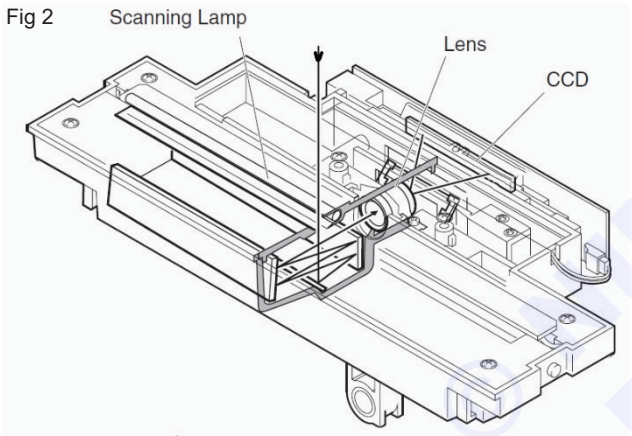
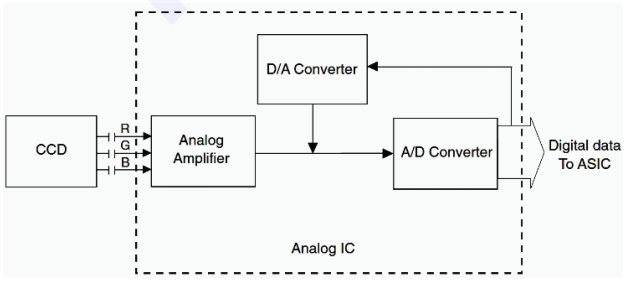


Image processing system

Output signal from the CCD /CIS is an analog signal which cannot be used as image data. So RGB output signal from the light sensitive device is amplified by analog amplifier to generate analog data. The generated data is converted into averaged analog signal by D/A converter, then got feedback to the A/D converter to output constant digital data to the ASIC - Application-specific integrated circuit.

Fig 3 shows the blocks in the Image Processing system of the scanner.

Fig 3



1 D/A converter

D/A converter removes un-uniform analog data generated by the CCD. It adjusts CCD output to keep max. 5V of input signal to the A/D converter, to make the black level of the image constant.

2 A/D converter

The A/D converter converts the black-level-corrected image signal (analog signal) to a 16-bitimage data.

(Digital signal) in the order of red, green and blue image signal.

5V is applied to the Vcc terminal and reference voltage is applied to the Vref terminal. A/D converter outputs "0" when input signal is 5V, and outputs "255" when input signal is reference voltage. This converts 1 pixel signal into the image data of 65536 gradations for red, green and blue each.

Network scanner

A network scanner is a software tool that scans the entire network and its nodes for the following:

- Identify connected devices
- Find possible loopholes
- Scan, assess, and evaluate the strength of the network

It is an essential component of network scanning that allows the admin to gather information about the network and its endpoints. Regular network scanning helps the system with the following:

- Maintenance
- Management
- Monitoring
- Security assessment

Working principle of Network Scanner

Network scanning identifies and examines the state as well as the interaction of all the active hosts connected to the network. It then maps them to their IP addresses.

- A packet or a ping is sent to a range of IP addresses, automatically or manually specified by the admin.
- All the hosts that respond to the packets are considered active, while the rest are labeled inactive.
- The responses received are scanned by the software and checked for inconsistencies.
- If any anomaly is detected, it's reported to the manager.

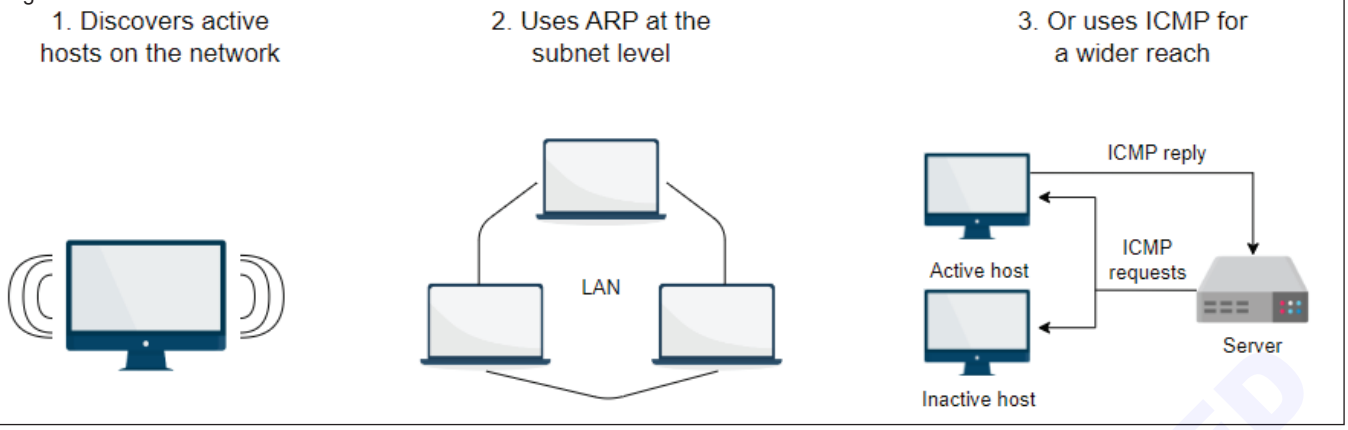
Note: Nmap is network scanning tool that uses IP packets to map the devices attached to the network.

Protocols

Numerous protocols can be used in network scanning depending upon the administration and network requirements. Following are some of the protocols:

- **Address Resolution Protocol (ARP):** Administration can manually ping the subnet using an ARP scan.
- **Internet Control Message Protocol (ICMP):** We can map the network topology using ICMP. (Fig 4)

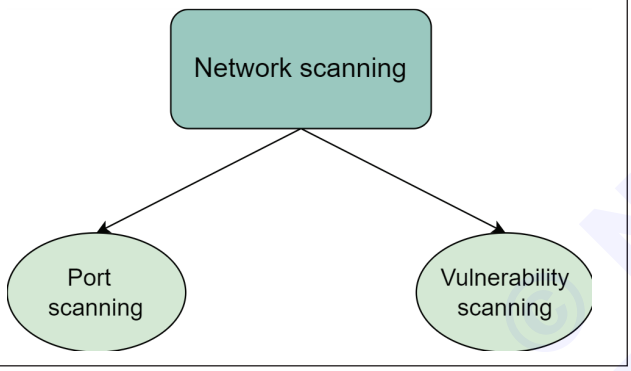
Fig 4



Components

Network scanning has two components-port scanning and vulnerability scanning. (Fig 5)

Fig 5



Port scanning

The network scanner sends data packets to a specific service port number. This helps in identifying network services available for the particular system.

Data received from the active hosts are used to assess the security levels of an organization.

Vulnerability scanning

The network scanner identifies weak spots and vulnerabilities in the operating system and application software in this scan.

Note: Cyber criminals use network scanning to identify loopholes in the system and prepare for an attack accordingly.

Benefits of network scanning

- It allows the organization to stay aware of the available UDP and TCP services.
- It allows the organization to identify and protect against cyberattacks.
- It allows the organization to increase network performance.
- It allows the organization to identify the filtering systems being used between the nodes.
- It allows the organization to access the operating systems of active devices through their response.

Multi-Function Printer (Fig 6)

Fig 6

An MFP (Multi-Function Product/ Printer), or Multifunction Device (MFD) or multifunction copiers(MFCs) includes the functionality of multiple devices in one. A typical MFP may act as a combination of some or all of the following devices.

- Email
- Fax
- Photocopier
- Printer
- Scanner
- Networking

According to usage MFP can be categorised as home use and office use or both. MFPs intended for home use are mostly inkjets, which provide better photo quality than lasers. They also provide photo-friendly features such as LCD preview screens and the ability to print photos from USB thumb drives, memory cards, and

cameras. For home photo Lab use photo-lab MFPs are also used.

In office use more text is printed than photos, which means a laser or laser-class printer can be preferred to ink jet printers equipped with office-centric features like ADF and fax modem.

Features of Multi-Function Printers

Printing

A MFD should be capable of printing from a computer or independently using USB thumb drives, memory cards and cameras. Printer can be a Laser or an Ink jet printer depending upon the needs as stated above. The maximum and minimum size that can be printed is also an important feature to be considered. Nowadays a number of inkjets are faster than many lasers. Inkjets usually offer superior photo quality. Lasers still are generally faster than a typical inkjet, have greater paper capacity, the ability to handle higher-volume printing, lower running costs, and better text quality. Colour printing can be done using colour laser or colour ink jet capable MFPs.

Scanning

MFPs should be capable of scanning documents to the system directly through USB or through networked systems. Most MFPs include flatbeds suitable for scanning photos or single-sheet documents. A flatbed scanner, on the other hand, requires each page to be individually placed on the scanning surface. While this is convenient for single pages, copying more pages would require a lot of manual page-loading.

ADF

An Automatic Document Feeder (ADF) is used in copiers and scanners to feed pages into the machine. It allows multiple pages to be copied or scanned at one time without the need to place each individual page in the copier or scanner. For MFPs with letter-size flatbeds, an ADF helps in scanning legal-size page. Some ADFs have duplex function i.e. scanning both sides of a page.

Copying

MFPs are capable of taking Photostat copy of a document with the help of the system or independently. A copy function button is included in the machine to fulfil this option.

FAX

A fax feature includes standalone faxing, which can be controlled through the MFP's keypad or a PC Fax function i.e. faxing documents directly from the PC without having to print them first. PC Fax can be in the form of a fax utility, a fax driver that can be used like a print driver, or both.

Email

Email features also come in two forms. Direct email scans and sends an email directly to the Internet service provider (ISP) or an in-house email server on the network. The more common choice for low-end MFPs is to open an email message on a PC and add the scanned document as an attachment. MFP can offer either or both kinds of email. Some direct email features will not work with all ISPs.

Duplex scanning and Printing

MFPs that support duplex scanning do so by scanning one side of the document, turning it over, and then scanning the other side, but some provide one-pass.

scanning i.e. scanning both sides of the page at once, which is much faster. Some MFP includes a print duplexer, the combination will usually let you copy both single- and double-sided originals to your choice of single- or double-sided copies.

Multifunction Printer Working principle

The multifunction printer is cutting-edge, practical, and convenient. It simplifies life. But what is it exactly, and how does it work?

These efficient machines can make a significant impact in your life, whether at home or at work. However, the more you understand how they work, the better you will be able to get the most of your machine and maximize your everyday efforts.

Here's an overview of the multifunction printer and its amazing technology.

Working Principle of MFD

1 Printing Function

The core function of an MFP is printing, as the name implies.

MFPs may use either inkjet or laser technology, each with a unique operation process.

Inkjet printers print by spraying small droplets of ink onto paper.

The printer's control system directs the print head where and when to release the ink based on the document's data.

On the other hand, laser printers use a laser beam to produce an image on a photosensitive drum.

The image attracts toner particles, which are then transferred onto the paper through heat and pressure.

2 Scanning Function

Scanning is another crucial feature of MFPs.

The scanner uses a light source (usually a light-emitting diode or a cold cathode fluorescent lamp) that moves across the document.

As the light reflects off the document, it hits a sensor array that converts the light into electrical signals.

These signals are then digitized and stored in the computer as an image file.

3 Copying Function

The copying function is essentially a combination of scanning and printing.

When you place a document on the scanner bed and select the copy option, the MFP first scans the document to create a digital image.

This image is then sent to the printer component, which prints a replica of the original document.

4 Faxing Function

Faxing might seem outdated in the era of emails and instant messaging, but many businesses still use it for secure document transmission.

When you feed a document into the MFP's fax component, the device scans the document and converts the information into audio frequency tones.

These tones are transmitted over a phone line to another fax machine, which decodes the tones back into a document.

5 Connectivity and Control

Modern MFPs offer various connectivity options, including USB, Ethernet, and Wi-Fi.

These connections allow the MFP to communicate with computers, smartphones, and other devices.

The user sends a print command from their device, and the MFP's internal processor interprets the command and initiates the appropriate action.

Conclusion

Multifunction printers are marvels of modern technology, combining several essential office functions into one efficient device. They operate through a series of complex processes, from interpreting digital commands to deploying mechanical components.

Understanding how these machines work can help users troubleshoot issues and better appreciate the technology they use daily. Whether you're a business owner seeking to streamline your office operations or a tech enthusiast curious about everyday gadgets, MFPs are a fascinating study of technological integration and innovation

Advantages of a Multifunction Printer

Convenience

A multifunctional printer combines numerous features into a single device to provide more ease. You can use the same machine to scan and print an image. You will save time by not having to walk to two different devices. This also makes the print environment easier to manage because all printing activities take place on the same network.

Controlling the printing environment reduces printing expenses and also increases security. It prevents illegal printing and safeguards sensitive information. Employees will be discouraged from printing personal materials as a result of this. Wireless functionality allows multifunction printers to connect to other devices without the usage of cables. It also allows you to print on the go with mobile devices by connecting to a multifunction wireless printer.

Better Document Management

A multifunction printer helps in the digital and physical management of the company's printing infrastructure. Multifunction printers contain strong software that allows them to be operated by any wireless device, such as smartphones. Because of the increased use of mobile devices in office management, wireless printing is becoming more popular in offices. The office employees will benefit from the ease of designing and printing documents from a single interface.

The advantages of a digital copier lead to the transformation of an office into a productivity powerhouse. It also allows a company to strengthen its document management processes. When all documents travel through a single hub, security, visibility, and compliance improve. This also allows for the development of standardization methods that assist in office organization. Multifunction printers can handle high-volume workloads, reducing time and improving document handling convenience.

Energy Efficiency

One important advantage of getting a multifunction printer is that many of them use power efficiently. When not in use, they go into energy-saving mode.

Use

Since office staff only need to learn one interface, multifunction printers are simple to use and increase efficiency. Users can master a simple interface to execute all printing, copying, and scanning operations with a single action on multifunction printers, which include simple navigation devices and intuitive color touchscreens. This enhances office functions and keeps documents flowing because employees spend less time mastering only one interface and more time on other business tasks.

As a Multifunction Printer Distributor, we understand that our market may be difficult at times, and the range of options can be overwhelming for customers. We hope that this blog has helped you understand our industry a little better!

Follow our blog to learn more about printers and copiers.

Passbook Printer

The passbook is inserted into the passbook printer in the open state and after page information and other data have been read out by an optical reading device and a position at which the printing operation is to be performed has been confirmed, information is printed on the passbook by the printing means.

Working principle of Passbook printer

- Pressurized ink is supplied to the print head from the controller.
- Ink is fed to the nozzle which has the piezoelectric oscillator and discharge hole.
- The ink is discharged while being oscillated by the piezoelectric oscillator, and it is simultaneously given a negative electrostatic charge.

A Passbook Printing Kiosk is an automated machine that enables the customer to update their passbook. These machines are primarily available in banks and other financial institutions that require account updating or bookkeeping. It fetches all the account transaction detail.

The printing process work

Offset Litho uses printing plates clamped inside a printing press around a plate cylinder. The plate cylinder is flanked by a series of ink and damping (water) rollers. These rollers distribute ink and water onto the plate. The water acts as a carrier for the oily ink which adheres to the imaged areas on the plate.

The advantages of passbook printing

Easy to use & update. Low power consumption. No need to wait in long queues at branches. Self-service gives high satisfaction.

High Speed Printer

A high-speed printer is a printing device which produces documents at a high volume per unit time. Printers capable of producing more than 90 A4 pages per minute are considered to be high-speed. This would equate to 1.5 (or more) A4 pages per second, demonstrating the efficiency required for a printer to gain this label. In fact, all RISO printers are classed as high-speed with the VALEZUS TS200 being capable of producing up to 330 A4 pages per minute, meaning that it brings a new, express definition to the term high-speed printing.

Laser printer is known to be the fastest printer. It is a type of printer linked to a computer producing good-quality printed material by using a laser to form a pattern of Electrostatically charged dots on a light sensitive drum, which ink powder.

High-speed printers working Principle

RISO printers use FORCEJET™ inkjet technology, a rapid cold printing process exclusive to the company. To find out more about the mechanics behind the process, The innovative technology enables the ink to dry instantly, meaning that the worries of smudging and distortion often associated with high-speed printing can be forgotten.

Benefits of a high-speed printer

An investment in printing and copying devices which are certified to be high-speed can bring with it a multitude of benefits. Of course, you have the obvious implications of a reduced waiting time, meaning that those printing in both work and home environments can save time and avoid last-minute printing panics. Imagine shorter queues at the office and fewer delays when the kids forget to print out their homework before school. There are also some less obvious consequences of high-speed printers. For example, swift printing processes reduce the cost-per-page and thus increase productivity whilst decreasing expenditure. Who could deny the positive impact this would have on a home or work environment? Faster printing is also more environmentally friendly as less operational time means that less energy is used overall.

To get a high-speed printer

If the idea of a high-speed printer seems appealing to you, you may be wondering how you can purchase one. RISO offers a wide range of premium high-speed, high-capacity printers which boast many advantages and benefits. For an extensive list of the high-speed printers available from RISO, which print between 100 and 330 pages per minute.

Line Printer

A line printer is an impact printer which makes use of a continuous feed of paper and prints one line of text at a time. Although they have been replaced in most instances by high-speed laser printers, they are still used in some business as they are low cost and have the ability to print on multi-part forms.

A line printer is also known as a bar printer. (Fig 7)

Fig 7

Explanation Line Printer

Line printers make use of continuous form paper which is usually perforated instead of individual cut sheets. Line printers print the full width of the page, one line of text at a time, instead of a print head moving back and forth across the page. The two main types of line printers are chain printers and drum printers. Although the basic printing technology used in line printers dates back to the 1930s, they are still suited for high-speed printing.

High speed is one of the advantages of line printers. Compared to other printers, they are low in cost and more durable. The consumables of line printers are

less harmful to the environment and are less costly as well. They are especially well suited to industrial environments and shop floors where other printers could be easily damaged by temperature extremes, dust or other factors.

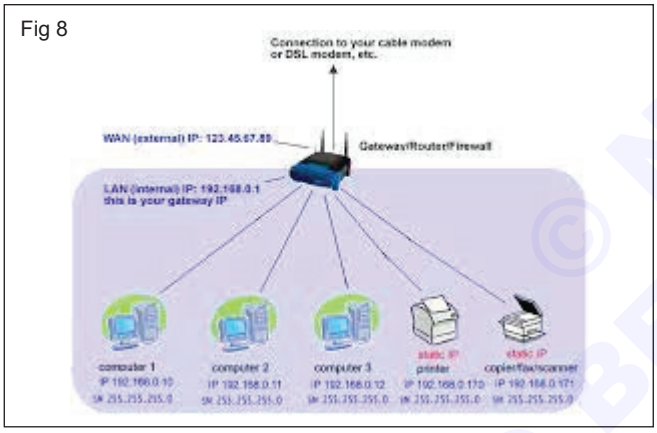
There are also disadvantages associated with line printers. The print quality is mostly low and they cannot print graphics. Line printers are very noisy while operating and may need soundproofing. The continuous feed forms for line printers are not easily available anymore, as they are no longer in high demand.

Advantages and Disadvantages

Although their basic technology dates back decades, line matrix printers remain a viable option for high-speed business printing. Their primary disadvantages are their noisiness and their reliance on continuous-feed forms, which aren't as widely available as they were a few decades ago. However, line printers are physically more durable than laser printers, and their consumables are both less costly and less harmful to the environment. Laser printers are limited in the number of pages they can print in a given time frame. By contrast, line printers are limited only by the number of hours in a day.

Network printer (Fig 8)

Fig 8



A network printer is any printer connected to a network, whether through Ethernet or Wi-Fi - the latter being the more contemporary option. Whereas a local printer would be cabled straight to the device that requires it, a network printer can be accessed by multiple devices simultaneously on the same network. This is different again to a print server, where the printing device connects to a server, which staff then access to use the device.

Benefits of a network printer

1 Less money wasted on redundant IT equipment

When using a network printer, users can connect directly to the device via direct IP, eliminating the need for excess IT equipment. In this way, you don't need to purchase a print server device or dedicate a computer to the printer to act as a server. Both of these reduce your budget spend on new equipment, so you can invest more on the printer itself.

The added bonus to reducing IT equipment is that you also eliminate the need for extra cables - the more cables you can remove from the office, the tidier it will look and the less chance of tripping your staff have.

2 Highly scalable

So long as your users are accessing the network, they can print on a network printer. In this way, you can easily scale the amount of staff needing print access without the IT setup costs. It's as easy as discovering the device and then printing to it.

Additionally, you can add more printers. For example, for those who require different printer types in one office - say, a document printer, label printer and photo printer - staff could print to any of these devices without needing to plug in different cables (or even leave their desk!).

3 Print from anywhere

By installing a network printer with direct Wi-Fi, your staff can print from anywhere in the office. In fact, with an email-enabled device, you could be anywhere in the world! You just send the document to the printer's address and it takes care of the rest.

4 Flexible device installation

Following on from point three above, a network printer with direct Wi-Fi does not need to be tethered to an Ethernet port or router. This enables IT managers to place the device at the most logical position in the office to maximise efficiency, even if that placement is nowhere near a router. It also means you can have multiple devices in close proximity without hogging Ethernet cables, should you desire to create a dedicated printing room.

By printing via Wi-Fi, you can print with nearly any device, such as smartphones and tablets.

5 Print from any device

Another limitation of a local printer is that if your device doesn't have a USB port, it won't connect to the printer. And if your device can't connect to the server, again - it won't connect to the printer. Therefore, a network printer frees your staff to use whatever device they need to print from, whether that's a PC, tablet or smartphone.

When paired with an app like i Print your team could literally travel across the globe with just a tablet, take a photo or draft a document, and print at the office back home in Australia, all without carrying their computer with them.

6 Scan and file share remotely

Let's say you need a multi-function printer that has scanning in-built. Normally you would need to travel to the device, scan your file and then upload it to your computer with a USB cable. But when you're connected to the network, you can scan the file and transfer it to your device of choice via Wi-Fi.

Remote file sharing works the same. Let's say you took an important photo on your digital camera or you have it on a USB drive. With the right network printer, you can plug either of these into the printer and send files to your phone or tablet using iPrint (or vice versa, if you want). No computer involved.

7 Connect to a range of apps

Contemporary network printers such as those from Epson are designed to work in tandem with iPrint and a variety of other common apps. These include Dropbox, Google Drive, Evernote, Microsoft SkyDrive and Box.

Print server

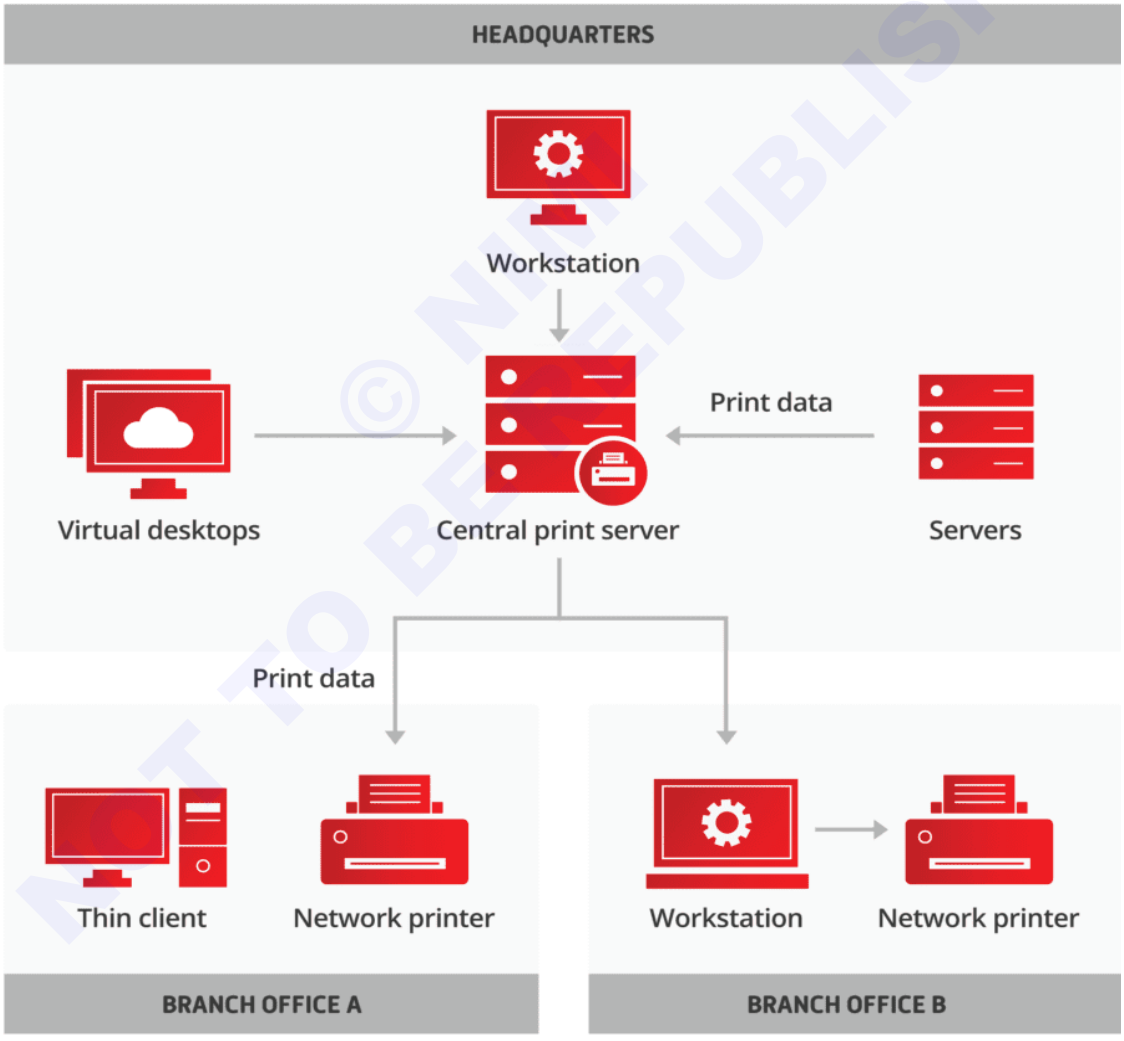
A print server is a piece of equipment that establishes a network connection between several printers. Rather than directly attaching each printer to a particular computer, users can send printing jobs to the print server, which will then distribute them to the relevant printer. This simplifies connectivity, optimizes bandwidth, and reduces bottlenecks by ensuring that each print job is sent to the right printer at the right time. (Fig 9)

Print servers essentially boil down to two types: wireless and wired.

- **Wireless print servers** use Wi-Fi to connect computers, servers, and other devices on a local area network (LAN).
- **Wired print servers** connect printer and compute devices on a network by linking directly to a router via an Ethernet cable.

It is also worth noting that, as processors and wireless technology have grown in sophistication, many print server tasks that formerly required a dedicated server are now simply handled by one or more networked computers, or even integrated into Wi-Fi printers themselves. In large enterprises or dispersed campuses, though, a dedicated print server is often still necessary.

Fig 9



Why do I Need a print server

A print server is the main hub for organizing and allocating print tasks to various printers in a networked environment. It simplifies and increases the efficiency of the printing process by doing away with the requirement for a direct connection between each computer and each printer. The following are strong arguments in favor of using a print server:

- **Centralized printer management:** By combining operations like driver installation, printer configuration, and maintenance into one place, a print server makes printer management easier. This centralized method guarantees uniform printer settings throughout the network and lessens the workload for IT personnel.
- **Enhanced print job efficiency:** By prioritizing print jobs according to user or department needs, print servers queue up and streamline the processing of print jobs. This helps avoid printer overload, and ensures urgent documents are printed on time.
- **Enhanced security:** In addition to being protected under the network firewall, print servers can impose secure printing policies such as demanding job release codes or PIN authentication to stop unwanted access to private data. In addition to preventing illegal printing, this secures sensitive information.
- **Cost-effective solution:** Print servers provide an affordable option for companies and organizations with several printers. Print servers can reduce total IT expenditures by centralizing printer administration and eliminating the need for several direct connections.
- **Scalability and flexibility:** Print servers can expand with a company as needed. It's relatively easy to add more devices to the print server to accommodate the extra burden as the number of users or printers grows.

How do print servers work?

Print servers are software or hardware that uses a network to link computers and printers. By receiving printing jobs from computers and forwarding them to the appropriate printer, they serve as a go-between for computers and printers. They accomplish this by locally storing and queuing print requests to prevent overtaxing a busy printing device.

At its most basic, here is how a print server works:

1 **The user submits a print job:** The user selects the printer they wish to print and clicks the "Print" button. In more advanced configurations, they may simply select the server itself.

2 **The print server receives the print job:** The print job is transmitted across the network from the user's PC to the print server, which selects the appropriate printer and adds it to the printer's queue.

3 **The print server awaits the printer's availability:** The print server monitors the condition of all available printers and forwards the task to the chosen printer when it becomes available.

4 **The printer prints the job:** After receiving the print job, the printer produces the document. Print server maintenance is crucial for optimal performance and longevity. Regular software updates, disk space monitoring, print queue management, printer status monitoring, preventive maintenance, security measures, backups, and documentation are essential for a reliable printing experience.

What is print server software?

Print server software is a program that enables a computer to function as a print server. It manages print jobs, distributes them to network printers, and monitors the status of printers. Print server software can be either included with the operating system or purchased as a separate product.

Many different types of print server software are available, each with its own set of features. Some of the most common features include:

- Print job queuing and management.
- Printer status monitoring.
- Job accounting.
- Secure printing.

Print server software can be valuable for businesses and organizations with multiple network printers, but without the level of large, complex network infrastructure that demands a dedicated printer. It can help to improve print job efficiency, reduce IT costs, and increase security.

Printing protocols

A set of guidelines and conventions known as printing protocols control how computers and printers communicate. They are necessary to guarantee accurate transmission and reception of print jobs.

Although several printing protocols are in use today, the most widely used ones are:

- **Line Printer Remote (LPR):** An outdated protocol called LPR was first created for Unix systems. Even now, many people still use this straightforward protocol. LPR operates by sending the complete print job to the printer at once. Thus, LPR may be sluggish, particularly for assignments requiring high volume.
- **Internet Printing Protocol (IPP):** A more recent protocol built on HTTP is called IPP. Although it is a more complicated protocol than LPR, it has several benefits, such as the ability to monitor and cancel jobs. IPP is gaining popularity and is the recommended protocol for new printers.

- **Server Message Block/Common Internet File System (SMB/CIFS):** On Windows networks, printing is possible via the network file-sharing protocol Although SMB/CIFS is a straightforward and user-friendly protocol, it lacks the strength of LPR or IPP.
- **Jet Direct:** HP created the proprietary protocol known as Jet Direct. While it is not as extensively supported as LPR or IPP, it is a common protocol for HP printers.
- **TCP/IP:** The most widely used network protocol worldwide is TCP/IP. It is employed for a huge array of network tasks, only one of which is printing. TCP/IP is a dependable protocol for printing across both wired and wireless networks.

Here is a closer look at some of the advantages and disadvantages of each protocol:

Protocol	Description	Advantages	Disadvantages
LPR	Simple protocol that is still widely used.	Easy to use.	Slow for large print jobs.
IPP	Newer protocol that offers more features.	Supports job status monitoring and job cancellation.	More complex than LPR.
SMB/CIFS	Simple protocol that is easy to use.	Easy to use for Windows networks.	Not as powerful as LPR or IPP.
Jet Direct	Proprietary protocol that is popular for HP printers.	Fast and reliable.	Not as widely supported as LPR or IPP.
TCP/IP	Reliable protocol that can be used to print over both wired and wireless networks.	Widely supported.	More complex than LPR or SMB/CIFS.

Apart from these widely used protocols, several other specialized printing protocols exist. Usually, these protocols are used for specialized tasks, including printing to large-format printers or mobile devices.

Common issues and troubleshooting

Several typical issues, like printer faults and network issues, can occur when managing print servers. These problems can make printing difficult and frustrate users. Maintaining a seamless and effective printing environment requires quickly identifying and fixing these problems.

Network connectivity

It is important to confirm that the print server is physically connected to the network when experiencing problems with print server network connectivity.

Ensure the print server has a working IP address and is correctly connected to the network. Examine network cables for damage and make sure they are connected securely.

Types of monitor

Objectives: At the end of this lesson you shall be able to
- **define monitors**
- **types of monitors**
- **display card components**
- **steps to installing graphic card**
- **difference between CRT & LCD.**

Definition of Monitor

A monitor is an electronic output device that is also known as a video display terminal (VDT) or a video display unit (VDU). It is used to display images, text, video, and graphics information generated by a connected computer via a computer's video card. Although it is almost like a TV, its resolution is much higher than a TV. The first computer monitor was introduced on 1 March 1973, which was part of the Xerox Alto computer system. (Fig 1)

Older monitors were built by using a fluorescent screen and Cathode Ray Tube (CRT), which made them heavy and large in size and thus causing them to cover more space on the desk. Nowadays, all monitors are made up by using flat-panel display technology, commonly backlit with LEDs. These modern monitors take less space on the desk as compared to older CRT displays.

Fig 1

- In 1964, the Uniscope 300 machine included a built-in CRT display, which was not a true computer monitor.
- A. Johnson invented the touch screen technology in 1965.
- On 1 March 1973, Xerox Alto computer was introduced, which had the first computer monitor. This monitor included a monochrome display and used CRT technology.
- In 1975, George Samuel Hurst introduced the first resistive touch screen display, although it was used only before 1982.
- In 1976, the Apple I and Sol-20 computer systems were introduced. These systems had a built-in video port that allowed them to run a video screen on computer monitor.
- In 1977, James P. Mitchell invented LED display technology. But even 30 years later, these monitors were not easily available to buy in the market.
- In June 1977, the Apple II was released, allowing for color display on a CRT monitor.
- In 1987, IBM released the IBM 8513, first VGA monitor.
- In 1989, VESA defined the SVGA standard for the display of computers.
- In the late-1980s, the color CRT monitors were able to support 1024 x 768 resolution display.
- Eizo Nanao manufactured the Eizo L66, the first LCD monitors for desktop computers, and released it in the middle-1990s.
- In 1997, the color LCD monitors were started developing by IBM, Viewsonic, and Apple that provide better quality and resolution than CRT monitors.
- In 1998, the color LCD monitors for desktop computers were manufactured by Apple.
- Later in 2003, CRT monitors outsell for the first time by LCD monitors. Till 2007, CRT monitors consistently outsell by LCD monitors, so they become more popular computer monitor.
- In 2006, Jeff Han released the first interface-free, touch-based monitor at TED.
- In 2009, the LED monitor MultiSync EA222WMe was released by NEC company. It was the first monitor released by NEC.
- AMD and Intel announced to end support for VGA in December 2010.
- In 2017, touch screen LCD monitors became more affordable for the customers as they started to decrease the price.

Types of Monitors

There are several types of monitors some are as follows:

1 Cathode Ray Tube (CRT) Monitors

It is a technology used in early monitors. It uses a beam of electrons to create an image on the screen. It comprises the guns that fire a beam of electrons inside the screen. The electron beams repeatedly hit the surface of the screen. These guns are responsible for generating RGB (Red, Green, Blue) colors, and more other colors can be generated with the help of combining these three colors. Today's Flat Panel Monitors replace the CRT monitors. (Fig 2)

Fig 2

2 Flat Panel Monitors

These types of monitors are lightweight and take less space. They consume less power as compared to CRT monitors. These monitors are more effective as they do not provide harmful radiation. These monitors are more expensive than CRTs. The flat-panel monitors are used in PDA, notebook computers, and cellular phones. These monitors are available in various sizes like 15", 17", 18" & 19" and more. The display of a flat-panel monitor is made with the help of two plates of glass. These plates contain a substance, which is activated in many ways. (Fig 3)

Fig 3

Flat-panel monitor screens use two types of technologies, which are given below

- **Liquid Crystal Display:** LCD (Liquid crystal display) screen contains a substance known as liquid crystal. The particles of this substance are aligned in a way that the light located backside on the screens, which allow to generate an image or block. Liquid crystal display offers a clear picture as compared to CRT display and emits less radiation. Furthermore, it consumes less power and takes less space than a CRT display.
- **Gas Plasma Display:** This display uses gas plasma technology, which uses a layer of gas between 2 plates of glass. When voltage is applied, the gas releases ultraviolet light. By this ultraviolet light, the pixels on the screen glow and form an image. These displays are available in different sizes of up to 150 inches. Although it offers effective colors as compared to the LCD monitor, it is more expensive. That's why it is less used.

3 Touch Screen Monitors

These monitors are also known as an input device. It enables users to interact with the computer by using a finger or stylus instead of using a mouse or keyboard. When users touch the screen by their finger, it occurs an event and forward it to the controller for processing. These types of screens include pictures or words that help users to interact with the computer. It takes input from the users by touching menus or icons presented on the screen. (Fig 4)

Fig 4

There are different types of touch screen monitors three common types are given below

- **Resistive Touch Screen:** Generally, this screen includes a thin electrically conductive and resistive layer of metal. When the touch is pressed, a change in the electrical current occurs that is sent to the controller. Nowadays, these screens are widely in use. These monitors are more reliable as they cannot be affected by liquids or dust.
- **Surface Wave Touch Screens:** These monitors process the input through ultrasonic waves. When a user touches the screen, the wave is processed and

absorbed by the computer. It is less reliable as they can be damaged by water or dust.

- **Capacitive Touch Screen:** This screen includes a cover with an electrically-charged material. This material continuously flows the current over the screen. It is mainly used by the finger rather than a stylus. These monitors contain better clarity and do not damage by dust. Nowadays, capacitive touch screen is mostly used in smartphones.

4 LED Monitors

It is a flat screen computer monitor, which stands for light-emitting diode display. It is lightweight in terms of weight and has a short depth. As the source of light, it uses a panel of LEDs. (Fig 5)

Nowadays, a wide number of electronic devices, both large and small devices such as laptop screens, mobile phones, TVs, computer monitors, tablets, and more, use LED displays.

It is believed that James P. Mitchell invented the first LED display. On 18 March 1978, the first prototype of an LED display was published to the market at the SEF (Science and Engineering Fair) in Iowa. On 8 May 1978, it was shown again in Anaheim California, at the SEF. This prototype received awards from NASA and General Motors.

Fig 5

Advantages of LED Monitor

- It includes a broader dimming range.
- It is a more reliable monitor.
- It is often less expensive.
- It consumes less power (20 watts), and run on a lower temperature.
- It has a more dynamic contrast ratio.

Comparison between LCD and LED monitors

Resolution 1920 x 1080	LCD Monitors	Led Monitors
Brightness	250 cd / m2	250 cd / m2
Energy Star Certified	No	Yes
Weight	2.4 kg	2.4 kg
Contrast Ratio	12,000,000 : 1	100,000,000 : 1

5 OLED Monitors (Fig 6)

Fig 6

It is a new flat light-emitting display technology, which is more efficient, brighter, thinner, and better refresh rates feature and contrast as compared to the LCD display. It is made up of locating a series of organic thin films between two conductors. These displays do not need a backlight as they are emissive displays. Furthermore, it provides better image quality ever and used in tablets and high-end smartphones.

Nowadays, it is widely used in laptops, TVs, mobile phones, digital cameras, tablets, VR headsets. The demand for mobile phone vendors, more than 500 million AMOLED screens were produced in 2018. The Samsung display is the main producer of the AMOLED screen. For example, Apple is using AMOLED OLED panel made by SDC in its 2018 iPhone XS - a 5.8" 1125x2436. Additionally, iPhone X is also using the same AMOLED display.

6 DLP Monitors

DLP stands for Digital Light Processing, developed by Texas Instruments. It is a technology, which is used for presentations by projecting images from a monitor onto a big screen. Before developing the DLP, most of the computer projection systems produced faded and blurry images as they were based on LCD technology. DLP technology utilizes a digital micro mirror device, which is a tiny mirror housed on a special kind of microchip. Furthermore, it offers better quality pictures that can also be visible in a lit room normally. (Fig 7)

Fig 7

7 TFT Monitors (Fig 8)

Fig 8

It is a type of LCD flat panel display, which stands for a thin-film transistor. In TFT monitors, all pixels are controlled with the help of one to four transistors. The high-quality flat-panel LCDs use these transistors. Although the TFT-based monitors provide better resolution of all the flat-panel techniques, these are highly expensive. The LCDs, which use thin-film transistor (TFT) technology, are known as active-matrix displays. The active-matrix displays offer higher quality as compared to older passive-matrix displays.

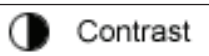
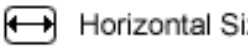
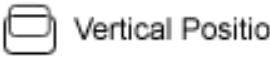
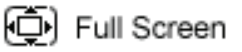
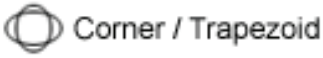
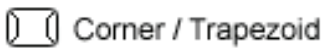
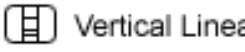
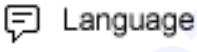
8 Plasma Screen Monitors (Fig 9)

Fig 9

A plasma screen is a thin, flat-panel, and capable of hanging on a wall like LCD and LED televisions. It is a brighter screen as compared to LCD displays and thinner than CRT displays. It can be used to either display modes of digital computer input or analog video signals, and sometimes, it is marketed as 'thin-panel' displays. Plasma displays have wide viewing angles, high contrast ratios, and high refresh rates, which is used to reduce a blur video. Additionally, it provides better quality pictures as it supports high resolutions of up to 1920 x 1080.

The plasma screen also includes some disadvantages such as the chance of screen burn-in, consumes more power, loss of brightness with time, can be heavier in weight.

- **SVGA (Super VGA):** One of the more popular labels placed on video cards and monitors. A SVGA card or monitor is capable of displaying more pixels (dots on the screen) and/or colors than basic VGA. For example, an SVGA graphics card may be able to display 16-bit color with a resolution of 800x600 pixels.
- **3D Acceleration Cards:** These cards include specialized hardware that speeds up the process of displaying three-dimensional images on the screen. They are usually designed to work with an SVGA monitor.
- **VGA (Video Graphics Adapter):** Currently the base standard for PC video cards and monitors. True VGA supports 16 colors at 640x480 pixels or 256 colors at 320x200 pixels.
- **XGA:** A standard used on some IBM PS/2 models. XGA supports 256 colors at 1024x728 pixels, or 16-bit colors at 640x480 pixels.
- **EGA (Enhanced Graphics Adapter):** Following CGA, an adapter that could display 16 colors with a screen resolution of 640x350 pixels.
- **CGA (Color Graphics Adapter):** The first color monitor and graphics cards for PC computers. Capable of producing 16 colors at 160x200 pixels.
- **MDA (Monochrome Display Adapter):** A monitor or graphics card that can display only one color. No longer in common use but may be found on some older systems. Usually supports only text.
- **Hercules Graphics Card:** A card that enabled a PC to display graphics on a MDA monitor.
- **Bus Standards:** A bus is a communication system that transfers data between components inside a computer, or between computers. Buses are parallel electrical wires with multiple connections. Modern computer buses use both parallel and bit serial connections.

Monitor Icon	Description of Icon function
 Power	**Power** - Turns the monitor on or off.
 Brightness	**Brightness** - Using this button or wheel the user can increase and decrease the brightness on the screen.
 Contrast	**Contrast** - Using this button or wheel can increase and decrease the amount of contrast on the screen.
 Horizontal Size	**Horizontal Size** - Allows for the picture on the screen to be stretched to the horizontal edge of the monitor.
 Vertical Size	**Vertical Size** - Allows the picture on the screen to be stretched to the vertical edges of the monitor.
 Horizontal Position	**Horizontal Position** - Allows the picture to move moved horizontally, once in the center the user can then use the Horizontal size to stretch it to have an equal amount of black border on each side.
 Vertical Position	**Vertical Position** - Like the Horizontal Position, using this button or wheel the user can move the picture up or down to center the picture more appropriately.
 Full Screen	**Full Screen** - Sets monitor to full screen.
 Degauss	**Degauss** - This button will degauss the CRT, restoring possible color impurities. After this button has been pressed the degaussing circuit will be activated and then deactivated after a few seconds. Pressing and holding this button for a few seconds may cause your computer monitor to reset all data.
 Corner / Trapezoid Correction  Corner / Trapezoid Correction	**Corner and Trapezoid Correction** - Using this button or wheel the user can either round the edges of the picture or move the picture inward like an hour glass or outwards.
 Vertical Linearity	**Vertical Linearity** - Sets the width of the vertical lines.
 Moiré	**Moire** - Removes or reduces the Moire effect, if any.
 OSD Controls	**OSD Controls** - If the monitor contains OSD controls, allows for the OSD menus to be adjusted.
 Power Management	**Power Management** - Allows the user to define the power management settings through the monitor itself and not the software.
 Monitor Status	**Monitor Status** - Displays the current monitor settings such as refresh rate and other settings.
 Language	**Language** - Sets the language on the monitor.

Display card

A graphics card (also called a video card, display card, graphics adapter, VGA card/VGA, video adapter, display adapter, or colloquially GPU) is a computer expansion card that generates a feed of graphics output to a display device such as a monitor.

Video card on PC

The graphics card in a PC is typically located in the motherboard's expansion slot. This slot is usually positioned towards the back of the PC case.

Graphic card components

1 Interface
2 GPU
3 Graphics memory
4 Cooling
5 Memory
6 BIOS
7 Graphics chip
8 Outputs
9 Graphics card

The most common connection systems between the graphics card and the computer display are

- Video Graphics Array (VGA) (DE-15)
- Digital Visual Interface (DVI)
- Video-in video-out (VIVO) for S-Video, composite video and component video.
- High-Definition Multimedia Interface (HDMI)
- DisplayPort.
- USB-C.

A display controller

A video display controller or VDC (also called a display engine or display interface) is an integrated circuit which is the main component in a video-signal generator, a device responsible for the production of a TV video signal in a computing or game system.

Types of display controller

Display controller IC (integrated circuit), touchscreen controller, LCD screen controller, LCD panel controller, smart display controller, TFT LCD controller or digital display controller for a graphic LCD controller card.

Ram chip

A RAM chip is a microchip used as RAM storage for computers and other devices. This is the actual chip that is soldered onto small circuit boards in order to create RAM cards or sticks, and it is rated for performance and capacity differently, depending on the model and manufacturer.

Dual port feature in computer

The Dual-Port feature supports two physical ports per CHPID. Each port is independent and can be independently configured as an OSA-ICC. The server definition for each physical port is restricted to a unique TCP port number and subnet.

How does a computer graphics card work?

A graphics card works with other components in your computer system to deliver a smooth and realistic visual experience. The CPU, or the central processing unit, sends instructions and data to the GPU, which then processes them and sends the output to the monitor.

The CPU, working in conjunction with software applications, sends information about the image to the graphics card. The graphics card decides how to use the pixels on the screen to create the image. It then sends that information to the monitor through a cable.

Uses

Sending graphics data to the output unit. A Display card is an expansion card that generates a feed of output images to a display device. Graphics cards allow computers to produce graphics and images more quickly.

Steps to Installing Your Graphics Card

1 Turn off your computer and unplug all power cords. Remove the side panel to gain access to the inside of your computer. Don't touch any of the components inside.

2 With the side panel off, lay your computer on its side. Locate either the PCI-Express slot on your motherboard.

3 If you're building this computer for the first time, the IO plate covering the AGP/PCI-Express slot in the back of your computer should still be in place. Remove it, being careful not to touch any components. Some cases have their IO plates secured with screws or tabs, others simply require you to twist them off.

4 Carefully remove your graphics card from its box, and it should be in an anti-static bag. It's a good idea to keep your graphics card in this bag until the very moment you're going to install it. Open the bag and pick up your video card by its side edges (try to touch the card as little as possible too). If you're not using an anti-static wrist band, then make sure you're holding onto your computer case with one hand when picking up the video card in your other, so that you don't create static electricity that may damage your card.

5 Now you're ready to plug your card into the PCI-Express slot. Do this gently, but make sure the card is firmly slotted in. When your graphics card is in place, some cards require you to screw it in. Check the documentation that you got with the card if you are unsure about this (or anything else for that matter.

6 Once the graphics card has been secured to the case, you can re-install the side panel of your case, connect your monitor to your graphics card, and turn your computer back on.

Installing the Graphics Card Drivers

Now that your graphics card has been installed, the only thing left to do is install the drivers. Your graphics card should come with its own drivers on CD, so once you've turned your PC on, simply insert the drivers CD and follow the instructions.

It's important to note that the drivers that come with your graphics card are sometimes outdated. So you will need to visit your video card manufacturer's website and download the latest drivers.

The main precautions are

1 You should place your cabinet above the ground level.

2 You must have to wear good insulated boots because the capacitors in the PSU of the cabinet might have charge which can release when you become a path to the ground.

3 You might have to remove a metal strip from the motherboard for the outlet ports of the graphic card, so be careful.

4 Don't forget to put the lock back after attaching the graphic card to the PCI-express slot.

Some precautions to keep in mind when installing a graphic card

Make sure you have the right type of card for your computer. Check the specifications of your motherboard and power supply to ensure compatibility.

Turn off your computer and unplug it before installing the card. This will prevent any damage from static electricity.

Handle the card carefully. It is a delicate piece of hardware and can be easily damaged.

Follow the instructions provided by the card's manufacturer for proper installation.

Connect any necessary power cables to the card.

Reinstall any other hardware that was removed and turn on your computer.

Update your drivers and graphics settings to ensure optimal performance.

If you're experiencing any issues or have any doubts, please consult the graphic card's manufacturer or a professional for assistance.

Liquid Crystal Display Monitor Mean

A liquid crystal display (LCD) monitor is a computer monitor or display that uses LCD technology to show clear images, and is found mostly in laptop computers and flat panel monitors. This technology has replaced the traditional cathode ray tube (CRT) monitors, which were the previous standard and once were considered to have better picture quality than early LCD variants. With the introduction of better LCD technology and its continuous improvement, LCD is now the clear leader over CRT, in terms of color and picture quality, not to mention capabilities for large resolutions. Also, LCD monitors may be made much more cheaply than CRT monitors. (Fig 10)

Fig 10

Explains Liquid Crystal Display Monitor

Liquid Crystal Display Monitor

Various different LCD technologies are used today, including:

In Plane Switching (IPS) Panel Technology: These panels are considered to have the best color accuracy, viewing angles and image quality in LCD technology.

Super Plane to Line Switching (PLS): Developed by Samsung, this LCD panel is very similar to the IPS panel but reportedly, it is 10 percent brighter, has wider viewing angles and is cheaper to produce.

Vertical Alignment (VA) Panel Technology: These panels are considered to be in the middle of TN and IPS technology. Compared to TN panels, they offer wider viewing angles and better color quality but have slower response times. They have higher contrast ratios, compared to the other panels but have a downside, in terms of color shifting, where the brightness display is unevenly distributed throughout the screen.

Twisted Nematic (TN) Panel Technology: These panels are the most commonly used type of panel in LCD technology. They are cheaper and offer faster response times, making them a preferred choice for gamers. The downside is that the viewing angles, contrast ratios and color production are considered the lowest of LCD panel types.

TFT Monitor

A TFT monitor uses thin-film transistor technology in an LCD display. LCD monitors, also called flat panel displays, are replacing the old-style cathode ray tubes (CRTs) in both televisions and computer displays. Nearly all LCD monitors today use TFT technology. (Fig 11)

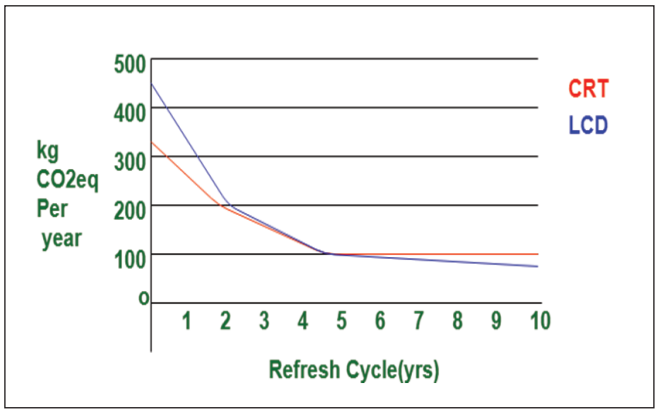
Fig 11

The benefit of thin-film transistor technology is the separate, tiny transistor for each pixel on the display. Because each transistor is so small, the amount of charge needed to control it is also small. This allows the screen to refresh very quickly, as the image is re-painted or refreshed several times per second.

A desktop computer with a TFT monitor

Prior to TFT, passive matrix LCD displays could not keep up with fast moving images. A mouse dragged across the screen, for example, from point A to point B, would disappear between the two points. A TFT monitor can track the mouse, resulting in a display that can be used for video, gaming, and all forms of multimedia.

Difference between CRT and LCD



CRT stands for cathode Ray Tube and LCD stands for Liquid Crystal Display area unit the kinds of display devices wherever CRT is employed as standard display devices whereas LCD is more modern technology. These area unit primarily differentiated supported the fabric CRT stands for Cathode Ray Tube and LCD stands for Liquid Crystal Display area unit the kinds of display devices wherever CRT is employed as standard display devices whereas LCD is more modern technology. These area unit primarily differentiated supported the fabric they're made from and dealing mechanism, however, each area unit alleged to perform identical perform of providing a visible variety of electronic media. Here, the crucial operational distinction is that the CRT integrates the 2 processes lightweight generation and lightweight modulation and it's additionally managed by one set of elements. Conversely, the LCD isolates the 2 processes kind one another that's lightweight generation and modulation.

Let's see that the difference b/w CRT and LCD

S.No.	CRT	LCD
1	CRT stands for Cathode Ray Tube.	While LCD stands for Liquid Crystal Display
2	CRT consumes more power.	While it consumes less power.
3	The cost of CRT is less than LCD.	While it is costlier than CRT
4	CRT is faster than LCD in terms of response	While it is slower than CRT in terms of response.
5	CRT is larger than LCD in terms of size.	While it is small in terms of size.
6	It has not image confinement.	While it has good image confinement
7	CRT's resolution is lower than LCD..	While LCD's resolution is more than CRT
8	It is used only in personal computers	While it is used in personal computers as well as in laptops and cellular phones
9	Image Flickering is there in CRT.	Image Flickering is not there in LCD
10	Electron Gun is used to form images.	Liquid crystals are used to form images.

It is through the rotation of the color wheel, the white light beam emitted from the lamp through the RGB filter on the color wheel, filter out the color light, then through the lens, and finally on the screen to form a color image. The single-chip projector is relatively simple in structure and low in cost, but the color effect is not as good as the three-chip projector.

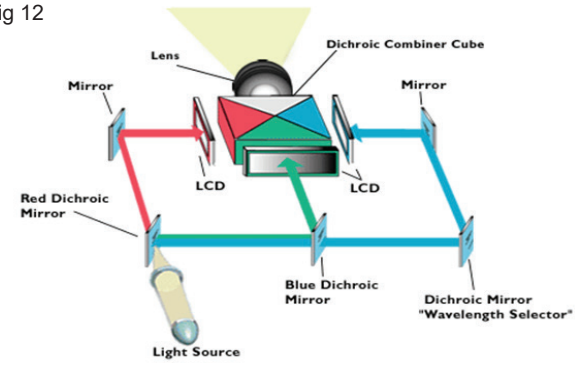
LCD PROJECTOR

An LCD projector works with an optical light engine, which incorporates three small LCD (Liquid Crystal Display) panels, one each for Red, Green and Blue paired with a light source (lamp, LED, Laser Phosphor, Discrete RGB Laser), various filters, mirrors and a prism to create the image. (Fig 12)

LCD projectors work by using three liquid crystal panels, a lamp, a prism, and filters to create the image on the screen. The lamp provides white light that passes through a polarizing filter. Polarizing works by accepting light that is traveling on the same plane. All other light will be blocked.

From the polarizing filter the light is then passed through a series of dichroic mirrors. Dichroic mirrors work by only allowing certain colors in the light spectrum to be reflected, while others pass through. The dichroic mirrors in LCD projectors separate the light into the three primary colors, green, red, and blue.

Fig 12



These three colors are then sent to a separate LCD panel remember there are three of them. From there the LCD panels send the light through the dichroic prism which recombines the light and sends it out the main lens in the LCD projector to the surface against which it is projected. Each LCD is only capable of controlling one color. So if you were to see a picture of a red plane against a blue sky, the green LCD would block the light from passing to the dichroic prism and out the lens.

LCD panels in LCD projectors work by allowing the polarized light to travel through a pane of glass into the liquid crystal inside the display. The liquid crystals bend the light, and it is traveling on a different plane then when it entered through the polarizing filter. If you apply an electrical current to the liquid crystal they will align, allowing the light to pass through on the same plane as when it entered. If you add a second polarizing filter at the other end of the liquid crystal you can then effectively block all light from passing through. Each LCD panel has a separate system to control the electrical current that passes through the liquid crystal, allowing each to be controlled individually.

The resolution, or how sharp the image is, of each LCD is determined by the number of cells which are called pixels, with the higher the number of pixels meaning more clarity to the image. Each LCD panel also has the ability to control what color each pixel will be in that particular panel so that when all the light is recombined at the dichroic prism, it will be the right color. Think of it working the same way that the old dot matrix printers used to work. They would combine dots of the three main colors to provide the desired color. This is the same way that LCD panels work.

1 Purple Dots on the Screen

Purple or magenta spots on a screen could affect the quality of images being beamed by an LCD projector, and these can distract users. The usual causes of this are dust and dirt particles that have accumulated on a projector's green panel. You should regularly clean the projector for foreign materials to ensure that the images are always of high quality.

2 Projector Not Turning Off

Another common problem with LCD projectors is that they will not turn off when the power off button is pressed. The usual root cause of this technical problem is an ill-fitted lamp assembly. To address this issue, re-fit and adjust the lamp assembly. You can usually get installation instructions from the owner's manual. If the problem still persists even after all the necessary adjustments are made, contact technical support to help diagnosis the problem.

3 Poor Image Quality

You may sometimes see images that are of inferior quality; this problem can be caused by an unaligned computer resolution. Many new LCD projector models are equipped with an automatic setup feature that instantly aligns the projector's resolution to a computer's resolution. However, there may be occasions where the projector is not able to conform to a computer's resolution, thereby affecting the quality of the images displayed. To resolve this, adjust the computer's resolution until the images improve.

4 Images Don't Display Fully

Sometimes a user does not see the images getting fully beamed by the LCD projector. You may find that the bottom of the image is cut off or the text has missing parts. This problem can be rectified by aligning the computer's resolution to the projector's resolution. Adjusting the resolution can get tricky with laptops, especially if its standard resolution exceeds that of a projector's resolution. If you still don't get full images even after adjustments have been made on the laptop's resolution, you might have to disable your laptop's desktop.

5 Infrared Remote Controls Not Functioning

An LCD projector remote control that is not working may be caused by several factors. One reason is that its batteries are already weak and need to be replaced. Another reason is that you may be using it in excess of the recommended distance range. One other probable reason is that you're doing the presentation with fluorescent lights on. This disables infrared remote control functions.

Touchpad

Touchpads operate in several ways, including capacitive sensing or resistive touchscreen. The most common technology used in the 2010s senses the change of capacitance where a finger touches the pad. Capacitance-based touchpads will not sense the tip of a pencil or other similar ungrounded or non-conducting implements.

There are two principal means by which touchpads work In the matrix approach, a series of conductors are arranged in an array of parallel lines in two layers, separated by an insulator and crossing each other at right angles to form a grid. A high frequency signal is applied sequentially between pairs in this two-dimensional grid array. The current that passes between the nodes is proportional to the capacitance. When a virtual ground, such as a finger, is placed over one of the intersections between the conductive layer some of the electrical field is shunted to this ground point, resulting in a change in the apparent capacitance at that location. This method received awarded to George Gerpheide in April 1994.

The capacitive shunt method, described in an application note by manufacturer Analog Devices, senses the change in capacitance between a transmitter and receiver that are on opposite sides of the sensor. The transmitter creates an electric field which oscillates at 200 - 300 kHz. If a ground point, such as the finger, is placed between the transmitter and receiver, some of the field lines are shunted away, decreasing the apparent capacitance.

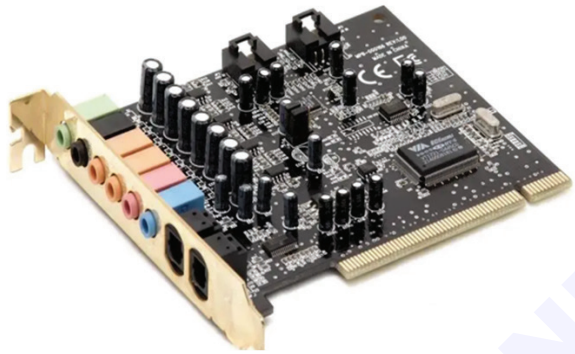
Trackpads such as those found in some Blackberry smartphones work optically, like an optical computer mouse.

Working principle and installation procedure of sound card

Objective: At the end of this lesson you shall be able to
- **sound card, function of sound card, features of sound card, specification of sound card installation of sound card.**

Definition of sound card: A sound card is a computer expansion card that is fixed on the motherboard to support audio input and output. It is also known as a PC sound card, audio card, or audio interface. It converts digital signals from computers to analog signals to be played on the speakers. Computer sound cards can be internally built within the motherboard or they can be external for more professional audio production. (Fig 1)

Fig 1 **Sound Card**



The main features of a sound card are CODEC, audio input/output, digital signal processor, and amplifier among other components. An audio card is used to convert digital signals to audio signals and vice versa. The main advantage of using the card are the improved quality of sound and more features than the inbuilt sound card.

Sound Blaster(1988) – The creator of Sound Blaster is the Singapore based firm Creative Technology. – Argues Sound blaster 16 16-bits complex tones Sound blaster 64 Gold 64-bits complex tones,3D 120db dynamic range, 96db Signal to Noise Ratio Sound blaster Live 5.1.

Functions of sound card

The main purpose of the audio card is to convert the digital signal to analog that can be outputted on the speakers. Other functions of the card are:

1 **Allows for audio input and output:** the card has ports that allow a microphone for sound input and a speaker port for sound output.

2 **Enhance sound quality:** the cards are designed to improve the quality of the sound that the system produces. For professional audio producers, the external audio card can even offer better-quality sound.

3 Convert audio from digital to analog and vice versa for playback and recording.

Features of an audio card

1 **Analog-to-Digital Converter (ADC):** the component converts analog audio signals to digital signals for recording. Most current cards have a combination of ADC and DAC to create a CODEC which performs the function of both components.

2 **Digital-to-Analog Converter (DAC):** Converts digital audio signals to analog signals for playback to the speakers.

3 **Audio Input and Output Ports:** a standard sound card at least has an input connection for a microphone and an output for the speaker or headphones.

4 **Motherboard to card connector:** for the card to be able to communicate with the computer processor it requires a connection interface through the computer motherboard. The most common audio card-to-motherboard connectors are ISA and PCI, or PCIe interfaces.

5 **Digital Signal Processor (DSP):** some advanced sound cards have a processor built within that can do most of the processing. This is similar to how we have a graphics processor in graphic cards. This makes the processing of audio data fast. They perform digital signal processing tasks such as audio mixing and sound enhancement.

6 **Memory:** sound cards have a small capacity RAM that can be used to speed up audio data processing.

7 **Amplifier:** it is used to boost the audio signals to the output device such as a speaker or headphones.

8 **Firmware ROM:** this is the memory that stores basic data such as card drivers that control the card. It also helps the sound card to initialize when booting for the first time.

Main components of sound card:

Sound cards typically have four major components:

- A digital-to-analog converter (DAC) which makes it possible to convert digital data to analog sound
- An analog-to-digital converter (ADC), which makes it possible to make digital recordings from analog sound inputs
- An interface to connect to the motherboard, typically using Peripheral Component Interconnect (PCI)

- Input and output connectors so you can plug in headphones, speakers or a microphone - many computer systems have speakers and a microphone built-in, but connectors allow you to use higher quality external devices to play or record sound

On some sound cards the two types of converters are integrated into a single coder/decoder chip, referred to as a CODEC. Some sound cards also have their own processing unit called a digital signal processor (DSP). This takes some of the load of the central processing unit (CPU) to convert between analog and digital. Similarly, some sound cards have their own memory. Sound cards without a DSP or memory will use the motherboard's CPU and memory. Regardless, the basic set of connections included on most audio cards and onboard audio include the following:

Stereo line out or audio out connector (lime green) The line out connector sends sound signals from the audio adapter to a stereo device outside the computer. It is used for hook up the cables from the line out connector to stereo speakers, a headphone set, or stereo system. Some systems use the same lime-green color for surround audio jacks as for the stereo/headphone jack. Check additional markings on the jacks or system documentation for help.

Stereo line in or audio in connector (light blue) with the line in connector, for recording or mix sound signals from an external source, such as a stereo system camcorder, to the computer's hard disk. In place of a dedicated line in jack, some sound cards use a multipurpose jack (Creative calls it a "Flexi Jack") to support line in, microphone in, and optical out.

Rear out and subwoofer/center or speaker connectors (no standard color) - Virtually all modern sound cards and desktop systems with integrated audio include jacks that support rear, center, and subwoofer output for use in 5.1 and greater surround audio systems. Systems that support 5.1 audio use three jacks: one for front (stereo) audio, one for rear audio, and one for center/subwoofer audio. Systems that support 6.1 or 7.1 audio might feature additional jacks or might reassign rear and center/subwoofer jacks with software to provide additional output. Depending on the software driver, need to run a setup program provided with the sound card or motherboard to enable surround audio. Alternatively, selecting the surround audio setup through the OS's speaker configuration utility might be sufficient.

Uses of sound card

1 **PC audio playback:** Without the sound card your computer would not be producing any sound. So the components are used to play music, movies, and other audio content on all types of personal computers.

2 **Audio recording:** The card comes with an input port for the microphone that can be used to record voice, musical instruments, and other sounds.

3 **Voice recognition systems:** To be able to use a voice recognition system that can help visually challenged users, they should have an audio interface. The card helps the user to input sound as input to instruct the computer.

4 **Sound for gaming:** for the best experiences when playing games users can even use an external audio card to improve positional audio and surround sound.

5 **Music production:** Using external sound cards music producing companies can improve their production. It can also be used by individuals who want to start personal music production. They can be used either for a starter or professional music production.

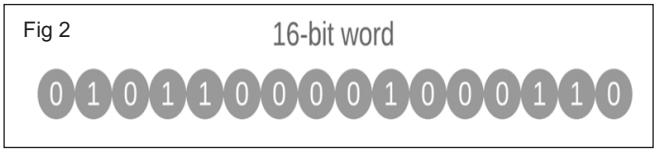
Specification of sound Card 16/32

The MixPre II models introduce the ability to record 32-bit floating point WAV files. For ultra-high-dynamic-range recording, 32-bit float is an ideal recording format. The primary benefit of these files is their ability to record signals exceeding 0 dBFS. There is in fact so much headroom that from a fidelity standpoint, it doesn't matter where gains are set while recording. Audio levels in the 32-bit float WAV file can be adjusted up or down after recording with most major DAW software with no added noise or distortion. To understand the nuts and bolts of 32-bit files, keep reading. This paper discusses the differences between 16-bit fixed point, 24-bit fixed point, and 32-bit floating point files.

16-bit Files

Traditional 16-bit WAV files store uncompressed audio samples, where each sample is represented by a binary number with 16 digits (binary digit = "bit"). These numbers are "fixed-point", because they are whole numbers (no decimal point). A 16 bit number in binary form represents integers from 0 to 65535 (216). (Fig 2)

Fig 2



Numeric values represent a discrete voltage level corresponding to the signal amplitude. 65535 represents the maximum amplitude (loudest) the signal can be, and the lowest values represent the noise floor of the file, the lowest bit toggling between 0 and 1. Since there are 65536 levels, the noise = (1/65536).

Putting this noise in dB form:

dBnoise = 20 x log (1/65536) = -96.3 dB

The max level in dB form:

dBmax = 20 x log (65536/65536) = 0 dB

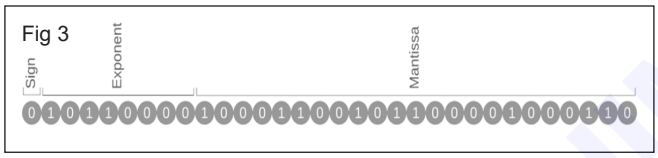
The maximum dynamic range that can be represented by a 16 bit WAV file is (0 dB – (-96.3 dB)) = 96.3 dB

16-bit WAV files, whether in a digital audio recorder or DAW software, call the largest signal captured 0 dBFS,

meaning 0 dB relative to the full-scale (of the file). So, 16-bit WAV files can store audio from 0 dBFS down to -96 dBFS. Each audio sample consumes 16 bits of space on a hard disk or memory, and at a 48 kHz sampling rate this means that 16 x 48,000 = 768,000 bits per second are needed to store a single channel 16-bit, 48 kHz file.

32-bit float

Compared to fixed-point files (16- or 24-bit), 32-bit float files store numbers in a floating-point format. This is fundamentally different than fixed point, because numbers in these WAV files are stored with “scientific notation”, using decimal points and exponents (for example “1.4563 x 106“ instead of “1456300”). This difference is significant because much larger and smaller numbers can be represented compared to a fixed-point representation. The formatting and encoding of the 32-bit word is not intuitive–it has been optimized for computers to be able to perform common math functions on it rather than for human-readability. The first bit indicates a positive or negative value, the next 8 bits indicate the exponent, and the last 23 bits indicate the mantissa. More info is available regarding this format (called IEEE-754). (Fig 3)



The largest number which can be represented is ~3.4 x 1038, and the smallest number is ~1.2 x 10-38. Doing the math:

dBnoise = 20 x log (1.2 x 10-38) = -758 dB

dBmax = 20 x log (3.4 x 1038) = 770 dB

The dynamic range that can be represented by a 32-bit (floating point) file is 1528 dB. Since the greatest difference in sound pressure on Earth can be about 210 dB, from anechoic chamber to massive shockwave, 1528 dB is far beyond what will ever be required to represent acoustical sound amplitude in a computer file.

There is one other aspect of 32-bit float files which is not immediately obvious. Files recorded with 32-bit float record sound where 0 dBFS of the 32-bit file lines up with 0 dBFS of the 24- or 16-bit file. Keep in mind that unlike the 24- or 16-bit files, the 32-bit file goes up to +770 dBFS. So compared to a 24-bit WAV file, the 32-bit float WAV file has 770 dB more headroom.

Modern, professional DAW software can read 32-bit float files. When a DAW first reads a 32-bit file, signals greater than 0 dBFS may first appear clipped since, by default, files are read in with 0 dB of gain applied. By applying attenuation to the file in the DAW, signals above 0 dBFS can be brought below 0 dBFS, undistorted, and used just like any 24- or 16-bit file.

For 32-bit float recording, exact setting of the trim and fader gain while recording is no longer a worry, from a fidelity standpoint. The recorded levels may appear to be either very low or very high while recording, but they can easily be scaled after recording by the DAW software with no additional noise or distortion. This can be seen with these sample files. This is the same source, one recorded with 24-bit fixed and the other with 32-bit float. Both files appear clipped when initially read into DAW software, but the 32-bit file’s gain can be scaled by the DAW.

Each audio sample for 32-bit float files consumes 32 bits of space on a hard disk or memory, and for a 48 kHz sampling rate, this means that 32 x 48,000 = 1,536,000 bits per second are needed for 32-bit, 48 kHz files. So for 33% more storage space compared to 24-bit files, the dynamic range captured goes from 144 dB up to, essentially, infinite (over 1500 dB). But more importantly, audio signals above 0 dBFS are preserved in the file, rendering clipped audio a thing of the past.

Install a Sound Card

Resources required before installation

Opening Your Case

1 Ensure that you need a sound card. Nearly all modern computers have a sound card built into the motherboard. You can double-check that you have a sound card built-in by looking for speaker jacks on the back of the computer. Sound cards are really only necessary for audiophiles and recording studio computers, or for very old computers that don't have built-in sound.

2 Power down your computer and remove all the cables. This will allow you to move your computer to a place that allows you to easily access it. Place the computer on its side on a table, with the ports on the back closest to the table. The ports are connected to the motherboard, so having them closest to the table will ensure that you can get to the motherboard when the case is open.

3 Remove the side panel on your computer. Most newer cases have thumbscrews, but you may need a Phillips-head screwdriver. The screws run down the back of the computer. Remove the panel on the opposite side of the motherboard and set it aside.

4 Ground yourself. You should always ground yourself when working inside your computer. You can use an electrostatic wrist strap or touch a metal water tap to discharge any electrostatic buildup. If you don't ground yourself, you run the risk of damaging your components with electrostatic discharge.

5 Clean out any dust. Since your computer is open, you should take this opportunity to clean out the dust that has built up inside the case. Too much dust can lead to overheating, which can lead to your components failing.

- Use compressed air to remove as much dust and debris as possible. Make sure to get in all of the nooks and crannies.

Installing the Card

1 Locate the PCI slots. These are the slots that you can install expansion cards into. PCI slots are typically white, and you may have 1-5 of them. The slots line up with the removable panels on the back of the case.

- If you're having difficulty identifying the PCI slots, check your motherboard's documentation. You can look this up online if you have the motherboard's model number.

2 Remove the existing sound card (if necessary). If you are replacing an old card, remove the old card first. Having two cards installed will lead to hardware conflicts. Remove the screw securing the card to your case and pull the card directly out of the slot.

- You may need to disconnect the sound card from your CD/DVD drive.
- Make sure that any speakers connected to the old sound card are disconnected before you remove the old card.

3 Insert the new card. Remove the corresponding dust guard panel from the back if you are installing the new card. Make sure that the notches in the slot line up with the card, and press the card straight down firmly. Don't force the card into the slot, and ensure that the ports on the back line up with the with the bay opening.

4 Secure the card with a screw. Screw a single screw into the metal tab that secures the card to the computer chassis. Don't overtighten, but ensure the card is snugly fastened to the case.

5 Connect the sound card to the CD/DVD drive (optional). Some older sound cards may connect to the CD/DVD drive with a small cable. This is optional on virtually all newer computers, as this connection is now handled by the hardware.

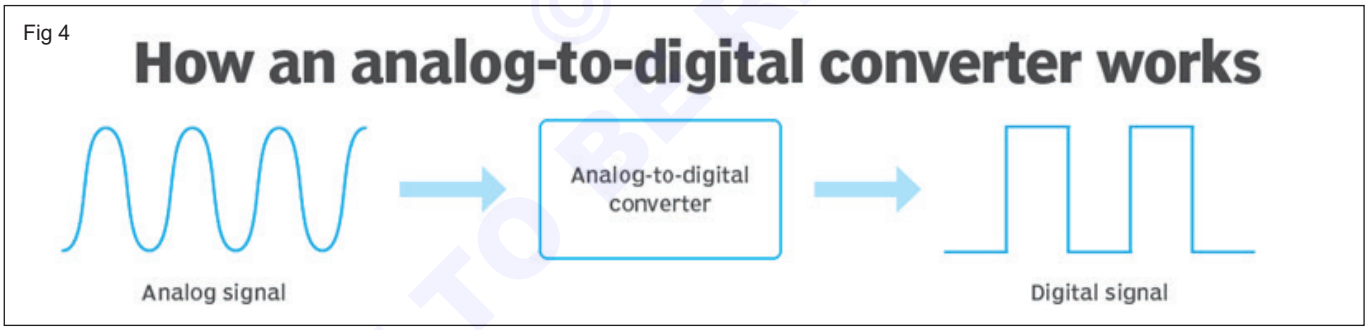
6 Close the case. Return the side panel to the computer and secure it. Place the computer back at your desk and plug the cables back in.

Sound cards working principle

A sound card operates through a digital-analog-converter (DAC) and an analog-digital-converter (ADC) and uses dedicated chips to lessen the CPU load. A preamplifier (preamp) boosts signal levels and controls volume. It may also be able to perform audio processing, such as audio equalization. (Fig 4)

Sound cards used to be expansion cards for early computers, often with ISA or PCI slots. Newer cards use PCIe. However, as audio recording and playback became ubiquitous, and the cost of components decreased, it became common to incorporate basic sound card functionality into the motherboard. Although most computers no longer have physical sound cards, the term "sound card" still refers to the chips and functionality that provide audio output.

Fig 4



External sound cards are typically called audio interfaces, and they usually connect over USB. Advanced sound production and recording require an audio interface with multiple independent audio inputs and outputs. They may also have specialized ports such as XLR.

Sound Card Specifications: When evaluating sound cards, several specifications are key: bit rate, sample rate, signal-to-noise ratio, and the number of channels. These specs determine the clarity, fidelity, and richness of the audio experience.

Advantages of using a sound card

1 **Improved audio quality:** sound card improves the quality of audio produced by devices compared to if they don't have them. For even better quality users can go for external sound cards that have more features. They have lower noise, more detail, and a better soundstage.

2 **Additional audio features:** Sound cards often come with features such as equalization, surround sound, and noise reduction. This means users have more control over the kind of audio they produce.

3 **Better compatibility:** the cards are compatible with a variety of audio devices and musical instruments. This means users can use any instrument to produce the best audio.

Disadvantages of an audio card:

1 **Extra Cost:** External sound card is expensive depending on the type and features that it has.

Additional hardware: expansion card requires space on the computer or laptop to be fixed on. Some computers may not have enough space and if they have they make the computer bulky.

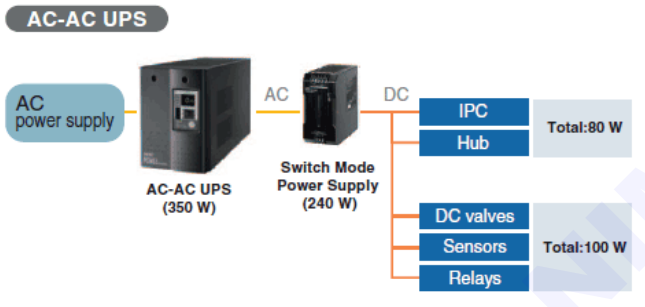
Types of UPS & their Functions

Objectives: At the end of this lesson you shall be able to
- **define UPS**
- **types of UPS**
- **working principle of UPS**
- **UPS fault finding.**

Definition of UPS: Uninterruptible power supplies provide backup power, protecting equipment from damage in the event of grid power failure. An uninterruptible power supply (UPS) is a type of device that powers equipment, nearly instantaneously, in the event of grid power failure, protecting the equipment from damage.

Function of UPS (Fig 1)

Fig 1



A UPS, or a uninterruptible power supply, is a device used to backup a power supply to prevent devices and systems from power supply problems, such as a power failure or lightning strikes.

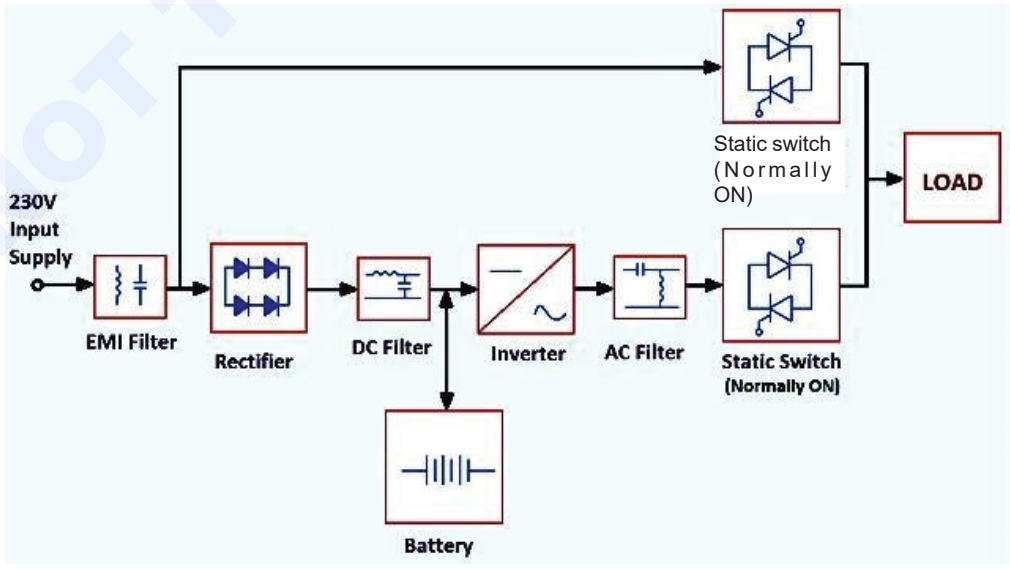
Components of UPS

There are four main components in any online double conversion uninterruptible power supply (UPS) system: Rectifier; UPS Batteries; Inverter; and Static Bypass Switch

Block Diagram of Online UPS

As you can see in the diagram above, there are nine blocks. Let's take a look at each block individually. 1. Inductors and capacitors are used to create an EMI filter. This EMI filter circuit's main purpose is to decrease or filter electromagnetic interferences. 2. To convert AC to DC, this rectifier circuit is used. As this UPS contains a battery, and the battery can only store DC, we must convert the input AC supply to DC. 3. The DC filter circuit is used to filter the impure DC that is produced by the rectifier circuit. The rectifier's DC output contains an AC component. As a result, the filter circuit is utilized to filter out any AC components from the DC supply. 4. The battery is linked to the DC filter circuit's output. The battery will charge when the UPS is connected to the power supply. 5. We have a DC supply now, but we need an AC supply as an output to drive the load. To convert DC to AC, an inverter circuit is required. High-speed solid state switches, such as MOSFETs and SCRs, are used in the inverter circuit. The Inverter Circuit is not necessary if your load requires DC power. 6. The AC filter circuit is used to filter the impure AC that comes from the inverter circuit. 7. Between the AC filter circuit and the Critical Load there is a static switch. According to the stated circumstance, this allows or disallows power flow from the UPS to the load shows the block diagram of online UPS (Fig 2)

Fig 2



Just after EMI filter supply, another static switch is connected between the essential load and the primary power source. The power flow from the main supply to the load is accepted or denied by this switch.

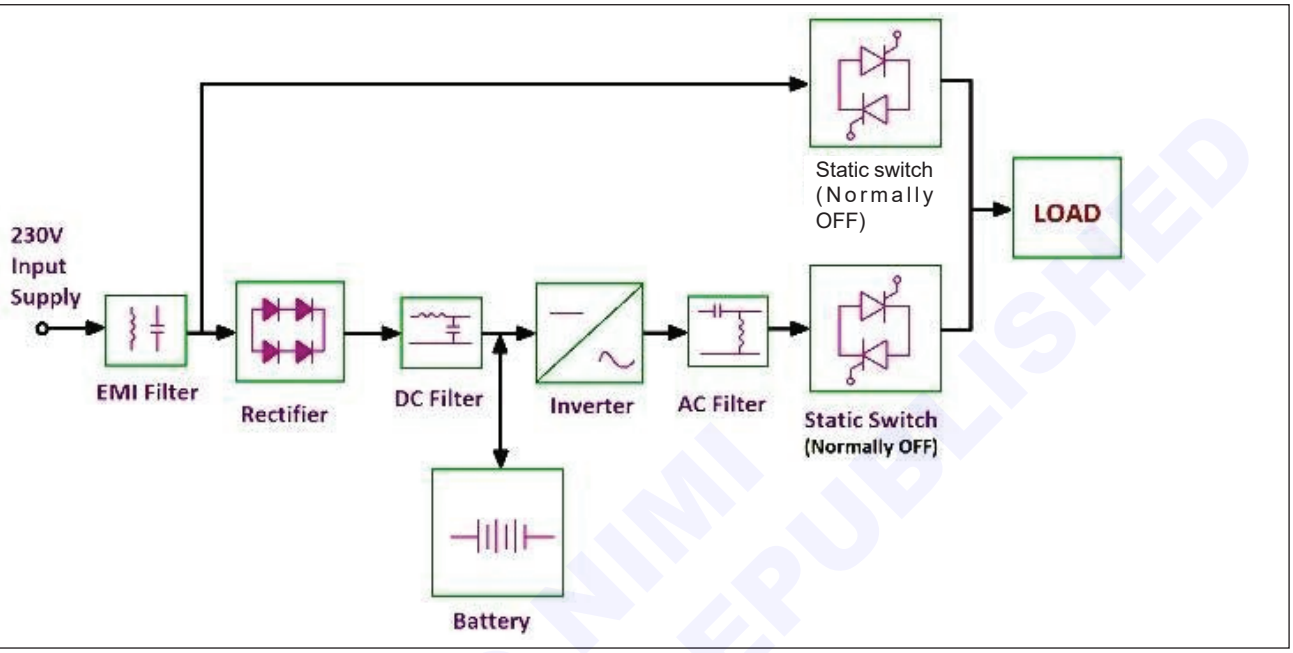
The lower static switch on an Online UPS is generally ON, whereas the upper static switch is normally OFF. As a result, in normal circumstances, power flows from the main supply to the load via the UPS circuits. When the main power supply is unavailable, the load uses the battery for power.

The upper static switch will be ON and the lower switch will be OFF if the UPS is unable to transmit power to the load. As a result, power will flow directly from the main supply to the load in this situation.

Block diagram of Offline UPS:

Now let's come to the block diagram of Offline UPS. (Fig 3)

Fig 3



Offline UPS is identical to that of Online UPS. There is a slight distinction between them.

The upper static switch on an Offline UPS is generally ON, whereas the lower static switch is normally OFF. In normal circumstances, power flows directly from the main supply to the load. The battery will charge at the same time. The upper static switch will be turned off and the lower static switch will be turned on when the main power source is unavailable. As a result, the load draws energy from the battery.

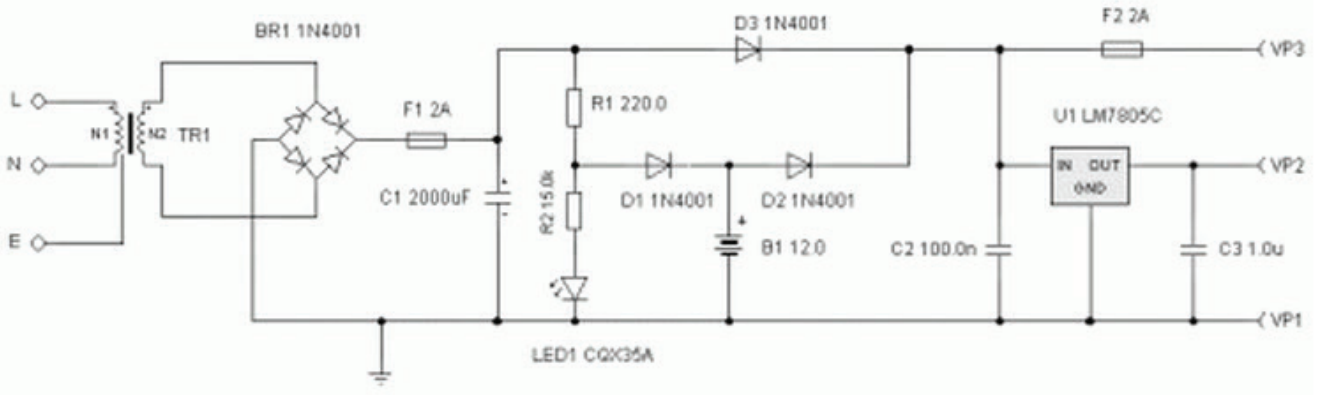
Uninterruptible Power Supply Circuit Diagram and Working

The full form of the UPS is an uninterruptible power source or uninterruptible power supply. It is an electrical device, gives emergency power to various loads when the input power typically fails. A UPS fluctuates from an emergency power system in that it will deliver near-instantaneous safety from i/p power interruptions by providing energy stored in batteries, super capacitors. The run time of battery for most UPS is relatively short but enough to start a standby power source. The main purpose of a UPS is to provide a protection to the equipments like computers, electrical equipment, computer and data centers when there is a power disruption. This device keeps a computer running for a few minutes after a power disruption and protects the data in the computer. In present days, there are various types of UPS systems coming with software component that enables you to automobile backup in case there is no power disruption when you are away from the computer.

Uninterruptible Power Supply Circuit Diagram

The circuit diagram of the UPS is shown below, which shows how the batteries in the equipments controls during a power disruption. The input voltage of the primary winding of the transformer (TR1) is 240V. The secondary winding of the transformer (TR2) can be raised up to 15V if the value is at least 12V running 2 amps. The fuse is used to give the protection to the owl circuit from the short circuits. The electricity presence will cause the led1 to glow. The LED glows will set off upon power disruption and the battery of the UPS will take over. This circuit is designed to provide a more flexible pattern where it can be modified by using different batteries and regulators to offer regulated & unregulated voltages. Using two 12V batteries in series and a positive input of 7815 regulators, we can control a 15 Volts supply Fig 4 shows the circuit diagram of UPS.

Fig 4



Types of UPS

Electrical power supply intrusions can come in a different forms like surges, voltage dips, voltage spikes and harmonics. These troubles can cause serious damage to electrical gears, mostly during the production stages or critical processing of an action. To decrease the risk of power supply distortion, UPS systems are frequently integrated in electrical networks. Electronic power supply equipment makers can offer consistent, high-quality power flow for various electrical load gear and these devices are generally found in industrial processing applications, medical services, emergency gear, telecommunications, & computerized data systems. A UPS system can be a helpful device for ensuring accurate power supply performance.

Uninterruptible Power Supply devices are classified into three types such as

- The Standby UPS
- The Line Interactive UPS
- Online UPS

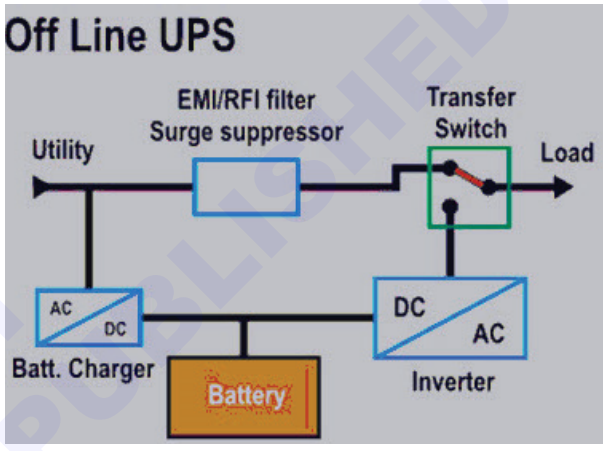
The Standby UPS

The standby Uninterruptible Power Supply is also called as off line UPS, that is generally used for PCs. The block diagram of this UPS is shown below. This UPS includes a battery, an AC or DC & DC or AC inverter, a static switch and a LPF which is used to decrease the switching frequency from the o/p voltage & a surge suppressor. The standby UPS system works with the switch arrangement to select the AC i/p as a primary power source, and interchanging to the battery & inverter as backup sources in case of primary power gets disrupted. The inverter normally relies on standby, only triggering when the power fails and the transfer switch routinely switches the load to the backup units. This kind of UPS system offers a small size, high degree of efficiency, & pretty low costs, making of this UPS is easy. (Fig 5)

The Line Interactive UPS

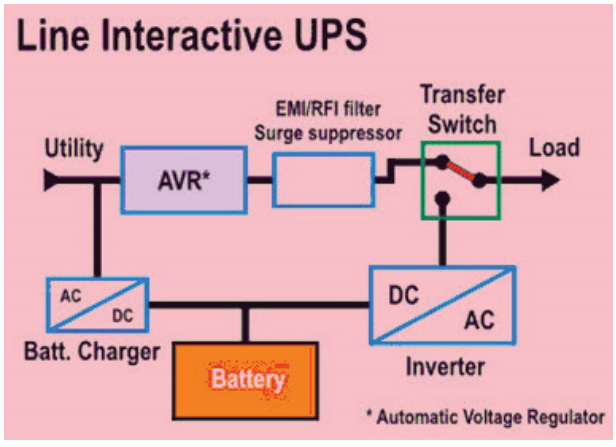
The block diagram of Line Interactive UPS is shown below, it is the most common UPS used for small

Fig 5



business. The designing of line interactive UPS is alike to a standby UPS, in addition the design Line Interactive generally includes an automatic voltage regulator(AVR) or a tap-changing transformer. This enhances the regulation of voltage by regulating transformer taps as the i/p voltage differs. Voltage regulation is a significant feature when the conditions of a low voltage exist, otherwise the UPS would transfer to battery & then finally down the load. The usage of more common battery can cause early battery failure. The features of this UPS are small size, low cost, high efficiency can make the UPS in the range of 0.5-5kVA power. (Fig 6)

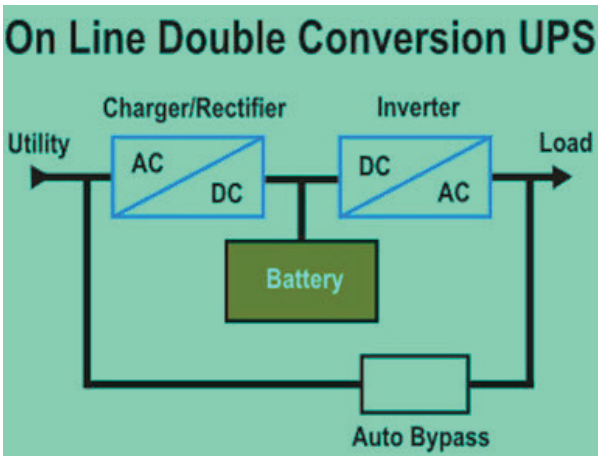
Fig 6



Online UPS

The online UPS is also called as double conversion online uninterruptible power supply. This is the most commonly used UPS and the block diagram of this UPS is shown below. The designing of this UPS is similar to the Standby UPS, excluding that the primary power source is the inverter instead of the AC main. In this UPS design, damage of the i/p AC does not cause triggering of the transfer switch, because the i/p AC is charging the backup battery source which delivers power to the o/p inverter. So, during failure of an i/p AC power, this UPS operation result in no transfer time. (Fig 7)

Fig 7



In this design, both the inverter and the battery charger change the total load power flow, resulting in reduced efficiency with its associated increased heat generation. This UPS affords nearly perfect electrical o/p performance. But the constant wear on the power components decreases reliability over further designs and the energy spent by the electrical power inefficiency is an important part of the life-cycle cost of the UPS. Also, the i/p power drawn by the large battery charger has been frequently non-linear and can interfere with the building power wiring with standby generators.

UPS Working Principle and Types – Offline and Online UPS Systems

UPS stands for the uninterrupted power source. As the name implies, it is used to provide a continuous power supply to the load using an automatic switching method; to prevent the device and equipment from damage or preventing the plant from going into a shutdown mode.

There are many devices that require a safe shutdown for proper operation; otherwise, sudden power loss can damage the equipment.

A simple example can be considered a computer. Not properly shutting it down due to abrupt power off can corrupt its operating system or cause some other damage.

A UPS in this case will provide power for some time; so that the device shuts off properly. Though the time is short; it will provide a safe shut down for a device.

A UPS takes AC supply, stores it in batteries and these batteries then feed the power back to the load device in case of mains power failure. This is the basic working of UPS.

Every UPS has a semiconductor static switch, which is used to switch power between the main AC supply and batteries to the load. Failure of this switch can cause the UPS to be worthless because it will damage the working of UPS.

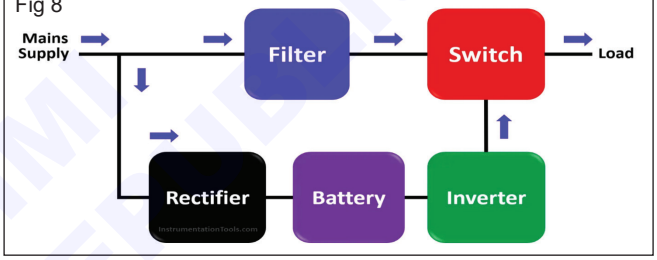
The basic components of UPS are – a rectifier (conversion of AC to DC for feeding batteries), inverter (conversion of DC to AC for feeding load), battery (for providing DC power to the inverter), and a semiconductor switch for switching load transfer between mains AC supply and inverter supply.

Offline UPS Working Principle

The offline UPS is also called standby UPS.

The Offline UPS is the simplest one of all types. As you can see, the load is normally supplied power from mains AC supply. (Fig 8)

Fig 8



The AC supply is also used to charge the battery bank. The battery is used to feed DC power to the inverter; for converting it to AC supply.

When the mains supply fails, the switch will automatically cut off power from it and supply power to the load from the inverter circuit.

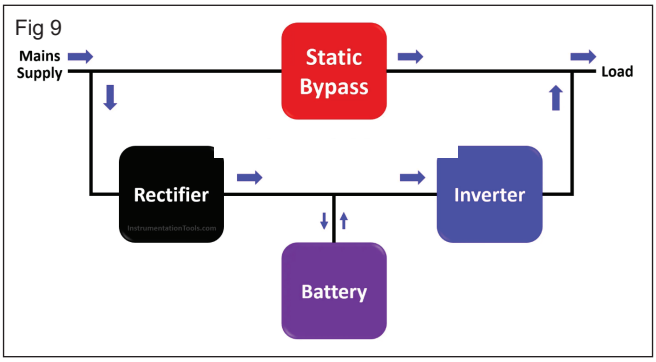
The switching time is usually around 25 milliseconds. This type of inverter is the least expensive one; because the main issue is the large switching time.

Online UPS Working Principle

The online UPS is a complex type of UPS. As you can see, the load is normally supplied power from the inverter.

The AC supply is used to charge the battery bank through a rectifier, as well as supply DC power to the inverter. (Fig 9)

Fig 9



When the main supply fails, the battery will automatically supply power to the inverter. The rectifier will be bypassed in this case.

One more added feature is the addition of a static bypass switch. When the UPS fails (means failure of the inverter, battery, or rectifier), this switch is turned on which supplies direct AC power to the load as shown in the above figure.

The switching time is usually very low (around 4-5 milliseconds; between inverter circuit and static bypass switch). Apart from this, the online UPS is very fast in operation; because the battery immediately supplies power to the inverter in case of mains AC failure.

The output type of UPS is a pure sinusoidal waveform and is a perfect replacement for the mains AC supply in case of power failure. It will provide temporary power to the load for a time based on battery backup or resumption of AC power.

Main components of UPS system

There are four main components in a UPS system:

1 The UPS batteries

2 The Rectifiers

3 The Inverter

4 The Static bypass switch

What are UPS Batteries?

The UPS batteries are the “heart” of any UPS system. UPS batteries are the source of emergency power in the event of a power loss. During a utility power failure, the UPS batteries support the connected load. Either the rectifier or a separate charger ensures that the batteries are always charged.

There are several types of UPS batteries, but the most common are

1 Valve Regulated Lead Acid (VRLA),

2 Flooded Wet Cell (commonly called VLA), and

3 Lithium-Ion.

All UPS systems contain at least one “string” of batteries, or a connected number of required batteries. The number of batteries in a string will depend on the UPS system’s DC (direct current) voltage. In smaller UPS systems, battery strings might be housed inside the UPS unit itself. In larger UPS systems, batteries may look like separate pieces.

Because batteries are connected in strings, and the strings are connected in a series, if one battery goes bad, it could cause the entire UPS system to fail. For this reason, the regular inspection and maintenance of UPS batteries is critical, regardless of their age.

UPS Rectifier

The rectifier serves a few critical functions. First, the rectifier is the piece of the UPS system that converts input power from AC, or alternating current, to DC, or direct current. DC power routes to the inverter. This is the first half of a double conversion process.

UPS Inverter

The inverter is another key part of the double conversion process. The double conversion process works as a filter for events like electricity surges or spikes, and electrical noise.

As explained above, the rectifier converts input power from AC to DC power, and DC power routes back to the inverter. The inverter works as part of the double conversion process by converting the DC voltage back to AC output. This AC output is what powers the critical load.

The conversion process basically looks like AC -> DC -> AC again. The output of the process should be a pure sine waveform.

UPS Static Bypass Switch

The UPS static bypass switch is the superhero in the event of a failure of the UPS system. The status bypass switch works as a safeguard, automatically connecting the load to the main supply.

The static bypass switch gets its name because in the event of a system failure, it bypasses the other three main UPS system components (the rectifier, batteries, and inverter.)

The static bypass switch is a backup. It doesn’t perform the filtering function like the double conversion process described above. However, the existence of the static bypass switch within a UPS system ensures the system can keep working on utility power in the event the batteries, inverter or rectifier fail. Please keep in mind that some components cannot safely be worked on while the UPS is in Static Bypass. That is why FCG recommends adding an external maintenance bypass to any critical UPS application

An External Maintenance Bypass

An External Maintenance Bypass is a separate device consisting of breakers (sometimes a rotary switch) and bussing that allows the user to completely isolate the UPS system from power while still providing Utility power to the load. In other words, the allows utility power to wrap around the UPS system and shut power off to the UPS and Batteries without dropping the load.

In some cases, with the use of an External Maintenance Bypass, you can completely remove an older UPS and replace it with a brand new unit without losing power to the load.

Other Parts of UPS Systems

Depending on your specific UPS system, and its size and type, your system may include several other components. Your UPS system might include fans, capacitors, external maintenance bypass, or transient volt surge suppressors, for example.

Scheduling preventative maintenance visits are crucial to preserving the functionality of your UPS system. FGC Service offers a wide variety of maintenance services of Uninterruptible Power Systems, including emergency service, NOC monitoring, site surveys, generator & HVAC service, rental services, and construction management.

We understand the importance of proper UPS battery maintenance and the technical requirements needed to install and recycle any string of batteries.

To speak with one of our product specialists directly, we invite you contact us or start a chat with our team in the chat feature at the bottom right corner of this page!

UPS management, maintenance

In order to keep your UPS operating at maximum efficiency, simple preventive maintenance should be performed on a regular basis. In the past, it was difficult to test and monitor a UPS. However new designs provide users simpler, yet more advanced ways to monitor their UPS. Today's UPS models are designed to provide regular, automatic status updates.

Despite the inclusion of self-monitoring software and auto-notification features of many new UPS models, timely inspections are still necessary to assure a UPS is operating properly. Proper care and regular maintenance will help avoid unnecessary downtime, saving time and money. Most serviceable UPS components are designed to be touch-safe to ensure the safety of the person servicing the device; however it is still important to keep safety at the forefront when servicing the UPS. The UPS is directly connected to a source of power, and general electrical safety precautions should always be taken. When providing maintenance inspections to the UPS, the following general best practices are recommended:

Be proactive: This is always the best approach to both battery and UPS replacement. UPSs that have been in service for more than 5 years have a higher risk of unanticipated downtime due to the increased likelihood of internal component failure.

Be prepared: battery replacements could be kept on site to increase availability and avoid downtime.

Be organized: Maintenance inspections should be scheduled routinely to keep the user up to date on UPS operations. This should include documentation of the performed inspections and the date on which the inspection was performed. Scheduling and performing preventative maintenance is vital to getting the most out of UPS systems. However, simply performing the inspections is not sufficient. Keep records of the type of maintenance performed and the condition of the equipment. Keeping detailed records of maintenance performed and areas of degradation (e.g., reduced battery runtime) will aid the user in predicting failures as well as help the support team if a problem does occur in the future. Due to the important equipment and information UPSs are designed to protect, they generally tend to be reliable and durable, however there is still a chance that an older UPS could malfunction mechanically or electronically. The following are the most common causes of a UPS failure:

- Batteries
- Fans
- Electrolytic Capacitors
- Metal Oxide Varistors (MOVs)
- Relay

Batteries and Maintenance

One of the most important parts of an UPS is the battery. The battery is the source of power when the mains supply fails. Proper working of UPS depends on the condition and capability of the battery being used.

Battery types: Commonly the following four types of batteries are used with UPS systems.

- Automobile batteries
- Tubular/Industrial lead acid batteries
- Sealed maintenance free (SMF) batteries
- Nickel - Cadmium batteries

All these batteries are available in different shapes, sizes and capacities.

Automobile batteries

These batteries are commonly used in the automobiles, car, trucks etc. These batteries are the cheapest of the batteries used in the inverter and are commonly available. A good quality automobile Lead Acid battery has a life span of only about 250-300 full charge/ discharge cycles. To increase battery life one can use a higher capacity battery than the required. These batteries require frequent topping up with distilled water.

Tubular / Industrial lead acid batteries

Compared to the automobile batteries, these batteries are designed for the heavy duty charge/discharge required by the inverter. These batteries have a operating life of more than 1000 charge/discharge cycles. These batteries are costlier than the automobile batteries, but have long life (6-8 years) These batteries too require topping up with distilled water if the acid level gets reduced. Some low maintenance batteries of Tubular/Industrial Lead Acid type are also available.

Tubular/Industrial Lead Acid batteries are to be checked by battery capacity meter which contains capacity and load tester. For checking 12V battery, the load tester should show the readings between 12 to 16V then the battery is ok. If the meter indicates less than 10V, then the battery is defective.

The electrolyte in the battery consists of sulphuric acid and water in proper ratio. Due to high temperature the water evaporates. As the sulphuric acid does not get evaporate, the PH value of electrolyte increases. This increased PH value of battery electrolyte cause damage to the cell plates.

Also, the reduced level of electrolyte and acid gives low ampere current output from the battery.

Thus in a Lead Acid battery the water level of the battery should be checked and maintained every 15 days. This is more important in the summer season.

Sealed Maintenance Free (SMF) batteries: These batteries are completely sealed and they do not require any kind of regular maintenance. These batteries do not contain any wet acid, these are Lead-Paste batteries. This allows the user to store these batteries in any position and also allows these batteries to be used inside the UPS. These batteries are smaller in size.

Sealed maintenance free batteries do not require any maintenance. However it is advised to discharge with the equipment and charge the battery once in 3 months, if the battery is kept idle.

Battery rating: Commonly batteries are available in 6V, 12V and 24V rating. Other than the voltage rating the ampere hour (AH) rating is used to define the power availability or capacity of the battery. The backup time provided by a UPS depends on the rating of the battery used in the system. The no. of batteries required depends on the DC Bus voltage of the inverter. It could be 24V, 48V, 72V, 120V and so on. Batteries are connected in series for higher voltage requirements. When connecting more than one battery in a bank, make sure that the AH ratings are same for all the batteries in one bank.

Battery charging methods

- Constant voltage
- Constant current
- Constant voltage constant current

Constant voltage: This type of charging method uses series, regulators for charging SMF batteries. This method will be useful for charging automobile and tubular/Industrial Lead Acid batteries.

Constant current: This charging method using shunt regulators is good for the automobile and tubular/ Industrial Lead-Acid batteries. But it can damage the SMF batteries by overcharging them.

Constant voltage constant current: This method has advantages of both the constant voltage and the constant current. This charging method is suitable for automobile and tubular/Industrial Lead Acid batteries and also for the SMF batteries. This method provides regulated charging to improve the battery life significantly.

Trickle charging: The word trickle basically means to slow flow of something such as water. In an UPS when the mains AC are available the battery gets charged. After the battery is fully charged the charger is cut-off after the battery gets fully charged. If the charger is not cut-off, then the battery will get damaged. Trickle charging is a special charging method used to keep the battery constantly in full charge position. Normally, for the trickle charging 100th part of the normal charging current is provided to the battery.

Batteries maintenance

No battery lasts forever, and UPS batteries are no different. However, the life span of the battery can be maximized by operating your UPS under the manufacturers' recommended conditions which are typically described in the user manual. To help users monitor their UPS, newer units have been equipped to alert the user when the battery is approaching the end of its useable life via:

- Predictive battery replacement dates
- Temperature-compensated charging
- Automated self tests

The most commonly used battery type in a UPS is a

valve-regulated lead-acid (VRLA) battery. The forecasted life span of these batteries is typically 3 to 5 years under the manufacturers' recommended conditions; however, this life expectancy will fluctuate greatly depending on five factors: placement, ambient temperature, cycling, maintenance, battery chemistry, and battery storage. Being proactive and aware of these characteristics and conditions will help maximize the life expectancy of a UPS and prepare for any imminent power failures.

Place of Installation - When installing a UPS, the user must determine where to install the unit to best provide power protection of the IT equipment in the room. It is recommended that the UPS be installed in a temperature-controlled environment. The UPS should not be placed near open windows or areas that contain high amounts of moisture; and the environment should be free of excessive dust and corrosive fumes. Do not operate the UPS where the temperature and humidity are outside the specified limits. The ventilation openings at the front, side, or rear of the unit must not be blocked.

Battery storage - Proactive UPS owners may seek to purchase a replacement battery before one is necessary in order to avoid the potential consequences of downtime. While this is an acceptable and even recommended practice, there are a few important factors to consider when placing your UPS battery into storage. Inevitably, an unused battery will experience a life cycle decrease. Lead-acid batteries used in UPS units experience automatic self-discharge; therefore it is recommended that a battery in storage be charged

every 6 months. Regardless of the frequency of battery recharge, cumulative storage time should not exceed one year. Failure to follow these recommendations will result in permanent loss of capacity within 18 to 30 months. If it is not feasible to charge a battery while in storage, it is recommended that the battery be stored at 10°C (50°F) or less. Doing so will slow the degradation cycle of the battery, and help to maximize its life expectancy.

Fans

As discussed in the previous section, temperature can have a significant impact on the life expectancy of UPS components. To lessen the effects of heat, most UPSs are equipped with fans to help cool the unit, and keep the ambient temperature within the recommended temperature range. Under recommended conditions fans in UPS units have a life expectancy of up to 10 years. The fan's life expectancy is strongly dependent on the environment the UPS is placed in. In a typical UPS, the fan will turn on or speed up under the following circumstances:

- Utility power is not available, and the UPS is forced to go on battery.
- The temperature within the unit surpasses a predetermined level - usually ~38°C (100°F).
- The load attached to the unit surpasses a predetermined threshold - usually between 70% and 80% of operating capacity.

The only way to prolong the life of the fan in a UPS is to limit the scenarios when it is forced to operate. Therefore keeping the ambient temperature within the specified range, monitoring the UPS for unusual or frequent cycling, and choosing a properly sized UPS that can comfortably support the attached load should maximize the life of the fan.

Relays

Similar to MOVs, the life expectancy of the relays within a UPS is difficult to predict. Relays are electrically operated switches which allow the UPS to operate and switch between on and off battery. Under normal circumstances, it is unlikely a UPS will cycle enough times to cause a relay failure, however incorrect or malfunctioning firmware setup could result in overuse, and an eventual failure. Unusually high cycling could indicate that the UPS is not operating properly, and the relays, as well as the battery may be suffering. Having the awareness to notice when these problems are occurring should allow a user to be proactive, and adjust the firmware settings to prevent substantial damage before it occurs.

Table summarizes the life expectancy and factors affecting the life of the five components discussed above

Table

Components	Function	Life expectancy	Factors affecting life
Battery	Provides power when utility power is not available	3-5 Years	• UPS placement • Ambient temperature • Cycling frequency • Maintenance • Battery chemistry • Battery storage
Fans	Provides cooling to the unit	upto 10 Years	• Load on the unit • Ambient temperature • Frequency of use • Duration of use
Electrolytic capacitors	Smoothness out and filters	upto 10 Years	• Ambient temperature • Humidity
Metal oxide	Protects circuits against	Variable	• Dependent on the number and severity of surge events.
Relays	Electrically operate switch	Variable	• Abnormal cycling

The importance of UPS management

While providing preventative maintenance is crucial to maximizing expected life, providing proper management optimizes the performance and capabilities of a UPS. Many manufacturers now offer software designed to provide protection, manageability, compatibility and convenience. Advanced management software should offer UPS configuration & control, safe system shutdown, and energy reporting capabilities. This reporting helps provide a greater understanding of the energy consumed by IT equipment enabling optimal energy usage.

Advanced analysis features can help to identify the causes of potential power related problems before they occur; ensuring the health of protected equipment. In addition to the management software, some manufacturers also offer management cards for proactive, 24x7 management and monitoring from a single software application.

These cards typically provide notification features that inform a user of problems as they occur. Fig 10 shows an example of a management card.

Fig 10

End-of-life (EOL)

Inevitably, every UPS will eventually reach the end of its usable life, however proper oversight and maintenance will ensure you maximize the life of your UPS. Depending on the factors discussed above, UPS being operated under recommended conditions have a life expectancy of up to 10 years with at least one battery replacement; however it may be wise to pursue a unit replacement before the UPS experiences a failure. While the UPS may continue to operate up to or even beyond 10 years, the efficiency of the UPS will likely begin to decline beforehand. In addition to the efficiency degradation considerations, by the time your UPS is 5+ years old, it is likely that extensive improvements and features have been implemented, some of which may be necessary for your new applications. As technology continues to advance, power requirements for equipment are growing rapidly. Older UPS technology combined with an efficiency deterioration likely make it beneficial to pursue unit replacement well before the UPS experiences a failure. Therefore, for mission critical applications that will not allow for downtime, a replacement unit should be pursued when the UPS efficiency begins to decline.

UPS Rating

The power rating of electrical equipment may be stated in Watts (W) or Volt Amperes (VA). UPS manufacturers generally use VA (or KVA) to describe the UPS output ratings, and it is this rating which determines the

maximum load that can continuously be supported by the UPS when the mains supply fails.

When selecting a UPS to service a particular load it is important that the combined load does not exceed the UPS output rating, and if the load equipment is specified in Watts it is necessary to convert this to VA in order to assess the UPS/load rating compatibility.

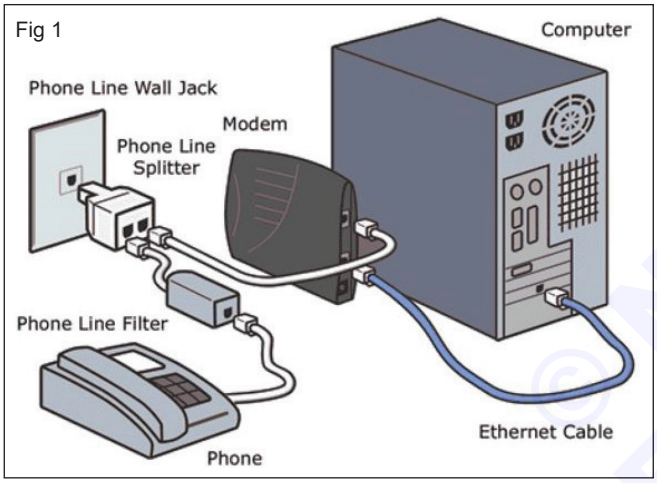
Modem Fundamentals

Objectives: At the end of this lesson you shall be able to
- **Define MODEM**
- **Define band width and band rate**
- **List out the types of modem.**

Definition of modern: A modem is a hardware which connects to a computer, broadband network or wireless router. Modem converts information between analogue and digital formats in real time making seamless two-way network communication. The full form of Modem or modem stands for modulator demodulator Fig 1 shows the modern connecting layout diagram.

Modem converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio.

Fig 1



There are following different types of Modem

- Cable Modems. Cable modems help in establishing communication between computer and ISP over landline connection. ...
- Telephone Modems. ...
- Dial modems. ...
- Satellite Modems. ...
- Digital Subscriber Line (DSL)

Types of Modem in Computer Network

- External Modem. External Modem in Computer System is connected to the computer system with the help of a serial cable. ...
- Internal Modem. ...
- Wireless Modem. ...
- Dial-Up Modem. ...
- Cable Modem. ...
- DSL Modem. ...
- Satellite Modem. ...
- Half-Duplex Modem.

A hardware Modem will have three components:

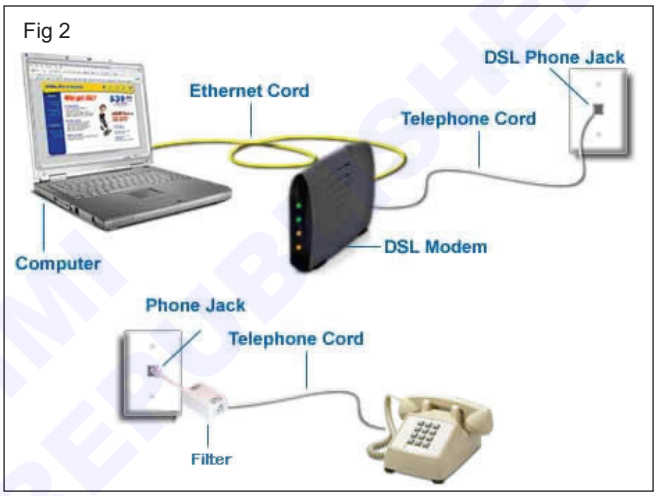
1 The Microcontroller Unit (MCU),

2 The Data Pump Unit (DPU),

3 The Data Access Arrangement (DAA).

DSL modem (Fig 2)

Fig 2

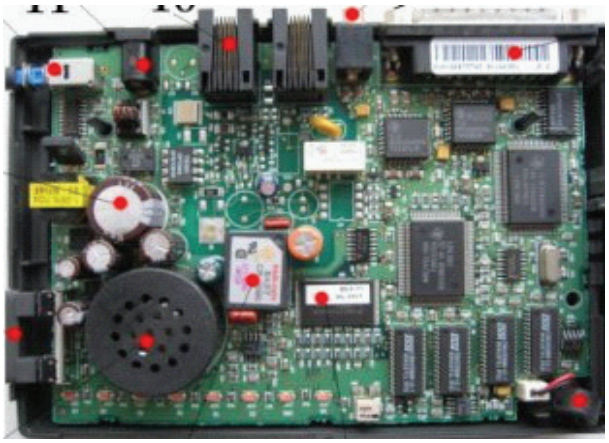


DSL (Digital Subscriber Line) is a modem technology that uses existing telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL provides dedicated, point-to-point, public network access.

Parts inside a Modem

Lift the lid on a dialup modem and this is what you'll find inside Fig 3 shows the modern main board components.

Fig 3



1 **On/off button:** Spring-loaded switch turns the power on and off.

2 **Capacitors:** Have a variety of jobs to do in a modem, including smooth out current peaks.

3 **Volume control:** Controls the loudspeaker volume.

4 **Loudspeaker:** Relays what's happening on the phone line as your modem dials.

5 **Modem chip:** Modulates (add digital information to the outgoing telephone signal) and demodulates (separate the digital information from the incoming signal).

6 **Other chips:** Control modem chip and other components.

7 **Microphone:** Allows you to send your own voice down the phone line.

8 **Serial connection:** Connects the modem to your computer's serial (RS-232) port. Newer modems connect to the USB port instead.

9 **Microphone socket:** Connects an external microphone so you can record messages in higher quality than if you use the built-in microphone.

10 **Telephone sockets:** Connect your modem to a phone socket with a standard (RJ11) telephone cable. There's a second socket where you can plug a telephone handset into your modem. This lets you to use your phone through the modem when your computer's not already using the line.

11 **Power input:** Connects the modem to an external power supply unit (electricity transformer) to your modem.

Modem functionality

Other than choosing a modem based on the type of internet connection there are a few other variables or requirements that should be looked for before purchasing.

1 **Compatibility -** Is the modem compatible with your computer (Windows, Mac, Linux, etc)? Furthermore, is it compatible with your computer's software (7, Vista, 10.4, etc)?

2 **Upload/download speeds -** Check the "upstream" and "downstream" speeds, as they'll differ from model to model. Often times it'll even be different from one direction (upload) to the next (download).

3 **Security -** Does the modem support security features such as WPS (WiFi Protected Setup), WPA/WPA2 Security Protocol and WEP, TKIP and AES (64/128 bit) Encryption?

4 **Size & mounting options -** How big/small is the modem? Will it fit well with the computer equipment? Some modems can even be attached to the wall.

5 **Price -** Modems vary in price from as little as Rs.1000 to as much as Rs 4000. The difference in price comes down to the type of connection and speeds.

WiFi vs DSL

While DSL is a method of connecting to the internet via telephone lines, WiFi refers to a wireless technology that allows devices to connect to a local internet network without physical cables. Here's a comparison: Connection Type: DSL is a wired connection, while WiFi is wireless.

ADSL modem (Fig 4)

Fig 4

Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.

The advantages of ADSL:-

- High-quality, reliable broadband connection.
- Internet access at the same time as making phone calls.
- Faster data transmission through a single connection.
- Connect to internet-enabled devices

Data card (Fig 5)

Fig 5

A data card and a dongle are both devices used to access the internet on a computer or other devices. A data card is a device that can be inserted into a computer's USB port to provide internet connectivity. It usually requires a SIM card to connect to a mobile network

Dongle (Fig 6)

Fig 6

A dongle is essentially a portable USB device that behaves like a small modem. You might hear it called other names, like internet stick, USB modem or USB network adapter. They all mean the same thing. Just plug a dongle into your computer's USB port and you'll get instant internet access, no software necessary.

Applications of modem

Some of these applications include data transfers, remote management, broadband backup, Point of Sale, Machine to Machine among many others.

Definition of bandwidth

The maximum amount of data transmitted over an internet connection in a given amount of time. Bandwidth is often mistaken for internet speed when it's actually the volume of information that can be sent over a connection in a measured amount of time – calculated in megabits per second (Mbps).

Bandwidth of Modem

A standard PC modem converts analog phone signals to digital data transmissions for data coming into the PC and vice versa. PC modems deliver bandwidth at transmission speeds of 14.4K bit/sec., 28.8K bit/sec. and 56K bit/sec. Modem speeds above 56K bit/sec.

Baud rate of modem

The baud rate is a measure of how many times per second a signal (for instance that sent by a modem) changes. For example, a baud rate of 1200 implies one signal change every 833 microseconds. Common modem baud rates are 50, 75, 110, 300, 600, 1200, and 2400. Most high speed modems run at 2400 baud.

Modem baud rates list

Standard baud rates include 110, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 128000 and 256000 bits per second.

Wireless and wired communication

Wired communication systems use cables, wires, or optical fibers to connect the devices. Wireless communication systems use electromagnetic waves, such as radio, microwave, or infrared, to transmit signals through the air or space.

Wireless communication

The term wireless communication was introduced in the 19th century and wireless communication technology has developed over the subsequent years. It is one of the most important mediums of transmission of information from one device to other devices. In this technology, the information can be transmitted through the air without requiring any cable or wires or other electronic conductors, by using electromagnetic waves like IR, RF, satellite, etc. In the present days, the wireless communication technology refers to a variety of wireless communication devices and technologies ranging from smart phones to computers, tabs, laptops, Bluetooth Technology, printers. (Fig 7)

Fig 7

Types of wireless communications

Introduction to wireless communication

In the present days, wireless communication system has become an essential part of various types of wireless communication devices, that permits user to communicate even from remote operated areas. There are many devices used for wireless communication like mobiles. Cordless telephones, Zigbee wireless technology, GPS, Wi-Fi, satellite television and wireless computer parts. Current wireless phones include 3 and 4G networks, Bluetooth and Wi-Fi technologies.

Types of wireless communication

The different types of wireless communication mainly include, IR wireless communication, satellite communication, broadcast radio, Microwave radio, Bluetooth, Zigbee etc.

Satellite communication (Fig 8)

Fig 8

Satellite communication is one type of self contained wireless communication technology, it is widely spread all over the world to allow users to stay connected almost anywhere on the earth. When the signal (a beam of modulated microwave) is sent near the satellite then, satellite amplifies the signal and sent it back to the antenna receiver which is located on the surface of the earth. Satellite communication contains two main components like the space segment and the ground

segment. The ground segment consists of fixed or mobile transmission, reception and ancillary equipment and the space segment, which mainly is the satellite itself.

Infrared communication (Fig 9)

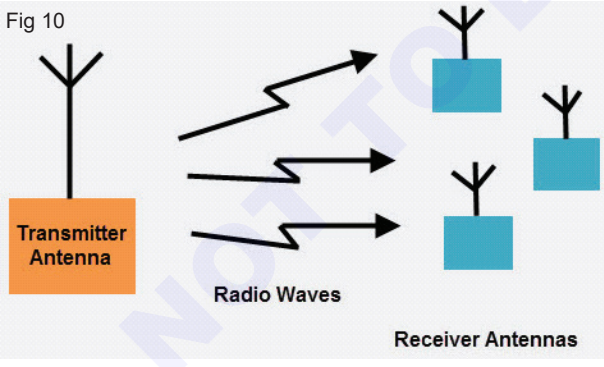
Fig 9

Infrared wireless communication communicates information in a device or systems through IR radiation. IR is electromagnetic energy at a wavelength that is longer than that of red light. It is used for security control, TV remote control and short range communications. In the electromagnetic spectrum, IR radiation lies between microwaves and visible light. So, they can be used as a source of communication.

For a successful infrared communication, a photo LED transmitter and a photo diode receptor are required. The LED transmitter transmits the IR signal in the form of non visible light, that is captured and saved by the photoreceptor. So the information between the source and the target is transferred in this way. The source and destination can be mobile phones, TVs, security systems, laptops etc supports wireless communication.

Broadcast radio (Fig 10)

Fig 10



The first wireless communication technology is the open radio communication to seek out widespread use, and it still serves a purpose nowadays. Handy multichannel radios permit a user to speak over short distances, whereas citizen's band and maritime radios offer communication services for sailors. Ham radio enthusiasts share data and function emergency communication aids throughout disasters with their powerful broadcasting gear, and can even communicate digital information over the radio frequency spectrum.

Mostly an audio broadcasting service, radio broadcasts sound through the air as radio waves. Radio uses a transmitter which is used to transmit the data in the form of radio waves to a receiving antenna(Different Types of Antennas). To broadcast common programming, stations are associated with the radio N/W's. The broadcast happens either in simulcast or syndication or both. Radio broadcasting may be done via cable FM, the net and satellites. A broadcast sends information over long distances at up to two megabits/Sec (AM/FM Radio).

Radio waves are electromagnetic signals, that are transmitted by an antenna. These waves have completely different frequency segments, and will be ready to obtain an audio signal by changing into a frequency segment.

For example, you can take a radio station. When the RJ says you are listening to 92.7 BIG FM, what he really means is that signals are being broadcasted at a frequency of 92.7megahertz, that successively means the transmitter at the station is periodic at a frequency of 92.700,000 Cycles/second.

When you would like to listen to 92.7 BIG FM, all you have to do is tune the radio to just accept that specific frequency and you will receive perfect audio reception.

Microwave communication (Fig 11)

Fig 11

Microwave wireless communication is an effective type of communication, mainly this transmission uses radio waves, and the wavelengths of radio waves are measured in centimeters. In this communication, the data or information can be transformed using two methods. One is satellite method and another one is terrestrial method.

Wherein satellite method, the data can be transmitted though a satellite, that orbit 22,300 miles above the earth. Stations on the earth send and receive data signals from the satellite with a frequency ranging from 11GHz-14GHz and with a transmission speed of 1Mbps to 10Mbps. In terrestrial method, in which two microwave towers with a clear line of sight between them are used, ensuring no obstacles to disrupt the line of sight. So it is used often for the purpose of privacy. The frequency range of the terrestrial system is typically 4GHz-6GHz and with a transmission speed is usually 1Mbps to 10Mbps.

The main disadvantage of microwave signals is, they can be affected by bad weather, especially rain.

Wi-Fi (Fig 12)

Fig 12

Wi-Fi is a low power wireless communication, that is used by various electronic devices like smart phones, laptops, etc. In this setup, a router works as a communication hub wirelessly. These networks allow users to connect only within close proximity to a router. WiFi is very common in networking applications which affords portability wirelessly. These networks need to be protected with passwords for the purpose of security, otherwise it will access by others.

Mobile communication systems (Fig 13)

Fig 13

The advancement of mobile networks is enumerated by generations. Many users communicate across a single frequency band through mobile phones. Cellular and cordless phones are two examples of devices which make use of wireless signals. Typically, cell phones have a larger range of networks to provide a coverage. But, Cordless phones have a limited range. Similar to GPS devices, some phones make use of signals from satellites to communicate.

Bluetooth Technology (Fig 14)

The main function of the Bluetooth technology is that permits you to connect a various electronic devices wirelessly to a system for the transferring of data. Cell phones are connected to hands free earphones, mouse, wireless keyboard. By using Bluetooth device the information from one device to another device. This technology has various functions and it is used commonly in the wireless communication market.

Fig 14

Advantages of wireless communication

- Any data or information can be transmitted faster and with a high speed
- Maintenance and installation is less cost for these networks.
- The internet can be accessed from anywhere wirelessly
- It is very helpful for workers, doctors working in remote areas as they can be in touch with medical centers.

Disadvantages of wireless communication

- An unauthorized person can easily capture the wireless signals which spread through the air.
- It is very important to secure the wireless network so that the information cannot be misused by unauthorized users.

Applications of wireless communication

Applications of wireless communication involve security systems, television remote control, Wi-Fi, Cell phones, wireless power transfer, computer interface devices and various wireless communication based projects.

Synchronous and Asynchronous Transmission

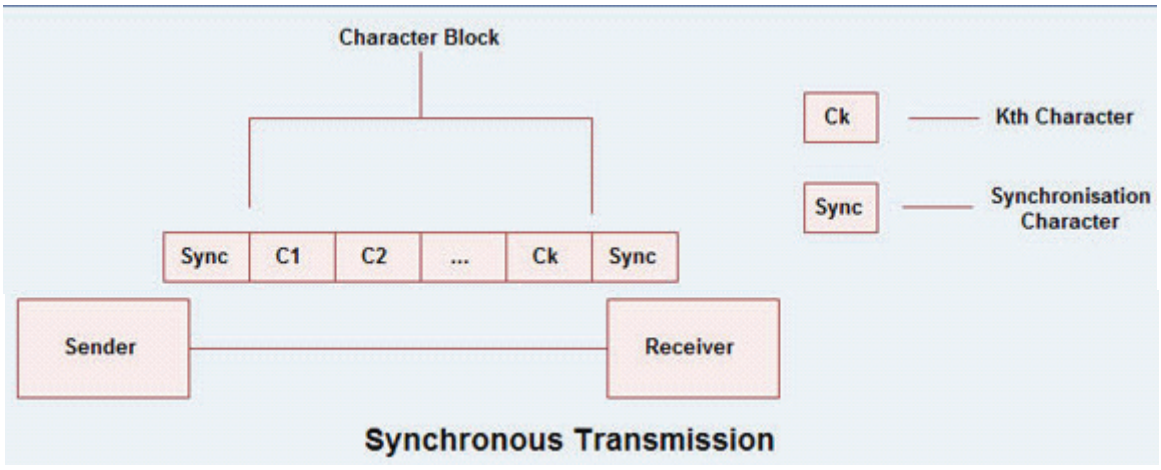
Data is transmitted between communication devices in multiples of fixed-length units, typically 8-bits. For example, if the computer is transferring a source program, the data will be made up of a block of 8-bit binary-encoded characters. On the other hand, if the data is in the form of a compiled object code of the program, the data will be made up of a block of 8-bit bytes. At the receiving end, the following parameters are determined to decode and interpret the message correctly. (Fig 15)

1 The start of each bit period.

2 The start and end of each character or byte.

3 The start and stop of each complete message block.

Fig 15



These three parameters are known as bit synchronization, character, or byte synchronization, respectively.

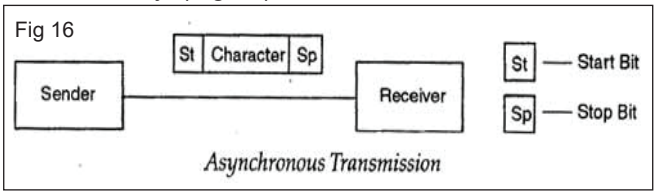
In general, there are two transmission modes; they are synchronous and asynchronous modes. In a synchronous mode, the transmitter and the receiver use the same clock. But in an asynchronous mode, two independent clocks are used on either side.

Synchronous mode Asynchronous transmission is used only when the rate at which characters generated is

unknown or the transmission data rate is too low. For the transmission of a large block of data at relatively higher bit rates, synchronous transmission is used. In synchronous mode, the sending and receiving devices are synchronized with a common clock signal. This eliminates the need for the start and stop bits. The complete block of data is transmitted with fixed time interval between the bits. Before the start of transmission, clocks at both ends are to be synchronized. This is achieved by sending special character bytes called sync bytes or sync characters between the sender and the receiver. The sender informs the receiver about the start of a block. The receiver figures out the start of each character by knowing the coding scheme used. If the sender is idle or does not transmit any character, the receiver searches for the next group of sync characters. The devices are then resynchronized to receive the next block of characters. The block length varies from few bytes to many hundreds of bytes. The most commonly used protocol is the BISYNC or Bit Synchronous Protocol.

Asynchronous mode is also known as start-stop mode. This mode is used when data to be transmitted is generated at random intervals. For example, when a user communicates with a computer using a keyboard, the time interval between two successive keystrokes is random. This means that the signal on the transmission line will be in idle state for a long time interval between characters. With this type of communication, the receiver must be able to resynchronize at the start of each new character received. To accomplish this, each transmitted character or byte is encapsulated between an additional start bit and one or more stop bits. This mode is mainly used for the transmission of characters between a keyboard and a computer. Asynchronous transmission can also be used for the transmission of a block of characters or bytes between two computers. The time interval between successive characters is a variable entity. (Fig 16)

Fig 16



Concept of System Resources

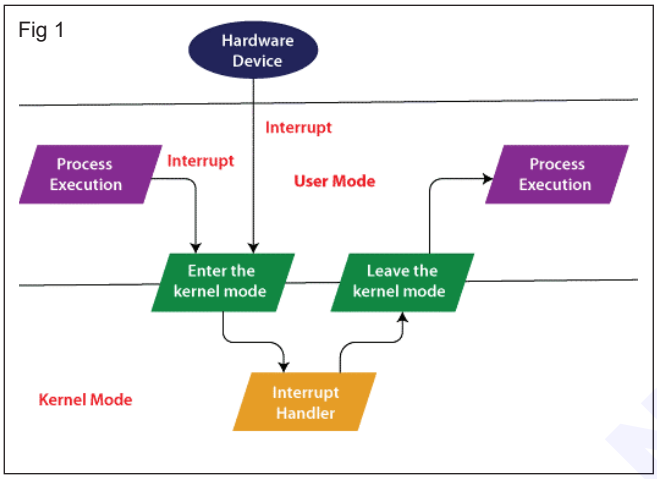
Objective: At the end of this lesson you shall be able to
- **define IRQ DMA, memory address, resource conflict and plug & play concept.**

Interrupt request

An interrupt request (IRQ) is a signal sent to a computer's processor to momentarily stop (interrupt) its operations. The signal is usually sent by a hardware device to interrupt the processor so the device gets some time to run its own operation.

Block diagram of IRQ (Fig 1)

Fig 1



Advantages and disadvantages of interrupts

The advantages of interrupts in computers are that they provide device independence, can be used to break up large tasks into smaller tasks, provide concurrency, and provide a way to respond to external events. The disadvantages of interrupts are that they consume processor time and cause a context switch.

DMA

DMA stand for in computer

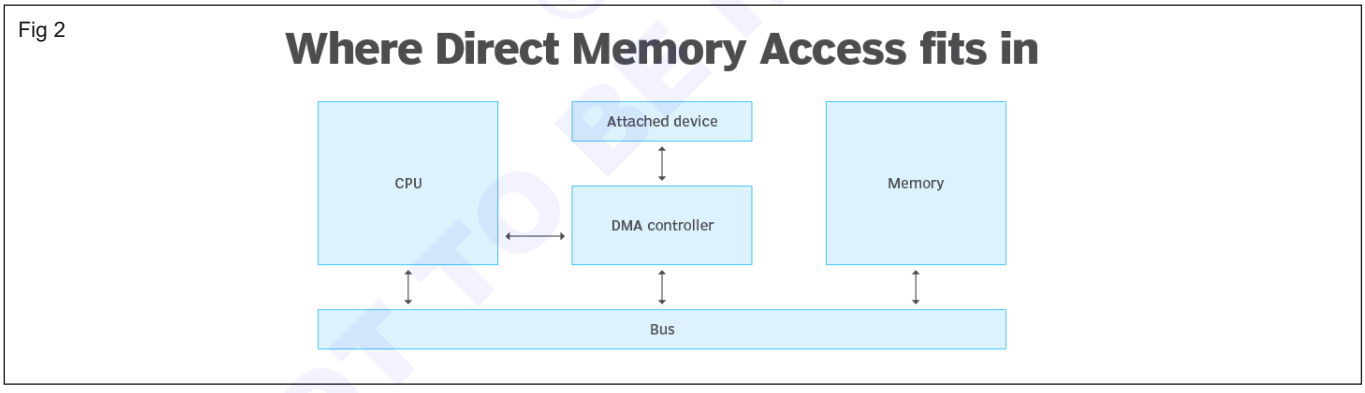
Direct memory access

Direct memory access (DMA) is a feature of computer systems that allows some hardware devices (either internal or external) to communicate directly with another computer system's RAM memory and transfer data from it without processing it using the CPU. (Fig 2)

Working principle of DMA

Direct Memory Access (DMA) is a capability provided by some computer bus architectures that enables data to be sent directly from an attached device, such as a disk drive, to the main memory on the computer's motherboard.

Fig 2



Types of DMA

Devices perform one of the following three types of DMA: Bus-Master DMA. Third-party DMA. First-party DMA.

Example of a DMA

Typical examples are disk controllers, Ethernet controllers, USB controllers, and video controllers

Usually the DMA controller built into these devices can only move data between the device itself and main memory – that is, it's not intended to be used as a general system DMA controller.

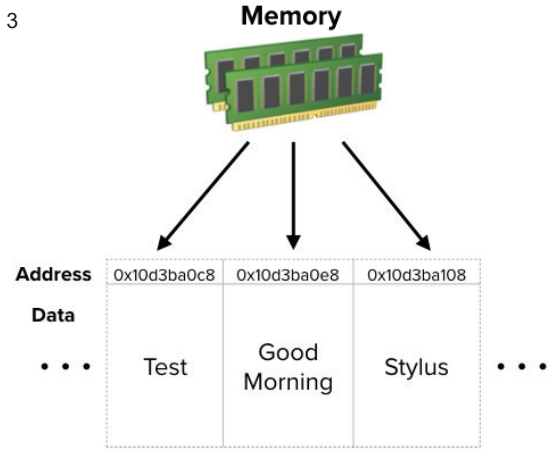
The advantages and disadvantages of DMA

Allows a peripheral device to read from/write to memory without going through the CPU

Improved System Performance: DMA can lead to improved overall system performance by offloading data transfer tasks from the CPU. Disadvantages: Security Risks: DMA can be exploited for unauthorized access to system memory, potentially leading to security vulnerabilities.

Memory address (Fig 3)

Fig 3



The memory address is the location of where the variable is stored on the computer. When we assign a value to the variable, it is stored in this memory address.

A memory address is a unique identifier used by a device or CPU for data tracking. This binary address is defined by an ordered and finite sequence allowing the CPU to track the location of each memory. (Fig 3)

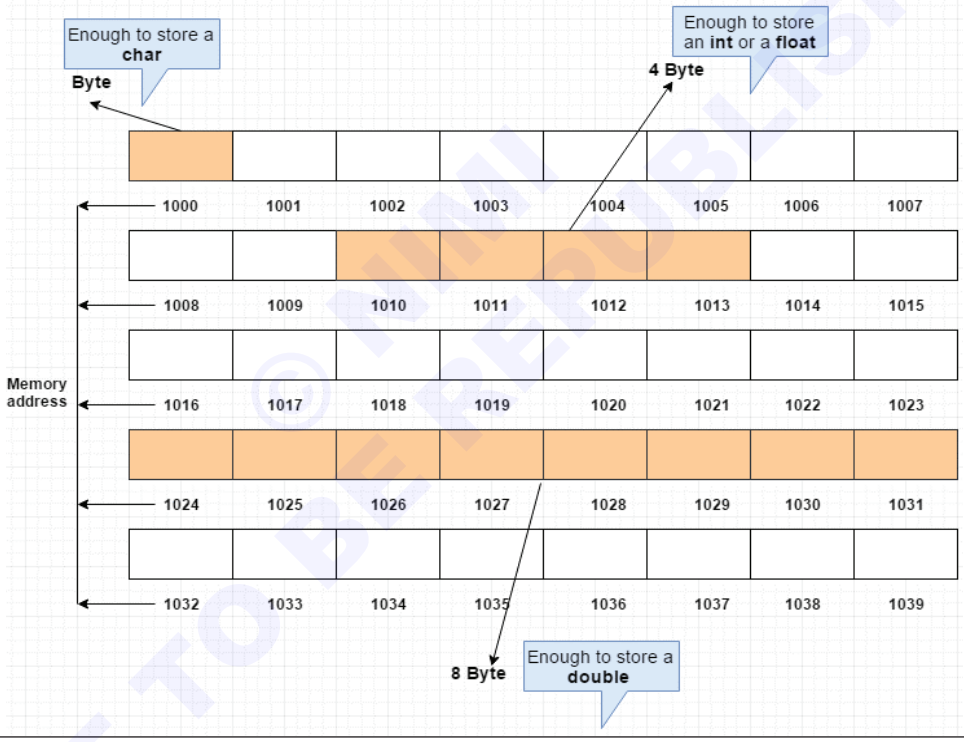
Memory address example

That location has a fixed address in the memory space, like this: While you think of the variable f, the computer thinks of a specific address in memory (for example, 248,440).

Types of address

There are two types of addresses used for memory in the operating system, i.e., the physical address and logical address. The logical address is a virtual address viewed by the user. The user can't view the physical address directly. (Fig 4)

Fig 4



Types of Addressing modes

- Register Addressing Mode.
- Direct Addressing Mode.
- Immediate Addressing Mode.
- Register Indirect Addressing Mode.
- Index Addressing Mode.
- Auto Increment Mode.
- Auto Decrement Mode.
- Relative Addressing Mode.

I/O address

I/O address, also called a "port address," references a separate memory space on PC peripheral boards, similar to memory-mapped peripherals that use blocks of memory. Peripherals often use both methods: an I/O address for passing control signals and memory for transferring data.

Types of Addresses

There are two types of addresses used for memory in the operating system, i.e., the physical address and logical address. The logical address is a virtual address viewed by the user. The user can't view the physical address directly.

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

The Logical Address is Virtual and the Physical Address is the actual address of the memory. The Logical Address is generated by the CPU and the Physical Address is calculated by MMU. Users can't view the Logical Address of a program whereas the Physical Address is visible to the user.

Types of logical addresses

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses. A source address is always a unicast address—the frame comes from only one station.

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Physical address examples

A MAC address typically follows a format like this: XX:XX:XX:YY:YY:YY. The first half (XX:XX:XX) represents the manufacturer identifier, while the second half (YY:YY:YY) is the device's unique identifier assigned by the manufacturer.

Logical address example

logical address 02FE would be translated into the physical address 01A0FE.

The concept of plug and play

Plug and Play (PnP) is the part of Windows that enables a computer system to adapt to hardware changes with minimal intervention by the user. A user can add and remove devices without having to do manual configuration, and without knowledge of computer hardware.

Resource conflict in computer

A hardware resource conflict generally occurs when a hardware device in the computer shares the same I/O port as another device. With computers running Microsoft Windows, hardware conflicts can be identified from the Device Manager.

System resource conflicts occur when two or more devices or programs try to use the same hardware or software resource, such as an interrupt request (IRQ), a memory address, or a port. These conflicts can cause errors, performance issues, or system crashes.

A problem that occurs when two programs cannot run in the same computer at the same time. It is generally due to a programming bug and typically manifests when two programs compete for the same resource (memory, peripheral device, register, etc.).

Plug and Play (PnP) Concept

Plug and Play (PnP) is the part of Windows that enables a computer system to adapt to hardware changes with minimal intervention by the user. A user can add and remove devices without having to do manual configuration, and without knowledge of computer hardware. (Fig 5)

Fig 5

Plug-and-play is used to describe computer equipment, for example, a printer, that is ready to use immediately when you connect it to a computer. [computing] ...a plug-and-play USB camera.

The difference between plug and play

For example, if you connect a Plug-and-Play mouse to the USB port on your computer, it will begin to work within a few seconds of being plugged in. A non plug-and-play device would require you to go through several steps of installing drivers and setting up the device before it would work.

The benefits of plug and play

Plug and play enhances efficiency and reduces the time lag in users' tasks. Plug and play reduces the required skill level to install and use the application. Staff at all skill levels are able to access and work on the applications because tasks are segregated on skill assessment levels.

Add on Cards

Objective: At the end of this lesson you shall be able to

- **explain add on cards (AGP, PCI, TV tuner card, DVR Card, video capture, SCSI, USB, NIC, firewire, network storage).**

AGP (Accelerated Graphics Port): Accelerated Graphics Port (AGP) is an advanced port designed for Video cards and 3D accelerators. Designed by Intel and introduced in August of 1997, AGP introduces a dedicated point-to-point channel that allows the graphics controller direct access to the system memory. Below is an illustration of what the AGP slot may look like on motherboard in Fig 1.

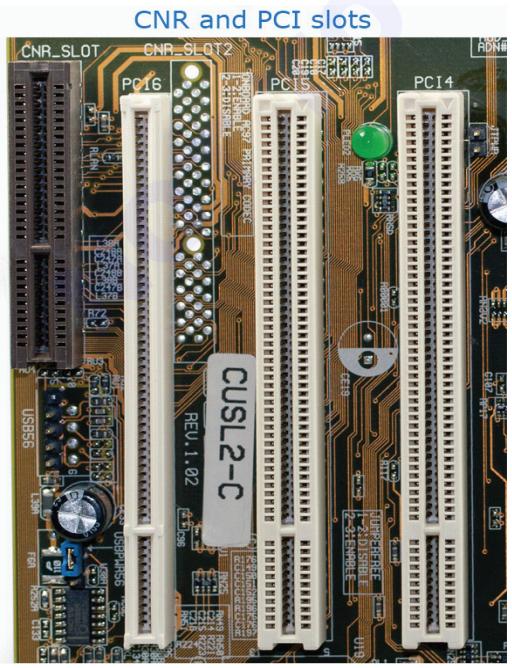
Fig 1

The AGP channel is 32-bits wide and runs at 66 MHz, which is a total bandwidth of 266 MBps and much greater than the PCI bandwidth of up to 133 MBps. AGP also supports two optional faster modes, with a throughput of 533 MBps and 1.07 GBps. It also allows 3-D textures to be stored in main memory rather than video memory.

AGP is available in three different versions, the original AGP version mentioned above, AGP 2.0 that was introduced in May of 1998, and AGP 3.0 (AGP 8x) that was introduced in November of 2000. AGP 2.0 added 4x signaling and was capable of operating at 1.5V and AGP 3.0 was capable of double the transfer speeds.

PCI (Peripheral Component Interconnect) (Fig 2)

Fig 2



Peripheral Component Interconnect, PCI was introduced by Intel in1992. The PCI bus came in both 32-bit (133MBps) and 64-bit versions and was used to attach hardware to a computer. Although commonly used in computers from the late 1990s to the early 2000s, PCI has since been replaced with PCI Express.

Revisions came in 1993 to version 2.0, and in 1995 to PCI 2.1 as an expansion to the ISA bus. Unlike ISA and other earlier expansion cards, PCI follows the PnP specification and therefore did not require any jumpers or dip switches. The picture below shows an example of what PCI slots look like on a motherboard. As you can see, there are three PCI slots: PCI4, PCI5, and PCI in the figure.

Examples of PCI devices

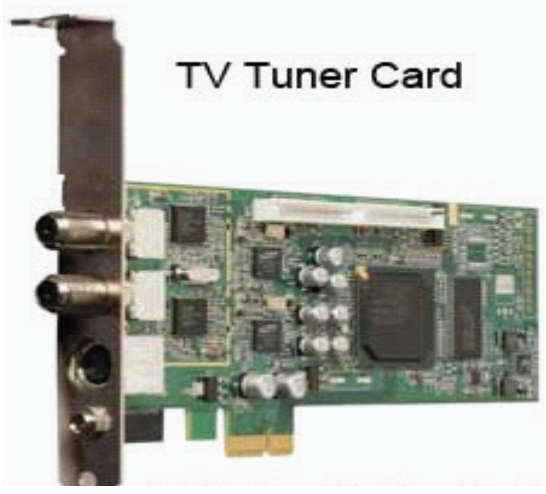
- Modem
- Network card
- Sound card
- Video card

PCI device drivers

If looking for PCI drivers, most likely need to download them for a specific PCI device. For example, if need a PCI Ethernet adapter driver, should install the drivers for the network card. See our drivers section for a listing of drivers for various devices.

TV tuner card (Fig 3)

Fig 3



A computer is capable of showing TV stations on a monitor by using a TV tuner card. The TV tuner card

allows the user to connect a coaxial cable to the computer. The computer could then display basic cable stations and even digital cable stations on the monitor. A TV tuner card can even provide a method for recording TV shows on the computer for later viewing, similar to how a Digital Video Recorder (DVR) device works.

One of the more popular and well known brands of TV tuner cards is Hauppauge. Their line of WinTV tuner cards work with many computers and operating systems,

including Windows XP, Vista, and 7. Internal TV tuner cards for desktop computers plug into either a PCI or PCI Express slot, and external TV tuners are also available for use with laptop and desktop computers. Some of these TV tuners also include a remote control for easy access and programming.

DVR (Digital Video Recorder) (Fig 4)

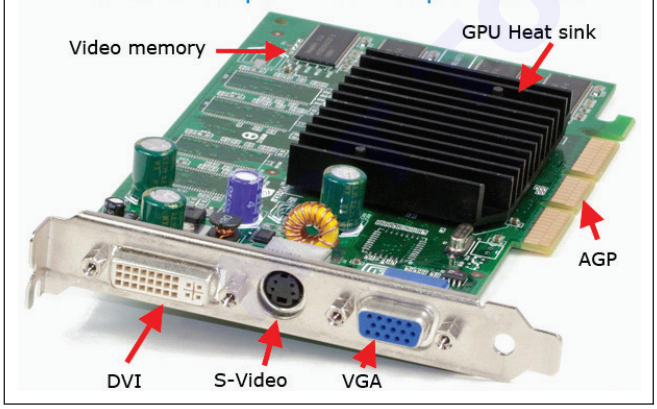
Fig 4

Alternatively referred to as a Personal Video Recorder (PVR) and short for Digital Video Recorder. DVR is a home electronic device similar to the VCR that enables users to record their favorite shows to a computer hard drive. What makes DVRs increasingly popular is their ease of use and the ability for a user to record their favorite shows and watch them anytime.

Video card

Alternatively known as a display adapter, graphics card, video adapter, video board, or video controller, a video card is an IC or internal board that creates a picture on a display. (Fig 5)

Fig 5 Internal computer video expansion card



The picture above is an example of a video card with three connections, or video ports, on the back.

- VGA connector
- S-Video connector
- DVI connector

In the past, VGA or SVGA was the most popular connection used with computer monitors. Today, most flat panel displays use the DVI connector.

When connected inside the computer the above video card uses the AGP expansion slot on the computer motherboard.

Video card expansion slots

Over the development of computers, there have been several types of expansion slots used for video cards. Today, the most common expansion slot for video cards is PCIe, which replaced AGP, which replaced PCI, which replaced ISA.

SCSI card

Short for Small Computer System Interface, SCSI is pronounced as "Scuzzy" and is one of the most commonly used interface for disk drives that was first completed in 1982. Unlike competing standards, SCSI is capable of supporting eight devices, or sixteen devices with wide SCSI. However, with the SCSI host adapter located on ID number 07 and boots from the ID 00. This leaves the availability of six device connections. In the picture below, is an example of a SCSI adapter expansion card with an internal and external connection. Once installed in the computer this adapter would allow multiple SCSI devices to be installed in the computer. More advanced motherboard may also have available SCSI connections on the motherboard. (Fig 6)

Fig 6 SCSI adapter card

USB

Short for Universal Serial Bus, USB (pronounced yoo-es-bee) is a standard that was introduced in1995 by Intel, Compaq, Microsoft and other computer companies. USB 1.x is an external bus standard that supports data transfer rates of 12 Mbps and is capable of supporting up to 127peripheral devices. The picture shows an example of a USB cable being connected into the USB port.

USB transfer speeds

USB 2.0, also known as hi-speed USB, was developed by Compaq, Hewlett Packard, Intel, Lucent, Microsoft, NEC and Philips and was introduced in 2001. Hi-speed USB is capable of supporting a transfer rate of up to 480 Mbps and is backwards compatible, meaning it is capable of supporting USB 1.0 and 1.1 devices and cables.

USB 3.0 devices were first made available in November 2009 by Buffalo Technology, but the first certified devices weren't available until January 2010. The first certified devices included motherboards from ASUS and Gigabyte Technology. Dell began including USB 3.0 ports in their Inspiron and Dell XPS series of computers in April 2011. Today, many devices use the USB 3.0 revision for improved performance and speed, including USB thumb drives, digital cameras, external hard drives, MP3 players, and other devices.

As of 2012, USB 3.0 also known as Super Speed USB is the latest version of the USB protocol. Most new computers feature USB 3.0 ports built-in, offering data transfer speeds of up to five gigabits per second. USB 3.0 improved upon the USB 2.0 technology with speed and performance increases, improved power management and increased bandwidth capability (providing two unidirectional data paths for receiving and sending data at the same time).

USB connector variations

USB connectors come in many shapes and sizes as there are many different devices that utilize them. Every version of USB connector including standard, Mini, and Micro have two or more variations of connectors.

USB cables - Length and Type

USB cables are available in multiple lengths, from around 3 feet to just over 16 feet in length. The maximum length of a USB cable is 16 feet 5 inches (5 meters) for high speed devices and 9 feet 10 inches (3 meters) for low speed devices.

These maximum lengths are due to data transfer timing and the risk of data loss if using longer cable lengths. However, by using USB hubs, can connect two USB cables together to effectively extend the distance between the two devices being connected together.

There are different types of USB cables as well. As mentioned above, there are different transfer speeds (2.0 and 3.0) for USB. Similarly, there are different types of USB cables to match with those speeds. You can get a USB 2.0 cable for use with a device using USB 2.0 or a USB 3.0 cable for use with a device using USB 3.0.

There are also USB extension cables that can connect to one end of a USB cable (typically the end that would connect to the computer) to extend the length of the cable. However, you should still avoid extending the cable

beyond the 16 feet 5 inches total maximum length limit, unless using a USB hub to connect another USB cable.

USB devices

Today, there are millions of different USB devices that can be connected to your computer. Below are just a few of the most common USB devices you'll likely find and use.

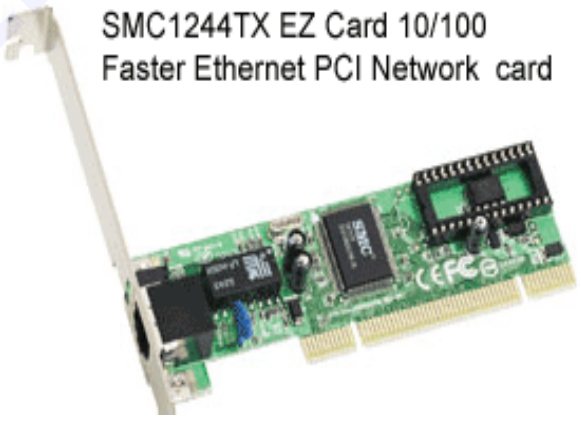
- Camera
- External drive
- iPod or other MP3 player
- Keyboard
- Keypad
- Microphone
- Mouse
- Printer
- Joystick
- Jump drive aka Thumb drive
- Scanner
- Smartphone
- Tablet
- Webcams

NIC (Network Interface Card)

Network Interface Card, the NIC is also referred to as an Ethernet card and network adapter. It is an expansion card that enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable with an RJ-45 connector.

Due to the popularity and low cost of the Ethernet standard, most new computers have a network interface build directly into the motherboard. The Fig 7 shows the SMC EZ Card 10/100 PCI network card, one of the more common examples. (Fig 7)

Fig 7



Graphics card: It is also called a video adapter or graphics card. It converts computer output into a video signal and sends it to the monitor to display. This card connects the motherboard to the computer monitor. The card contains Video RAM memory. The amount of memory located on the card must be enough to support the desired number of colors and resolutions (Fig 8)

Fig 8

Firewire interface card

Alternatively referred to as IEEE-1394, Firewire is a digital bus with a bandwidth of 400-800 Mbps. It can handle up to 63 units on the same bus, and is hot swappable. It was first developed by Apple in 1995.

Users more familiar with USB can consider Firewire similar to USB, as they has many similarities. Like USB, Firewire has dozens of different devices such as removable drives and cameras. (Fig 9)

Fig 9

Storage device

Alternatively referred to as digital storage, storage, storage media, or storage medium, a storage device is any hardware capable of holding information either temporarily or permanently.

There are two types of storage devices used with computers: Primary storage device, such as RAM, and a Secondary storage device, like a hard drive.

Secondary storage can be removable, internal, or external storage. The Fig 9 shows an example of a Drobo, an external secondary storage device.

Without a storage device, computer would not be able to save any settings or information and would be considered a dumb terminal.

Cables (Fig 10)

Fig 10

Alternatively referred to as a cord, connector or plug, a cable is one or more wires covered in a plastic covering that connects a computer to a power source or other device.

There are two main types of computer cables, a data cable and a power cable. A data cable is a cable that provides communication between devices. For example, the data cable that connects monitor to computer and allows computer to display a picture on the monitor.

Other examples of data cables include the CAT5, IDE/EIDE, SATA, and USB cables. A power cable is any cable that powers the device.

For example, the power cord that connects to computer and a Molex style cable inside the computer are both good examples of power cables. Below, is a listing of the most common types of cables found with computers and electronics and examples of devices that use them.

Connectors

A connection is a term that describes the link between a plug or connector into a port or jack. For example, your monitor, mouse, and keyboard all make a connection to the computer before they will be able to work.

Connecting - Describing the process of connecting a plug, wire, or other device to the computer. For example, connecting computer to the Internet.

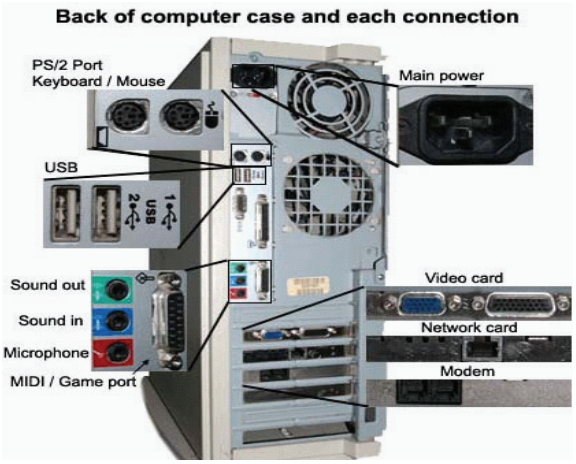
Connections - An overall description of all available ports and jacks (more than one) on a computer.

Connector - The description of the end of the cable that connects to the computer. Centronics, DB, and DIN are good examples of types of connectors.

Connect, connected, and connecting - This term can also be used in software, for example, when a user gets onto the Internet they are connecting to another computer to establish a connection.

Below is a picture (Fig 11) of the back of a desktop computer and each of connections or ports. Although desktop computer's layout may be different, this diagram dives a better understanding of where everything connects.

Fig 11



Types of cables and connectors

1 CAT5 - Used with network cards.

2 Composite (RCA) - Used with TV, projectors, and consoles.

3 DVI - Used with Monitors, Projectors, and other displays.

4 Firewire (IEEE-1394) - Used with digital cameras and external drives.

5 HDMI - Used with Monitors, Projectors, DVD/Blu-ray players, and other displays.

6 Molex - Power cable used inside your computer.

7 IDE/EIDE - Used with hard drives and disc drives.

8 PS/2 - Used with keyboards and mice.

9 SATA - Used with hard drives and disc drives.

10 Parallel - Used with printers.

11 USB - Used with keyboard, mouse, printer, MP3 players, and thousands of other devices.

12 VGA/SVGA - Used with monitors and projectors.

POST Error Messages

Objective: At the end of this lesson you shall be able to
- **identify the different types of POST error messages.**

POST in computer

When you press your computer's power button, multiple actions take place in the background, even before you see anything on your screen. These actions are collectively called the power-on self-test (POST).

Essentially, each time the user turns on their PC, the UEFI/ BIOS gathers information about the major system components and performs a special test called the Power On Self Test to make sure that each component is functioning properly.

While the entire process is more complicated than that and involves intricacies related to memory and system partitioning, the thing you need to keep in mind is that it's a kind of a diagnostic test. So if any particular part of the test fails, the BIOS figures out where the failure took place and displays an error message on the monitor, or if it occurs before the video signal, then on the POST code display.

A power-on self-test (POST) is a process performed by firmware or software routines immediately after a computer or other digital electronic device is powered on.

(Power On Self Test code) A proprietary number generated by each PC BIOS vendor indicating the current diagnostic test being taken at startup. The results are displayed on a small readout on a POST card that is plugged into the peripheral bus.

The principal duties of the main BIOS during POST are as follows:

- Verify CPU registers.
- Verify the integrity of the BIOS code itself.
- Verify some basic components like DMA, timer, interrupt controller.
- Initialize, size, and verify system main memory.
- Initialize BIOS.
- Pass control to other specialized extension BIOS's (if installed).
- Identify, organize, and select which devices are available for booting.

POST ERROR

POST stands for "Power-On Self-Test." It's a series of tests that your PC performs as soon as you switch it on. If POST finds an error, the PC switches off again immediately. A POST can fail for several reasons. With a self-assembled PC, it is often due to an error during assembly.

Port Problem Symptoms

Typical symptoms associated with serial, parallel, or game port failures include the following: A 199, 432, or 90x IBM-compatible error code displays on the monitor (printer port). The printer's Online light is on but no characters are printed when print jobs are sent to the printer.

POST indicate the error

If the specified hardware isn't detected or operating properly, the firmware usually stops the boot process and issues an error message. The message might be displayed on the computer's screen, sent as a series of coded beeps or both, depending on the nature of the problem.

Post error message code as an indication of a printer's problem

If your printer's status displays "Printer in error state," there may be a problem with the printer itself. Make sure the printer is turned on and connected to your PC by Wi-Fi or cable. Check it for low paper or ink, and be sure the cover isn't open and the paper isn't jammed.

After determining the cause of the POST failure, refer to the fixes listed below to resolve the problem.

1 Double Check if All the Components Are Compatible.

2 Disconnect Newly Installed Hardware. ...

3 Remove USB Drives, Discs, and Input Devices. ...

4 Swap RAM Slots or Reinstall the RAM. ...

5 Reconnect the Power Cables and Check the PSU.

Common Printer Problems and Fixes

- Paper Jams. Paper jams are a common problem for printers, resulting in time-consuming and frustrating delays. ...
- The Printer Is Offline. ...
- Loaded Queue. ...
- The Ink Cartridges Are Empty Or Low. ...
- Slow Wi-Fi Printing. ...
- Misaligned – Weird-Looking Text. ...
- Streaky, Wet, Plain Ugly Prints. ...
- Virtual Printer.

Indicate post error on windows startup problem

A Power On Self-Test (POST) issue can be caused due to a corrupt BIOS, bad connection between hardware components or faulty hardware. Some symptoms that indicate a Power On Self-Test (POST) failure are: The computer is stuck at the Dell logo. The computer beeps or the LEDs are blinking in repetitive patterns.

Indicate post error of an illegal operational problem in computer

Operating system error

A system failure may occur due to a hardware failure or a significant software problem, leading the system to freeze, reboot, or stop working completely. An error may or may not be displayed on the screen because of a system failure. The computer may shut down without warning or error message.

Error in computer and types of error

Errors can occur at various stages of the programming process. There are different types of errors in programming including syntax errors, run-time errors, linker errors, logical errors, and semantic errors. Syntax errors are the most common type of error, while run-time errors are often the most challenging to detect.

The indicators of computer system failure

several signs indicating a system failure, such as slow response times, error messages or warnings, crashes, freezes, data corruption, unusual system behavior, or the inability to access certain functions or services.

Indicate post error of an virus protection utility problem in computer

Symptoms of Malware

- Your computer or web browser has dramatically slowed down over a period of a few days/a week.
- Frequent freezing or crashing.
- Modified or deleted files.
- New programs or desktop icons that you do not recall installing/creating.
- Programs running without your consent.
- Programs closing without your consent.

An indication of a networks problem

Slow network speeds, weak Wi-Fi signals and damaged cabling are just some of the most common network connection issues that IT departments need to troubleshoot. Business networks are complex, and many things can go wrong that disrupt network performance.

The symptoms of network problems

Laggy video calls, bad call quality, slow application or network speed, buffering downloads, choppy VoIP Quality, and no Internet connection are examples of network problem symptoms.

Post error message code as an indication of an external devices problem

External hard drives are particularly prone to failure due to frequent improper use, outdated drivers, bundling with incompatible software on different operating systems, frequent connection and disconnection to different devices, and, in the case of portable or USB hard drives, unsafe ejection.

Modem Symptoms

Typical symptoms associated with modem failures include the following:

- There is no response from the modem.
- The modem does not dial out.
- The modem does not connect after a number has been dialed.
- The modem does not transmit after making connection with a remote unit.
- The modem does not install properly for operation.
- Garbled messages are transmitted.
- The modem cannot terminate a communication session.
- The modem cannot transfer files.

COM Port Conflicts

Every COM port on a PC requires an IRQ line to signal the processor for attention. In most PC systems, two COM ports share the same IRQ line. The IRQ4 line works for COM1 and COM3, and the IRQ3 line works for COM2 and COM4. This is common in PC compatibles. The technician must ensure that two devices are not set up to use the same IRQ channel.

If more than one device is connected to the same IRQ line, a conflict occurs because it is not likely that the interrupt handler software can service both devices. Therefore, the first step to take when installing a modem is to check the system to determine how its interrupts and COM ports are allocated.

To install a non-PnP device on a specific COM port (for example, COM2), you must first disable that port in the system's CMOS settings to avoid a device conflict. If not, the system might try to allocate that resource to some other device because it has no way of knowing that the non-PnP device requires it.

Windows Modem Checks

In Windows 9x, you can find the modem configuration information by navigating to Control Panel, Modems. The Modems Properties dialog box has two tabs—the General tab and the Diagnostics tab. The Diagnostics tab, provides access to the modem's driver and additional information.

The Windows 9x Diagnostics Tab of the Modems Properties dialog box

In Windows XP, the Diagnostics tab for the modem is available by clicking the Properties button on the Modems tab of the Phone and Modem Options dialog box. The Query Modem button on this tab can be used to perform low-level tests on the modem.

The Hayes AT Command Set

The Hayes command set is based on a group of instructions that begin with a pair of attention characters, followed by command words. Because the attention characters are an integral part of every Hayes command, the command set is often referred to as the AT command set.

AT commands are entered at the command line using an ATXn format. The Xn nomenclature identifies the type of command being given (X) and the particular function to be used (n).

Except for the ATA, ATDn, and ATZn commands, the AT sequence can be followed by any number of commands. The ATA command forces the modem to immediately pick up the phone line (even if it does not ring). The Dn commands are dialing instructions, and the Zn commands reset the modem by loading new default initialization information into it. After a command has been entered at the command line, the modem attempts to execute the command and then returns a result code to the screen. Table 1 describes the command result codes.

Table 1

Command Result Codes

RESULT	CODE	DESCRIPTION
0	OK	The OK code is returned by the modem to acknowledge execution of a command line.
1	CONNECT	The modem sends this result code when line speed is 300 bps.
2	RING	The modem sends this result code when incoming ringing is detected on the line.
3	NO CARRIER	The carrier is not detected within the time limit, or the carrier is lost.
4	ERROR	The modem could not process the command line (entry error).
5	CONNECT 1200	The modem detected a carrier at 1200 bps.
6	NO DIAL TONE	The modem could not detect a dial tone when dialing.
7	BUSY	The modem detected a busy signal.
8	NO ANSWER	The modem never detected silence (@ command only).
9	CONNECT 0600	The modem sends this result code when line speed is 7200 bps.
10	CONNECT 2400	The modem detected a carrier at 2400 bps.
11	CONNECT 4800	Connection is established at 4800 bps.
12	CONNECT 9600	Connection is established at 9600 bps.
13	CONNECT 7200	The modem sends this result code when the line speed is 7200 bps.
14	CONNECT 12000	Connection is established at 12000 bps.
15	CONNECT 14400	Connection is established at 14400 bps.
17	CONNECT 38400	Connection is established at 38400 bps.
18	CONNECT 57600	Connection is established at 57600 bps.
22	CONNECT 75TX/1200RX	The modem sends this result code when establishing a V.23 Originate.
23	CONNECT 1200TX/75RX	The modem sends this result code when establishing a V.23 answer.
24	DELAYED	The modem returns this result code when a call fails to connect and is considered delayed.
32	BLACKLISTED	The modem returns this result code when a call fails to connect and is considered blacklisted.
40	CARRIER 300	The carrier is detected at 300 bps.
44	CARRIER 1200/75	The modem sends this result code when V.23 backward channel carrier is detected.
45	CARRIER 75/1200	The modem sends this result code when V.23 forward channel carrier is detected.
46	CARRIER 1200	The carrier is detected at 1200 bps.
47	CARRIER 2400	The carrier is detected at 2400 bps.
48	CARRIER 4800	The modem sends this result code when either the high or low channel carrier in V.22bis modem has been detected.
49	CARRIER 7200	The carrier is detected at 7200 bps.
50	CARRIER 9600	The carrier is detected at 9600 bps.
51	CARRIER 12000	The carrier is detected at 12000 bps.
52	CARRIER 14400	The carrier is detected at 14400 bps.
66	COMPRESSION: CLASS 5	MNP Class 5 is active CLASS 5.
67	COMPRESSION: V.42bis	COMPRESSION: V.42bis is active V.42bis.
69	COMPRESSION: NONE	No data compression signals NONE.
70	PROTOCOL: NONE	No error correction is enabled.
77	PROTOCOL: LAPM	V.42 LAP-M error correction is enabled.
80	PROTOCOL: ALT	MNP Class 4 error correction is enabled.

Using the AT Command Set

At the command line, type ATZ to reset the modem and enter command mode using the Hayes-compatible command set. You should receive a 0, or OK response, if the command was processed. A returned OK code indicates that the modem and the computer are communicating properly.

You can use other AT-compatible commands to check the modem at the command-prompt level. The ATL2 command sets the modem's output volume to medium, to ensure it is not set too low to be heard. If the modem dials, but cannot connect to a remote station, check the modem's Speed and DTR settings. Change the DTR setting by entering AT&Dn.

- n = 0—The modem ignores the DTR line.
- n = 1—The modem goes to async command state when the DTR line goes off.
- n = 2—A DTR off condition switches the modem to the off-hook state and back into command mode.
- n = 3—When the DTR line switches to off, the modem is initialized.

If the modem connects, but cannot communicate, check the character-framing parameter of the receiving modem, and set the local modem to match. Also, match the terminal emulation of the local unit to that of the remote unit. American National Standards Institute (ANSI) terminal emulation is the most common. Finally, match the file transfer protocol to the other modem.

AMI BIOS beep codes

Below are the AMI BIOS Beep codes that can occur. However, because of the wide variety of different computer manufacturers with this BIOS, the beep codes may vary.

Beep code	Descriptions
1 short	DRAM refresh failure.
2 short	Parity circuit failure.
3 short	Base 64K RAM failure.
4 short	System timer failure
5 short	Process failure.
6 short	Keyboard controller gate A20 error.
7 short	Virtual mode exception error.
8 short	Display memory Read/Write test failure.
9 short	ROM BIOS checksum failure.
10 short	CMOS shutdown Read/Write error.
11 short	Cache memory error.
1 long, 3 short	Conventional/Extended memory failure.
1 long, 8 short	Display/Retrace test failed.
two-tone siren	Low CPU Fan speed, Voltage Level issue.

AWARD BIOS beep codes

Below are Award BIOS Beep codes that can occur. However, because of the wide variety of different computer manufacturers with this BIOS, the beep codes may vary.

Beep code	Descriptions
1 long, 2 short	Indicates a video error has occurred and the BIOS cannot initialize the video screen to display any additional information.
1 long, 3 short	Video card not detected (reseat video card) or bad video card.
Beeps repeating endlessly.	RAM problem.
Repeated high frequency beeps while PC is running.	Overheating processor (CPU)
Repeated beeps alternating high & low frequency.	Issue with the processor (CPU), possibly damaged.

If any other correctable hardware issues are found, the BIOS displays a message.

Dell beep codes

Beep code	Descriptions
1 beep	BIOS ROM corruption or failure
2 beeps	Memory (RAM) not detected
3 beeps	Motherboard failure
4 beeps	Memory (RAM) failure
5 beeps	CMOS Battery failure
6 beeps	Video card failure
7 beeps	Bad processor (CPU)

IBM BIOS beep codes

Below are general IBM BIOS Beep codes that can occur. However, because of the wide variety of models shipping with this BIOS, the beep codes may vary.

Beep code	Descriptions
No Beeps	No Power, Loose Card, or Short.
1 Short Beep	Normal POST, computer is ok.
2 Short Beep	POST error, review screen for error code.
Continuous Beep	No Power, Loose Card, or Short.
Repeating Short Beep	No Power, Loose Card, or Short.
1 Long and 1 Short Beep	Motherboard issue.
1 Long and 2 Short Beeps	Video (Mono/CGA Display Circuitry) issue.
1 Long and 3 Short Beeps.	Video (EGA) Display Circuitry.
3 Long Beeps	Keyboard or Keyboard card error.
1 Beep, Blank or Incorrect Display	Video Display Circuitry.

Limitations & Upgrading of PC

Objectives: At the end of this lesson you shall be able to
- **understand the limitation of a pc and scope for grading**
- **understand technical specifications for pc grading.**

The basic limitation of computer

A computer cannot act on situations that are not fed or programmed into them. They have zero IQ(Intelligent Quotient). These outputs are completely dependent on the user's input. That is they produce the wrong output if the wrong input is provided instead of correcting

Two limitations of a computer system

A computer system possesses some characteristics, which in comparison to human beings, turn out to be its capabilities but there are some limitations of computer system which are as follows:

1 Lack of commonsense, Zero IQ,

2 Lack of decision-making etc

Components are worth upgrading

1 System memory/storage (HDD or SSD)

2 Main memory.

3 Graphics card.

4 Processor.

5 CPU cooler and fan.

Important of PC upgrading

Upgrading your computer can bring you more speed and storage space at a fraction of the cost of a new computer, but you don't want to put new components in an old system if it's not going to deliver the speed increase you want

To upgrade your processor

1 Remove the Computer's Side Panel. ...

2 Locate and Remove the CPU Cooler. ...

3 Clean the Cooler's Contact Patch. ...

4 Lift the Retention Arm of the CPU Socket. ...

5 Remove the Old Processor. ... (Fig 1)

6 Insert the New Processor. ...

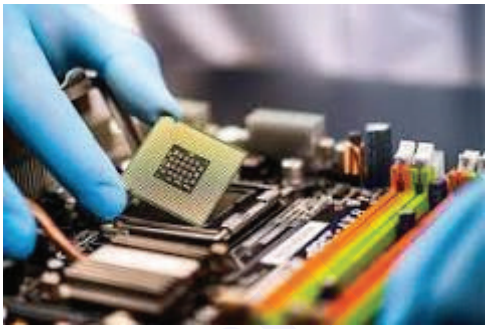
7 Apply Thermal Paste. ...

8 Reinstall the CPU Cooler.

PC parts to upgrade first

When you're deciding the best things to upgrade on your PC, we recommend RAM, SSDs, and graphics cards as the main areas to focus on. Ideally, you should always tailor your upgrades to your precise needs.

Fig 1



The concept of upgrading and maintenance of a PC

PC hardware maintenance is the process of auditing, upgrading, and maintaining a computer's physical parts to ensure the components perform optimally. IT hardware maintenance involves caring for components such as the keyboard, CD drives, hard disk, battery, and other peripherals.

Advantages of upgrading your PC

Cheaper: Replacing just one component saves a lot of money compared to buying new.

Saves time: You don't have to set up a new PC, install all the necessary programs, and move your data.

Of course, it is also more sustainable to replace only parts of the PC and not the whole computer.

Technical specifications for PC Upgrading

1 Upgrade RAM – Random Access Memory

Essentially, a computer's short term memory. A small amount of data can be stored here to be accessed quickly when the processor of your computer needs it. Unlike your internal SSD or HDD, RAM only stores data temporarily. It totally resets when your computer is rebooted.

Most laptops and desktops will allow you to add more memory and it can usually be done by anyone with just a screwdriver.

2 Upgrade Graphics Card

Upgrading graphics card is a must if you are a serious gamer, video editor or 3D animator. In fact, doing all these upgrades will give you significant speed improvements if you regularly game, edit or animate.

3 Upgrade to a Faster Hard Drive.

Upgrade your hard drive if you're running out of space or want faster performance or both!

A quick clean up of your hard drive may give you a few gigabytes of extra space but if you still need more space then an upgrade to your hard drive is the ONLY way to go.

As a rule you want to keep 10GB of free space for your machine's operating system. To use anything less may cause your machine to run very slowly or crash regularly.

A faster hard drive speeds up your whole user experience. The machine boots faster, will launch software and games faster and save files quicker.

Solid State Drives (SSD) can be much more expensive than the same sized disk drive.

4 Upgrade the CPU – Central Processing Unit.

Upgrading PC's main processor is not something most home or business users have the skill, or tools, to handle.

To install a new CPU requires a certain degree of knowledge, skill and experience.

Therefore a processor upgrade is something best left to professional technicians like our experts at The Tech-Shed and is only worth doing if you make a big leap to a much newer processor.

5 Upgrade software.

Upgrading software is usually a good way to get new features or upgrade the look and performance.

However, it might also slow your machine down or stop working altogether so you should be careful before clicking the "Update" button.

Revisions are usually bug fixes and minor improvements.

Minor updates include improvements, security updates and new features.

Major updates can be a total revision of the whole software and may require more memory or hard drive space.

Revisions and Minor updates should be installed as they roll out, especially if they include security patches or updates.

6 What Else Can we Upgrade

7 Everything! However, it will depend on what you use your computer for and your budget.

However, we would suggest you only upgrade components that meet your needs.

If you are a photographer, upgrade your graphics card.

If you are editing video, a new graphics card and an SSD may be the best choice.

If you are a gamer then more memory, faster CPU and an upgrade to your graphics card are the way to go.

New hardware can only speed up a system that is working efficiently so before you spend a lot of money on new hardware book a Tech-Shed call out and we'll scan your machine and give it a clean up so you get the most out of any hardware upgrade. We can also install more memory, graphics cards hard drives and processors. We do these upgrades all the time and can specify the very best hardware for your machine saving you time and money, especially if you get it wrong.

Scope of upgrading a PC

With computer hardware, an upgrade is a term that describes adding new hardware in a computer that improves its performance. For example, with a hardware upgrade could replace hard drive in a SSD and get a huge boost in performance or upgrade the RAM so the computer run more smoothly.

Benefits of a hardware upgrade:

1 Performance increase, which make the overall computer run faster and more smoothly.

2 Capacity increase. For example, adding a new hard drive allows the computer to store more information, and more memory increases the computers ability to run more.

3 It may be necessary to upgrade the computer to meet a program or games system requirements.

4 When referring to software, a software upgrade generally refers to any major upgrade to the software that adds significant changes to the program. For example, may be running version 1.0.1 of a program, version 2.0.0 is an upgrade, and version 1.0.2 is an update.

5 Another good example of a software upgrade is upgrading version of Windows. For example, Microsoft Windows XP were upgrade to Windows 7, it would be considered a software upgrade.

Functions of Drives

Objectives: At the end of this lesson you shall be able to
- **define drive**
- **list out the important parts of CD ROM drive, ZIP drive, DVD ROM drive and MOD drive**
- **working principle of different types of drives.**

The Main Function of the CD-ROM

A CD-ROM is a compact disc that contains read-only data. This means that the data on the disc can be read by the computer, but not written to or erased. CD-ROMs are used to distribute software, video games, and other data that does not need to be updated. CD-ROM stands for compact disc read-only memory.

The troubleshooting is done for CD and DVD drives

Resolving The Problem

To begin troubleshooting, check the following top issues. ...

Make sure the CD or DVD drive has power by pressing the eject button and observing the drive activity light. ...

Test the drive using different discs. ...

Make sure the drive is recognized and correctly placed in the System Configuration Utility.

Maintain a CD-ROM

1 Handle discs by the outer edge or the center hole.

2 Use a non-solvent-based felt-tip permanent marker to mark the label side of the disc.

3 Keep dirt or other foreign matter from the disc.

4 Store discs upright (book style) in plastic cases specified for CDs and DVDs.

5 Return discs to storage cases immediately after use.

There are some tips of maintaining the CD ROM drives, which will always work for you:

The first step is you have to clean your CD ROM drive after a specific time period this will keep your drive better to use, you can clean by cloth or some other things.

The second step for this is you have to use your CD ROM drive time to time, because if you will not use them time to time then after some time it will not work properly.

The third and last step is don't experiment with your CD ROM drive without knowledge of it, this can we harmful for your whole system because all things are connected with each other.

A CD-ROM sector contains 2, 352 bytes, divided into 98 24-byte frames. Unlike a music CD, a CD-ROM cannot rely on error concealment by interpolation, and therefore requires a higher reliability of the retrieved data. In order to achieve improved error correction and detection, a CD-ROM has a third layer of Reed–Solomon error correction. [4] A Mode-1 CD-ROM, which has the full three layers of error correction data, contains a net 2, 048 bytes of the available 2, 352 per sector. In a Mode-2 CD-ROM, which is mostly used for video files, there are 2, 336 user-available bytes per sector. The net byte rate of a Mode-1 CD-ROM, based on comparison to CDDA audio standards, is 44100 Hz × 16 bits/sample × 2 channels × 2, 048 / 2, 352 /8= 153.6 kB/s= 150 KiB/s. The playing time is 74 minutes, or 4, 440 seconds, so that the net capacity of a Mode-1 CD-ROM is 682 MB or, equivalently, 650 MiB.

A 1× speed CD drive reads 75 consecutive sectors per second.CD sector contents

A standard 74 min. CD contains 333, 000 blocks or sectors .Each sector is 2, 352 bytes, and contains 2, 048 bytes of PC(mode 1) data, 2, 336 bytes of PSX/VCD (mode 2) data, or 2, 352 bytes of audio .The difference between sector size and data content are the header information and the error-correcting codes, that are big for data(high precision required), small for VCD(standard for video) and none for audio. Note that all of these, including audio, still benefit from a lower layer of error correction at a sub-sector level.If extracting the disc in raw format(standard for creating images) always extract 2, 352 bytes per sector, not 2, 048/2, 336/2, 352 bytes depending on data type(basically, extracting the whole sector).

This fact has two main consequences: Recording data CDs at very high speed(40×) can be done without losing information. However, as audio CDs do not contain a third layer of error-correcting codes, recording these at high speed may result in more unrecoverable errors or 'clicks' in the audio. On a 74 minute CD, one can fit larger images using raw mode, up to 333, 000 × 2, 352= 783, 216, 000 bytes(~747 MiB). This is the upper limit for raw images created on a 74 min or~650 MiB Red Book CD. The 14.8% increase is due to the discarding of error correction data. The sync pattern for Mode 1 CD [3] An image size is always a multiple of 2, 352 bytes(the size of a block) when extracting in raw mode.

Zip Drive

A Zip drive and Zip disk is a hardware data storage device developed by Iomega that functions like a standard 1.44" floppy drive and diskette. What makes the Iomega Zip drive unique is its capability to hold up to 100 MB, 250 MB, or 750 MB of data on the later models. Iomega Zip drives became popular in late 1990s but quickly

became less popular as users needed larger storage capabilities. The drive was eventually replaced by CD-R (compact disc recordable) and CD-RW (compact disc re-writable) drives and discs as they became cheaper since they offered more storage and compatibility. (Fig 1)

In the picture is an Iomega Zip disk that is bigger than a floppy diskette and made of a much harder plastic. Much like a floppy diskette, the Zip disk contains a magnetic circular disk that holds information. To read and write information on a Zip diskette, it is placed into a Zip drive that moves the metal cover exposing the magnetic disk.

Fig 1

Explanation of Zip Drive

The Zip drive was available in 100- and 250-MB capacities. The initial versions of the drive could be connected to a computer by means of a parallel, SCSI or IDE port. The later versions had a USB interface and were thus simple to connect, being plug and play. The Zip drive was PC and Mac compatible and came with a manual and related software that provided ease-of-use features. The drive installed itself on a computer and would be assigned a new drive letter to distinguish itself from other drives. It could handle high-capacity Zip disks and had a large drive slot to fit the disks. The Zip drive also contained a retro-reflective spot for identifying the proper disk media in order to prevent damage to the disk and drive.

At the height of its popularity, the Zip drive was considered a larger version of the floppy drive and certain manufacturers included Zip drives internally in their devices. It was favored in the graphic arts vertical market and was also economical for home users at the time of launch for storing large data. Zip drives were reportedly prone to click-of-death failures, which potentially resulted in media and data loss.

Zip drive work

Zip drives utilize a rotating magnetic to read, store, and erase data on the Zip disk which is then allowed to be removed from the drive for storage or transport. A flash drive does not use a rotating magnet media for data storage but instead uses a flash memory chip which only utilizes electricity. (Fig 2)

Fig 2

The function of the Zip drive in a computer

A Zip drive is a now-obsolete storage format used by some in the mid to late 90s. Zip disks could store 100MB, with 250MB and 750MB disks made available later. Some saw them as good alternatives to floppy drives, although not all computers had Zip drives.

Nowadays, Zip drives are a poor choice for data storage. USB flash drives, external hard drives, and optical disks (CD, DVD, Blu-ray).

If you're playing around with vintage computers, Zip disks might be useful for their large capacity. Keep in mind that Zip drives and disks aren't widely available anymore, although you can find them on eBay, or even at stores with vintage computing equipment.

DVD-ROM

What is DVD-ROM? It is the abbreviation of digital versatile disc read-only memory. DVD-ROM is one of the various types of DVD. Blank DVDs are usually DVD-R or DVD+R, with a readable and writable format. + R or -R refers to the format standard and is a rewritable or recordable DVD.

It is a read-only digital versatile disc (DVD) usually used to store large software applications. It is similar to CD-ROM, but with a larger capacity. The DVD-ROM can store approximately 4.38 GB of data. CD-ROM usually stores 650 MB of data. If you want to learn more information about DVD-ROM, you can continue to read this post from MiniTool.

Compared with CD-ROM, DVD-ROM has the same 5-inch diameter and 1.2 millimeters (mm) thickness. However, since DVD-ROM uses a shorter wavelength laser and the pits are tighter, the capacity of the disc has increased. The smallest DVD-ROM can store about 7 times as much data as a CD-ROM.

DVD-ROM permanently stores data files that cannot be changed, overwritten, or erased. Personal computers with DVD-ROM or DVD-RAM drives are designed to read DVD-ROM discs. Generally, DVD-ROM discs are not equipped for use with a DVD drive connected to a home theater system or TV. But many DVD-ROM drives can usually read DVD movie discs.

Based on size, there are four types of DVD What is DVD-ROM? It is the abbreviation of digital versatile disc read-only memory. DVD-ROM is one of the various

types of DVD. Blank DVDs are usually DVD-R or DVD+R, with a readable and writable format. + R or -R refers to the format standard and is a rewritable or recordable DVD.

It is a read-only digital versatile disc (DVD) usually used to store large software applications. It is similar to CD-ROM, but with a larger capacity. The DVD-ROM can store approximately 4.38 GB of data. CD-ROM usually stores 650 MB of data. If you want to learn more information about DVD-ROM, you can continue to read this post from MiniTool.

Compared with CD-ROM, DVD-ROM has the same 5-inch diameter and 1.2 millimeters (mm) thickness. However, since DVD-ROM uses a shorter wavelength laser and the pits are tighter, the capacity of the disc has increased. The smallest DVD-ROM can store about 7 times as much data as a CD-ROM.

DVD-ROM permanently stores data files that cannot be changed, overwritten, or erased. Personal computers with DVD-ROM or DVD-RAM drives are designed to read DVD-ROM discs. Generally, DVD-ROM discs are not equipped for use with a DVD drive connected to a home theater system or TV. But many DVD-ROM drives can usually read DVD movie discs.

Single-sided one layer data DVD (4.7GB data)

Double-sided two layers of data DVD (9.5GB) records on both sides of a disk.

Single-Sided two layers of data DVD (8.5GB) records on one side but have two recordable layers by superimposing one on the top of the other.

Double-sided four layers of data DVD (17GB) records on both sides. Each side contains two recordable layers of data.

The functions of a DVD-ROM drive

DVD-ROM. Digital Versatile disc-Read Only Memory drives are the direct evolution from CD-ROM drives. DVDs had greater capacity and performance. DVD-ROM drives can read CD-DA, CD-ROM, and CD-R/RW discs, but they also read DVD-Video, DVD-ROM, and (sometimes) DVD-Audio discs (Fig 3)

Fig 3

Important parts of a DVD drive

Optical Drive: Function and Components

- Laser. The laser is a beam of light that is used to read and write data on an optical disc. ...
- Rotational Mechanism. The rotational mechanism, or spindle, is a motor that spins the disc. ...
- Actuator. The actuator is a device that moves the laser beam across the disc. ...
- Controller.

Types of CD and DVD drives

CD-ROM drives only reads from CDs.

DVD-ROM drives are meant to read both CD and DVD. It also burns files to CDs but not DVDs.

DVD-RW writers accomplish all tasks of reading from and writing back to both type of disks.

HD-DVD and BLU-RAY

These are the two types of high-definition disk formats. HD-DVD is developed by Toshiba and the other disk format, Blu-ray is developed by the electronics giant, Sony.

Recently, there was a competition between the two formats. Because of size and durability Blu-ray outranks HD-DVD and chosen by entertainment industries.

For example, Single-layer HD DVD disc stores 14.7GB data whereas Blu-ray single layer disc stores up to 25GB data.

Magneto-Optical Disk (MOD)

A magneto-optical disk is a rewritable disk that makes use of both magnetic disk and optical technologies. It is similar to a magnetic diskette except for its larger size. Magneto-optical disks are seldom manufactured and used due to the advent of flash drives and DVD/CD drives, which are less expensive and have better writing time and reliability.

DVDs are mass-produced using molding machines that physically stamp data onto the DVD. Such discs are a form of DVD-ROM because data can only be read and not written or erased. Blank recordable DVD discs (DVD-R and DVD+R) can be recorded once using a DVD recorder and then function as a DVD-ROM. Rewritable DVDs (DVD-RW, DVD+RW, and DVD-RAM) can be recorded and erased many times.

Explains Magneto-Optical Disk

One of the most well-known examples of a magneto-optical disk is the Sony MiniDisc.

The magneto-optical disk has the following features:

It is capable of having high data intensity by means of a magnetic read/write head and a laser.

Like diskettes, the magneto-optical disk allows multiple rewrites.

The driver for a magneto-optical disk can verify the information written to the disk and will report any errors to the operating system. This often results in faster reading but slower writing, although it helps make data storage more reliable.

The magneto-optical disk is a special removable disk.

The design of the drive allows the inserted disk to be exposed to the magnetic head on one side and to the laser on the other side.

Its writing speed is faster than that of diskettes, but is slower than that of CD/DVD drives.

Convenience and reliability are much better than those of diskettes, along with high data capacity.

Update drivers and uninstall older drivers

Because drivers control how the mouse interfaces with the operating system, if they're out of date or corrupt, the mouse is not going to work properly. Make sure to have the latest drivers from the mouse manufacturer.

We also recommend going into Add or Remove Programs and uninstalling all previous mouse drivers and software. Uninstalling old software is important when moving between mouse manufacturers, like going from a Logitech to a Microsoft mouse.

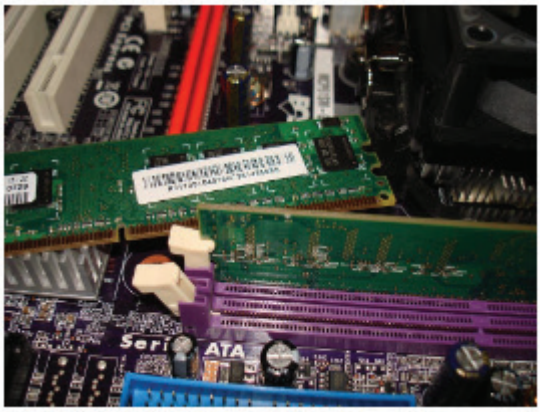
Computer Hardware Trouble Shooting

Objectives: At the end of this lesson you shall be able to
- **important points to be considered while purchasing and replacing componets of pc**
- **identify defects related computer hardware.**

Computer hardware safety rules

When installing/removing computer hardware and other peripherals (Fig 1)

Fig 1



- Wear proper apparel. Avoid acrylic or wool sweaters when working with electronic parts. Do not wear loose fitting clothing, rings, bracelets etc. (Fig 1)
- Unplug all computer equipment and peripherals before opening any covering cases.
- Keep your work area clean and well lit.
- Check for damaged parts.
- Do not force components into computer ports.
- Use an anti-static wrist strap or discharge yourself by touching a grounded metal object such as a computer casing.
- Power supplies produce several levels of voltage. Read the information on the power supply carefully and make sure that the power supply you are using is appropriate for the application.
- Replace all cases or coverings after inspections or installations.
- Check all circuits and installations with the instructor before power is applied.
- Retain all screws during disassembly in containers such as film canisters for proper reassembly.
- Electronic components should never become hot. Hot components means that there is a problem with the circuit. Disconnect any power immediately.

Safety Precautions

- Fully shut down and unplug the computer before you make any attempts to disassemble the tower.
- Take off any metal objects on your arms or fingers such as bracelets, rings or watches. Even if your unit is unplugged, there may still be some remaining electric charge.
- Make sure your hands are completely dry to avoid damaging any mechanical parts as well as to avoid electrocution.
- Work in a cool area to avoid perspiration for the same reason as seen in the previous number.
- Before touching any part within the tower, put your hands against another metal surface (such as the computer casing) to remove static charge, which may damage sensitive devices.
- Prepare a place to keep any screws you may remove. A container or piece of paper with labels for each part (casing, motherboard, CD drive, etc) is ideal to avoid confusion between the similar-looking screws.
- Handle all parts with care. Place each piece you remove carefully down onto a stable surface.
- If a component does not come out easily, do not forcefully remove it. Instead, check that you are removing it correctly and that no wires or other parts are in the way.
- Be careful when holding the motherboard, it's underside actually quite pointy and able to hurt you.
- Never attempt to remove the power source, a box attached to the side or bottom of the unit to which all cables are connected.
- When removing any cables, wires or ribbons, make sure to grasp the wire at the base or head to keep it from breaking.
- Be careful not to drop any small parts (particularly screws) into unreachable areas such as into the computer fan or disk drive.
- Take note that the three of the most damaging things to a computer are moisture (sweat, drinking water), shock (electric or from being dropped) and dust (any debris from household dust to bits of food).
- Have a safe experience in assembling your computer!

Important points to be considered while purchasing and replacing components

Being knowledgeable about what you need is the best way to save both time and money and make sure you have a reliable machine that does its job right. Before shopping, consider how you're going to use your new computer and do a little investigation to determine whether it's rated as a good buy for your buck.

- Most importantly, know what you want to use it for and set aside a realistic budget.
- The Processor. ...
- RAM (Computer Memory) ...
- Hard Drive. ...
- Graphics. ...
- Computer Software. ...
- Anti-Virus Software. ...
- Your Computer Lifeline, Internet.

Tools Required Active & Passive Maintenance

Preventive Maintenance Preventive maintenance is the key to obtaining years of trouble-free service from your computer system.

The two types of preventive maintenance procedures are active and passive. An active preventive maintenance program includes procedures that promote a longer, trouble-free life for your PC. This type of preventive maintenance primarily involves the periodic cleaning of the system and its components. The active preventive maintenance procedures include cleaning and lubricating all major components, reseating chips and connectors, and reformatting hard disks.

Active Preventive Maintenance Procedures Tools

- Contact cleaning solution
- Canned air
- A small brush
- Lint-free foam cleaning swabs
- Antistatic wrist-grounding strap
- Foam tape
- Computer vacuum cleaner
- Chemicals

Passive Preventive Maintenance

Passive preventive maintenance includes steps you can take to protect a system from the environment, such as

i Using power-protection devices;

ii Ensuring a clean, temperature-controlled environment; and

iii Preventing excessive vibration.

Passive Preventive Maintenance Procedures

Passive preventive maintenance involves taking care of the system by providing the best possible environment both physical and electrical for the system. Physical concerns are conditions such as

a Ambient temperature,

b Thermal stress from power cycling

c Dust and smoke contamination, and

d Disturbances such as shock and vibration.

Preventive Maintenance of Keyboard

i Do not spill liquids on the keyboard.

ii Periodically clean interior of keyboard with vacuum cleaner

iii Press the keys gently without applying force.

iv Use dust cover for keyboard when not used.

Preventive Maintenance of HDD

i Defragment hard disk at least once a month to maintain disk efficiency and speed.

ii Delete all temporary files such as *.temp,~*.*,*.chk and web browser history and temporary internet files.

iii Make periodic backup of your data and critical areas such as boot sectors, FAT and directory structure on disk.

Preventive Maintenance of FDD

i Clean read/ write head sensitivity using special diagnostic diskettes.

ii Check rotating speed of drive if it must be constant.

iii Clean & lubricate the mechanical part of drive

iv Clean read/write head using a head cleaning disk or clean head manually.

Preventive Maintenance of Monitor

i Use dust cover for monitor when monitor is off.

ii Do not put monitor near ti strong magnetic field which may cause improper deflection.

iii Clean the display screen so that it is dust free.

iv Provide proper ventilation such as cooling fan for heat dissipation to avoid intermittent failures.

v Do not put paper of anything on top of monitor

vi Preventive Maintenance of Monitor:

Preventive Maintenance of Printer

i Do not place printer near heat generating machines such as heaters and furnaces.

ii Clean exterior of printer using soft cloth with mild organic solvent.

iii Periodically clean out dust, paper fragments and dirt from its mechanism using soft brush.

iv Use quality ribbon to avoid damage to print head

v Use dust cover for printer when not used

vi Check paper feed path is free of jam vii) Lubricate mechanical parts.

Block diagram of a KB, function of controller, LED driver Sample circuit.

The LED driver circuit theory

In electronics, an LED circuit or LED driver is an electrical circuit used to power a light-emitting diode (LED). ... The voltage drop across an LED is approximately constant over a wide range of operating current; therefore, a small increase in applied voltage greatly increases the current. (Fig 2)

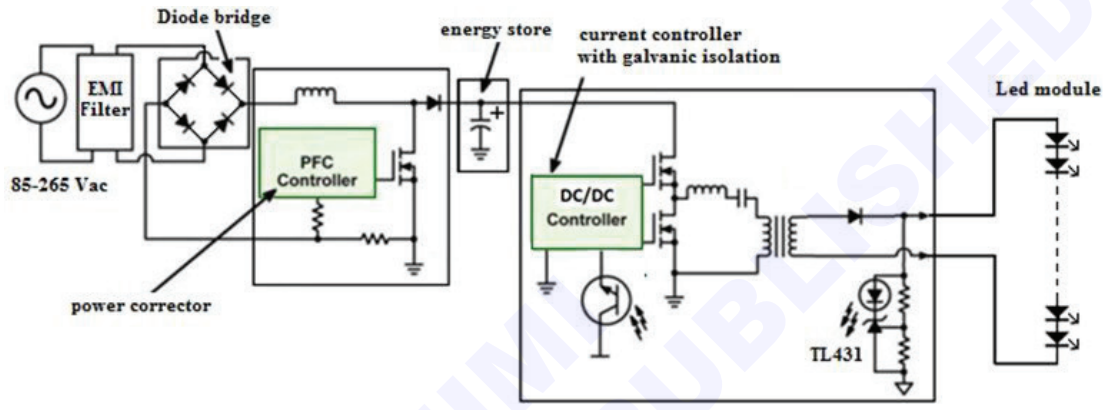
Function of LED driver

An LED driver rectifies higher voltage, alternating current to low-voltage, direct current. LED drivers also protect LEDs from voltage or current fluctuations. Any change in voltage could cause a change in the current being supplied to the LEDs

Troubleshooting Keyboard Problems

Most of the circuitry associated with the computer's keyboard is located on the keyboard itself. However, the keyboard interface circuitry is located on the system board. Therefore, the steps required to isolate keyboard problems are usually confined to the keyboard, its connecting cable, and the system board.

Fig 2



S.No.	Symptoms Basic	Keyboard Checks	Keyboard Hardware Checks
1	• No characters appear onscreen when entered from the keyboard. • Some keys work, whereas others do not work. • A Keyboard Error - Keyboard Test Failure error appears. • A KB/Interface Error - Keyboard Test Failure error appears. • An error code of six short beeps is produced during bootup (BIOS dependent).	The keys of the keyboard can wear out over time. This might result in keys that don't make good contact (no character is produced when the key is pressed) or that remain in contact (stick) even when pressure is removed. The stuck key produces an error message when the system detects it; however, it has no way of detecting an open key. An unplugged keyboard, or one with a bad signal cable, also produces a keyboard error message during startup. Ironically, this condition might produce a configuration error message that says "Press F1 to continue." If the keyboard produces odd characters on the display, check the Windows keyboard settings in Device Manager. Device Manager is located under the System icon (found in Control Panel) in Windows 9x and Windows Me. In Windows 2000, the path is similar—Control Panel, System,	If you suspect a keyboard hardware problem, isolate the keyboard as the definite source of the problem (a fairly easy task). Because the keyboard is external to the system unit, detachable, and inexpensive, simply exchange it with a known-good keyboard. If the new keyboard works correctly, remove the back cover from the faulty keyboard and check for the presence of a fuse in the +5V DC supply and check it for continuity. Neither the older five-pin DIN nor the six-pin PS/2 mini-DIN keyboards can be hot-swapped.

S.No.	Symptoms Basic	Keyboard Checks	Keyboard Hardware Checks
2	• The wrong characters are displayed. • An IBM-compatible 301 error code appears. • An Unplugged Keyboard error appears. • A key is stuck.	Hardware tab. However, in both Windows 2000 and Windows XP, Device Manager is usually accessed through the Computer Management console. If the keyboard is not installed or is incorrect, install the correct keyboard type. Also, be certain that you have the correct language setting specified in the Keyboard Properties dialog box (found by double-clicking the Keyboard icon in Control Panel).	If replacing the keyboard does not correct the problem, and no configuration or software reason is apparent, the next step is to troubleshoot the keyboard receiver section of the system board. On most system boards, this ultimately involves replacing the system board.

Defects related to Mouse and its related ports (COM, PS/2, USB) and servicing procedure

A computer mouse is a great tool when it's working properly. However, when it malfunctions, it can be a real headache. Luckily, most computer mouse issues are simple and can easily be resolved if you know what to do.

S.No.	Symptoms	Solutions
1	Movement of Mouse Cursor is Not Smooth	Due to dust in the sensor area of the mouse or on the surface on which the mouse is placed. Use a clean micro fiber cloth to clean the surface without using chemicals or other harsh cleansers. Then proceed to clean the surface where the mouse is used. If you happen to be using a surface such as a table or desk which has a glossy finish, this may interfere with how the mouse works. This is especially true in laser and optical mice. Glass may cause issues as well. If using the mouse on these glossy surfaces, try using a mouse pad instead, or any other mouse pad alternatives to see if this resolves the issue.
2	Mouse Lagging (Insufficient Hardware Resources)	Upgrade your hardware components, such as adding more RAM or replacing the graphics card, to improve mouse responsiveness.
3	Frozen Mouse Pointer	Check if your wired mouse is properly connected to your computer, or try plugging it into another USB port. If you're using a wireless mouse, make sure its batteries are full. When a mouse pointer freezes up, this can many times be because several applications are running in the background of the computer that you may not even be aware of. Check the Central Processor Unit, or CPU, to see what programs and applications you are currently running. If the computer mouse has simply frozen once, sometimes just waiting for several seconds may resolve the issue without doing anything further. If the problem persists, then check the bottom right corner of your desktop to see what programs may be running. Closing unnecessary programs can many times restore proper function to the mouse.

S.No.	Symptoms	Solutions
		If this does not resolve the problem, turn your computer off and restart it in order to get rid of any troublesome programs and applications that may have been lurking in the background.
4	Mouse is Just Not Working	A non functioning computer mouse could be the result of either software or hardware related issues. Possible causes could be a loose connection, bad wiring, faulty USB or PS/2 port, or a bad IR wireless receiver. Check out your ports with another device to make sure they are working properly. Also, some mice, either wireless or wired, require drivers to be installed in order to work properly. Make sure the driver is installed and up to date. If none of these steps get you up and running again, try the old standby of turning off your machine and re-starting it to see if this solves the problem
5	Too Fast or Too Slow	If your pointer is performing too fast or too slow, try going into the control panel, then to the mouse option, then to the pointer options tab. You will then be able to change the speed to a level that feels more comfortable to you. After making these adjustments, your computer mouse's pointer will most likely moving at a normal speed again and your problem solved
6	Double-Clicking Issues	Mouse double-clicking is frequently triggered by the accumulation of dust inside the mouse. To resolve this issue, try using compressed air to blow away the dust that has gathered around and under the mouse's buttons. Additionally, a defective mouse can also be a common cause of double-clicking. This occurs when the mouse circuit board malfunctions and registers a single click as a double click. If this is the case, consider either having your mouse repaired or purchasing a new one. Mouse double-clicking could be due to a software configuration issue as well. This can be resolved by going to the control panel, then mouse option, then buttons tab. Here you can change the speed level of the double click feature to a setting that works best for you
7	Unresponsive Buttons	Unresponsive buttons on a computer mouse can happen due to various reasons. Dust and debris buildup around the buttons can lead to decreased responsiveness or clicks not registering. Frequent use can cause physical wear and tear on the buttons, making them stick or become unresponsive. Loose connections within the mouse, such as wiring or connectors, can also result in intermittent button issues. Outdated or corrupted mouse drivers and conflicting software can interfere with button responsiveness.

S.No.	Symptoms	Solutions
8		To resolve unresponsive button issues, start by cleaning the computer mouse to remove dust and debris. Use compressed air or a cotton swab with alcohol for effective cleaning. Inspect the buttons for physical damage and consider repair or replacement if necessary. For wired mice, ensure a secure connection, and for wireless mice, check the battery. Update mouse drivers from the manufacturer's website and troubleshoot conflicting software by disabling unnecessary background applications.

Working principle of Light pen scanner and digitizer

A light pen detects changes in brightness of nearby screen pixels when scanned by cathode-ray tube electron beam and communicates the timing of this event to the computer.

A light pen is a computer input device in the form of a light-sensitive wand used in conjunction with a computer's cathode-ray tube (CRT) display.

It allows the user to point to displayed objects or draw on the screen in a similar way to a touchscreen but with greater positional accuracy. A light pen can work with any CRT-based display, but its ability to be used with LCDs was unclear (though Toshiba and Hitachi displayed a similar idea at the "Display 2006" show in Japan.

A light pen detects changes in brightness of nearby screen pixels when scanned by cathode-ray tube electron beam and communicates the timing of this event to the computer. Since a CRT scans the entire screen one pixel at a time, the computer can keep track of the expected time of scanning various locations on screen by the beam and infer the pen's position from the latest time stamps.

A digitizer, also known as a graphics tablet or drawing tablet, is a device that allows you to input drawings, sketches, and handwritten notes into a computer. It consists of a flat surface and a stylus or pen-like instrument that you use to draw or write on the surface.

Defects and symptoms related to HDD and its cable, connector and servicing procedure

S.No.	Problems	Solutions
1	**Hard Drive Not Found** (Chances are that while turning on your system, you might get the "Hard Drive Not Found" error on the screen. This makes your system standstill as it will not respond to most of the usual commands. The hard disk problem occurs when the internal cable connecting it has been damaged or is loose. Water or physical damage can also lead to this problem. A logical partition can also be lost or corrupted, in this case.)	**Solution 1:** Perform a hard reset This is the easiest way to fix this hard drive malfunction issue. Simply turn your system off and remove its power cord or battery. Also, disconnect all kinds of peripheral devices from it and press the Power button for 15 seconds. After waiting for a while, connect the battery/power cord (not the peripheral device) and turn it on. **Solution 2:** Check for physical damage While this might be a tedious job, you can consider opening up your system and checking the hard drive connection. If the connection is loose, then you can visit a professional as it would require soldering.
2	**Volume is Dirty (Hard Drive Error 0x80071ac3)** (As the name suggests, this error depicts that either the entire disk or a volume of the disk has been corrupted. When the problem occurs, users get an error like this with a hexadecimal code. The problem can happen with the internal as well as the external hard drive. A bad sector on your hard drive or an unexpected shutdown is the two primary causes of this hard disk problem. If it is an external drive, then an unsupported file system or driver can also be a reason for this.)	**Solution 1:** Check System Errors If a disk is not functioning in an ideal manner, then you should perform an automatic system check. To do this, just right-click its icon and go to its Properties. Under the Tools tab > Error Checking section, click on the "Check" button. Follow the simple on-screen instructions to resolve any system error. **Solution 2:** Reconnect the external device Most people get this error while using an external hard drive, USB drive, or SD card. In this case, simply remove the external drive and turn off your system. Restart it and connect the drive again to check whether you get the error back or not.

S.No.	Problems	Solutions
3	**Can't Boot the System** Since the internal hard drive also stores the firmware and the operating system, its failure can also result in the booting of your system. There are all kinds of prompts that users get in this case when the system can't boot. It happens when there is a change in the BIOS settings or the essential system files have been lost. The partition where the operating system has been installed can also get corrupt, resulting in this computer problem.	**Solution 1:** Restore default BIOS settings If there is an issue with your system's BIOS settings, then this will fix it. Turn on your computer and keep pressing the BIOS key, which can be F10, F12, F2, DELETE, etc. Once you enter the BIOS window, press F9 to restore the default settings. Exit it and restart your system now. **Solution 2:** Perform an advanced startup You can also take the assistance of a bootable media or a Windows installer to startup your system. Firstly, go to Windows Settings > Recovery > Advanced Setup and click on the "Restart Now" button. Also, connect a Windows CD/DVD or a bootable media to your system. This will let you reinstall Windows on the system or boot it from another media.
4	**Corrupted Hard Disk (Hard Disk #(XXX) Error)** As much as you try to avoid it, chances are that your hard disk can get corrupt unexpectedly. The error mostly occurs in HP systems, but even PCs from other manufacturers can also undergo the same. A malware attack on the system, a corrupted sector, or a bad program can be a major trigger for this. Also, if your system is trying to access any file that no longer exists, it can lead to this error.	**Solution:** Perform a Hard Drive diagnostic test Since this hard disk error is mostly associated with HP systems, we will consider its example to troubleshoot hard drives. In other systems, the respective key would be different. To fix this, just restart your system and press F2 to run System Diagnostics. The screen will display the relevant key to do it. As the diagnostic window will open, choose to perform Component Tests and select your Hard Drive from the available options. Confirm your choice and wait for a while as the system will run a thorough diagnostic and tries to fix this problem.1
5	**Hard Drive Error 0142** This is categorized as a major hard disk error as it depicts that the disk has failed to load the booting or system files. You might have to run a thorough diagnostic to fix this. If not, then you can consider resetting the system. The hard drive error mostly occurs due to a corrupted sector or a firmware related issue. You might have accidentally deleted a crucial system file as well, leading to the inaccessibility of certain OS components	**Solution 1:** Restart system in safe mode If a particular program or application has caused this hard disk problem, then you can consider restarting it in safe mode. To do this, just restart your system and press F8 a few times to enter its advanced boot options. The key might differ from one version to another. Use the arrow keys to select the "Safe Mode" option and press enter. This will boot your system in safe mode. **Solution 2:** Give your system a fresh start This is relatively a newer feature that is available in Windows 8 and 10. Ideally, it is equivalent to resetting a computer and will automatically remove all the installed programs and applications from it. Simply go to Windows Settings > Windows Defender & Security Settings > Device Performance and health. Go to the "Fresh Start" option here and get things started. Follow a simple click-through process to reset your system and get rid of any malicious entity.
6	**Data Loss from a Corrupt Hard Drive3** The hard drive is capable of storing a large amount of data which can be accessed at any time. However, sometimes you risk losing the important data contained in them because of failure or corruption of the hard disk. If an entire drive or a partition/sector has been corrupted, then it will automatically delete your saved files.	**Solution:** Use Recover it Data Recovery It doesn't matter what kind of data loss scenario you are facing, you would be able to move past it using Recoverit Data Recovery. It is one of the most advanced data recovery tools available for both Windows and Mac. The application is easy to use and has the highest recovery rates in the industry. You can recover your lost data not only from Windows/Mac's internal hard disk but also from external sources like USB drive, SD card, etc. All you need to do is follow these steps after downloading Recoverit on your system.

S.No.	Problems	Solutions
	There can be numerous reasons for causing data loss on your system. Corrupt storage, a faulty program, bad sector, malware attack, or any other disk-related issue can trigger it. You can also accidentally format or delete your data as well. While there are hardly any native solutions for this, you can try a dedicated third-party data recovery tool.	**Step 1:** Select where to scan Firstly, launch the Recoverit Data Recovery application on your system and select a location to scan. This can be your entire drive or a partition/folder in it. **Step 2:** Scan the hard drive As soon as you click on the "Start" button, the application will scan the selected drive or the partition. Simply wait for a while for the process to be completed successfully. **Step 3:** Restore your data In the end, the application will let you preview the files that it has extracted during the process. You can select the date of your choice and click on the "Recover" button to save it. Make sure you save it to a trusted location (and not the corrupt hard disk again).
7	**Corrupted Files** Corruption of system files usually occurs when the system shuts down suddenly, making it impossible for you to access your hard drive and thus your system. Some of the reasons for the corruption of the system files include power surges, use of malicious programs, accidental closure of a running program, and improper shutting down of the PC.	**Solution:** Close programs before PC shutdown The solution to this problem is to make sure that you close down all programs that are running before commencing to shut down your computer. Moreover, when shutting down the computer, you must do so in a standard manner. In addition to this, you should avoid installing malicious programs on your hard drive and keep cleaning it regularly so that no unwanted programs remain there for long.
8	**The Parameter is Incorrect** If you are trying to connect an external hard drive to your system, then you might get this error message. Subsequently, it won't let you access the data that is stored in your connected disk. An incompatible file system on the hard drive or physical damage can trigger this. If the disk is damaged, then it can also display the hard drive error.	**Solution 1:** Check USB port and drive Mostly, a damaged port, cable, or the drive can cause these hard drive issues. Make sure that the device is in working condition and the USB port is not damaged. Clean it thoroughly of any debris or dirt and reconnect the external hard disk to check its connection. **Solution 2:** Format the drive If the hard drive's disk format or file system is not compatible with your system, then it can also trigger this hard disk problem. To fix this, you can just format the drive. Simply connect it to your system, open My Computer, and right-click the hard drive's icon. Go to the "Format" option and select the file system to a compatible format (like NTFS). Click on the "Start" button to wipe the existing data on the drive and reset its file format.
9	**The Request Failed Due to Fatal Device Hardware Error** This is a fatal error that users get while working on an internal or external hard drive. While it is mostly linked to a hardware issue related to a device, sometimes even a logical error can also trigger this situation. If you are trying to access or copy a file that is no longer available, then you will get a hard disk error like this. Apart from a loose connection, a corrupt configuration, or incompatible driver can also be a trigger.	**Solution 1:** Reconnect the disk If these drive problems have occurred due to a loose connection, then you should consider this approach. Disconnect the external hard drive and restart your computer. Now, try to connect it again and check if the system detects the drive. You can consider disassembling the system and check if the internal hard drive has been connected properly or not. **Solution 2:** Reset the driver There are times when the hard drive malfunctions due to a driver related issue. In this case, you can consider resetting the driver to resolve this hard disk problem. Go to the Device Manager from the Start menu and expand the "Disk Drives" option. Select and right-click the driver option. From here, you can disable the device. Wait for a while and enable it again to resolve this hard drive issue.

Sl.No	Problems	Solutions
		Solution 3: Update the driver Apart from resetting the driver, you can also consider updating it as well. Simply launch the Device Manager option and select the driver listed under the "Disk Driver" feature. Go to its Properties > Driver tab and click on the "Update Driver" button. Now, you can just follow on-screen instructions to update the disk drivers on your system.
10	**The Disk is Full** This is certainly one of the most common hard drive problems that users face. If you have accumulated a lot of data on your disk, then it can run out of space. Not only can it corrupt your hard drive or cause it to malfunction, but it would also make your system run slow. The accumulation of tons of photos, videos, documents, and other unwanted files. You could have installed numerous unwanted applications as well. The frequent partitioning of the disk can also lead to its fragmentation.	**Solution 1:** Deleting unwanted content The easiest fix for this hard disk error is the deletion of any unwanted content. Just go to your disk's partition and start removing the videos, photos, documents, etc. that you no longer want. Just make sure that you don't remove any important system files in the process. Also, visit the Recycle Bin and empty it to make more free space on the disk. **Solution 2:** Uninstall unimportant applications If you have installed lots of applications and programs on your system, then consider getting rid of them. To do this, go to Control Panel > Programs > Programs and Features. In the newer Windows versions, go to Applications under Settings. Now, just select the program you want to remove and click on the "Uninstall" button. Follow the on-screen instructions to uninstall the selected program and restart your compute **Solution 3:** Defragment the disk When we keep on partitioning a disk or join different components, it leads to its fragmentation. Thankfully, with the help of the disk fragmenting tool, you can reclaim this lost space on your hard disk. To do this, just go to the Start Menu and look for "Disk Defragmenter". You can also access it from System Tools > Disk Defragmenter. Authenticate your account by entering the admin password and select the drive you wish to defragment.

Defects related to BIOS, upgrading and servicing procedure.

BIOS

A BIOS update is a process of updating the firmware that controls the basic functions of your computer hardware, such as booting, memory, and input/output devices. A BIOS update can improve the performance, stability, and compatibility of your system, but it also carries some risks and challenges. In this article, we will discuss some of the common errors or issues that may occur during a BIOS update process and how to avoid or fix them.

The common errors or issues that may occur during a BIOS update process

1 Wrong BIOS file

One of the most critical steps in a BIOS update process is to download and use the correct BIOS file for your specific motherboard model and version. If you use a wrong or incompatible BIOS file, you may end up with a corrupted or unusable system. To avoid this error, you should always check the manufacturer's website for the latest and compatible BIOS file for your system, and verify the file name and checksum before flashing it. You should also backup your current BIOS settings and data before updating, in case you need to restore them later

2 Power failure

Another common issue that may occur during a BIOS update process is a power failure or interruption. If the power goes out or the system shuts down unexpectedly while the BIOS is being flashed, you may damage the BIOS chip or render the system unbootable. To prevent this issue, you should always use a reliable power source and a surge protector when updating your BIOS, and avoid any activities that may cause the system to overheat or crash. You should also disable any power-saving features or automatic updates that may interfere with the BIOS update process.

3 Compatibility issues

Sometimes, a BIOS update may cause compatibility issues with some of your hardware or software components, such as memory, graphics card, operating system, or drivers. This may result in performance degradation, errors, or crashes. To avoid this issue, you should always read the release notes and changelog of the BIOS update file, and make sure that it addresses any known issues or bugs that affect your system. You should also update your drivers and firmware for your hardware devices before or after updating your BIOS, and test your system for stability and functionality.

4 User errors

Finally, some of the errors or issues that may occur during a BIOS update process may be caused by user mistakes or negligence, such as choosing the wrong update method, skipping important steps, or ignoring warnings or instructions. To avoid this issue, you should always follow the manufacturer's guidelines and recommendations for updating your BIOS, and use the appropriate tools and utilities provided by them. You should also backup your data and create a recovery disk or USB drive before updating your BIOS, and avoid any unnecessary changes or modifications to your BIOS settings.

Updating your BIOS can be a beneficial but risky procedure, so you should always be careful and prepared before attempting it. By following these tips and best practices, you can minimize the chances of encountering errors or issues during a BIOS update process, and enjoy the benefits of a smoother and more secure system

Defects related to CMOS, CMOS setup and servicing procedure

Primary Function of the CMOS

A computer's Basic Input Output System and Complementary Metal-Oxide Semiconductor together handle a rudimentary and essential process: they set up the computer and boot the operating system. The BIOS's primary function is to handle the system setup process including driver loading and operating system booting. The CMOS's primary function is to handle and store the BIOS configuration settings.

CMOS and Battery Backup

The CMOS is a physical part of the motherboard: it is a memory chip that houses setting configurations and is powered by the onboard battery. The CMOS is reset and loses all custom settings in case the battery runs out of energy, Additionally, the system clock resets when the CMOS loses power. The CMOS reverts to factory settings if it doesn't get power from the battery. It's a common practice to remove the battery to flash-back CMOS settings if there is a configuration problem.

CMOS Settings

The CMOS menu is accessed from the BIOS splash screen. You can typically enter it by pressing F1, F2, Del or Esc. The actual button varies from motherboard to motherboard. The CMOS menu contains the hardware customization options allowed by the motherboard, uses a simple graphical interface and is controlled by the keyboard. Customization features include memory handling, expansion port speed configuration, boot device order and power control. Microsoft recommends only adjusting these settings if you are an advanced user because some improper setting adjustments can render the computer unusable. Some advanced settings can overpower the system, causing it to produce enough heat to break it.

Troubleshooting

Incorrect CMOS Configuration

If the system can't start after a BIOS upgrade or a battery replacement, the CMOS might be corrupted. Re-enter the correct settings, save changes, and restart. An onscreen error message will usually indicate a CMOS problem. Otherwise, the settings might have been adjusted by a user. Try using the BIOS Setup auto-configure options, double-check drive configurations, save changes, and restart

S.No.	Trouble shooting	Rectification
1	**A power supply issue**	**Check the AC line.** • Check the power cord using a multimeter. • Open the cabinet. • Remove all power connections from various components. • Short green and black wire slots of ATX connector using a wire and check if the SMPS fan is working. • Check the output voltage. • Check whether the SMPS, connected to the motherboard is faulty.

S.No.	Trouble shooting	Rectification
2	**Motherboard errors**	**Remove the power connection from the motherboard.** • Check all the connections on the motherboard. • Restore the BIOS settings to default setting. • Check the CMOS battery.
3	**RAM**	**Remove the RAM modules and insert them into the slots again and start the PC.** • If there are multiple RAM slots, insert the RAM module into another slot and start the PC. • If there are multiple RAM modules, remove one RAM module and start the PC. If the PC is still giving problems, remove the RAM modules one by one and check. • If none of these steps help, replace the RAM module.
4	**HDD/ODD**	**Remove the connections to the motherboard and reconnect.** • Remove the power connection and reconnect. • Check by connecting the drive with another interface and power cable. • Check by connecting to a different SATA port on the motherboard. • Remove the HDD/ODD and connect it to a different system. If the HDD/ODD still gives problems, replace it.
5	**Issues with a Monitor**	**Check the power connection to the monitor.** • Remove the monitor connection from the PC and reconnect. • Check the connector if any pins are behinds. • Replace the interface cable.
6	**Keyboard/mouse**	**Disconnect keyboard/mouse from the PC and reconnect.** • Replace the keyboard/mouse.
7	**No display of a computer**	**Monitor is not on.** • Computer is a sleep mode. • Loose the display cable (VGA, HDMI). • Undo any recent changes. • NO post. • The binary Operating System may be corrupted. • Motherboard problem. • Bad RAM. • Video card is not working.
8	**No display problem**	**Check your monitor is Off or On and the computer is in sleep mode.** • Check whether your VGA or HDMI cable working properly or not. • Clear your BIOS configuration or clear your CMOS configuration. • Check whether your SMPS is working properly or not.

S.No.	Trouble shooting	Rectification
9	**No power**	• Power cord not connected properly. • Faulty power supply source. • Third-party hardware. • Defective power button of the cabinet. • Faulty POWER SUPPLY unit. • Motherboard not functioning properly.
10	**Keyboard not working**	**Check the connection between the keyboard and the system.** • Connect the keyboard directly to the system using a PS/2 or USB port. • Be sure that there are no bent, broken keyboards or missing pins in the PS/2 connector. • Verify that the keyboard is detected in BIOS. • Enable the USB setting in the BIOS for keyboard connection. • Check the port by connecting another keyboard to it. • To check if the keyboard is working, attach it to another computer. • Replace the keyboard controller or the entire motherboard in case the controller is damaged. • Otherwise the keyboard is replaced.
11	**Mouse issue**	**Check if the mouse is connected to the PS/2 or USB port properly.** • Verify that there are no obstacles like hair or fuzz to block the sensor. • Turn the mouse and remove the blocking from the hole, if any. • Clean or replace the surface of the mouse pad.
12	**Fatal error**	**Switch off the computer power and open the system case.** • Clear CMOS by removing the CMOS battery. • Switch on the computer and go to the BIOS setup. • Re-configure the BIOS settings to default and save changes & exit. • After the reboot, the computer should start normally.
13	Blue Screen of Death or Blue Screen Memory Dump (BSOD) is a Microsoft windows Operating System error screen that is displayed to indicate system conflicts and the potential for a crash.	**The main cause of BSOD** • Hardware malware attacks can cause this error. • Faulty memory. • Faulty hard disk. • Faulty BIOS settings. • Improper device drives installation. • Motherboard overheating. • Errors in the software of the system. • Issues regarding power supplies. • Overclocking the motherboard.
14	**BSOD error**	• Identify the problem or error code from the blue screen. • Research the error and its solution on internet. • Reset the BIOS settings to factory default settings.

S.No.	Trouble shooting	Rectification
15	**Beep codes**	**Turn on or restart the computer.** • When the computer begins to boot, listen to the beep codes carefully. Restart the computer to hear the beeping again. • Note down the pattern of the beeps. • Depending on the BIOS manufacturer, the solution will differ for the beep code. • Choose the correct beep code troubleshooting guide.
16	**Power button will not start computer**	If it is plugged into an outlet, make sure it is a working outlet. To check your outlet, you can plug in another electrical device, such as a lamp. If the computer is plugged in to a surge protector, verify that it is turned on. You may have to reset the surge protector by turning it off and then back on. You can also plug a lamp or other device into the surge protector to verify that it's working correctly.
17	**The sound isn't working**	• Solution 1: Check the volume level. Click the audio button in the top-right or bottom-right corner of the screen to make sure the sound is turned on and that the volume is up. • Solution 2: Check the audio player controls. Many audio and video players will have their own separate audio controls. Make sure the sound is turned on and that the volume is turned up in the player. • Solution 3: Check the cables. Make sure external speakers are plugged in, turned on, and connected to the correct audio port or a USB port. If your computer has color-coded ports, the audio output port will usually be green. • Solution 4: Connect headphones to the computer to find out if you can hear sound through the headphones.
18	**The screen is blank**	• Solution 1: The computer may be in Sleep mode. Click the mouse or press any key on the keyboard to wake it. • Solution 2: Make sure the monitor is plugged in and turned on. • Solution 3: Make sure the computer is plugged in and turned on. • Solution 4: If you're using a desktop, make sure the monitor cable is properly connected to the computer tower and the monitor.
19	**Hard Disk Failure**	Failure of hard disk can lead to serious problems. You can easily replace older hard disk with a new one but data stored on existing hard disk may become corrupt or lost. After installing new hard disk on you computer, you can attach existing hard disk as secondary disk on you computer. Mostly data stored on existing hard disk is displayed. After recovering the data your can dismantle the corrupt hard disk. They best way is that you should keep backups of your most important files and documents. Google drive or other such free cloud storage are good means to store data online which can be recovered easily in case of hard disk failure.

S.No.	Trouble shooting	Rectification
20	**Noises from computer**	Multiple functions take place while working with computer. Most commonly noises are produced by hard disk drives, optical disk drives, cooling fans when powering up or when in use. Cooling fans make noise as they spin. Many of these components can make noises as they fail or become old.
21	**Overheating**	As power flows through different components of a computer, they heat up. Components include CPU, hard disk drives, graphic cards, SMPS (power supply) and motherboard. Most of these components work perfectly fine with normal heat. But when the heat grows too high, it may cause system failure or even damage components. That's why CPU, graphic cards and power supply have their own cooling fans.
22	**Computer Automatically Turns Off or Restarts**	There are many reasons for this problem. If you're running a Windows operating system, an automatic Windows Update may restart the computer. If you're playing a video game and the computer shuts off, it could be due to problem with your power supply.
23	**Monitor Not Showing Anything**	• Check the video cable that connects monitor and the computer. If it is loose, you may not see the output on monitor screen. • It may happen due graphics card failure, driver issues, or problems with the graphics ports on the computer. • Detaching and attaching RAM on you motherboard can solve this problem. • There may be problem with the motherboard. You may get it repaired or replace it with new one to solve the problem.

S.No.	Explanation	Diagnosis	Troubleshooting steps
1	DRAM refresh failure The system is having a problem accessing the system memory to refresh it. Refreshing is done on all system memory to keep its contents active.	This code usually means a problem either with the system memory or with the motherboard itself.	Troubleshoot the mother board. • Treat as an apparent memory failure.
2	Parity circuit failure The parity circuit is responsible for generating and checking the parity bit on the system memory when parity checking is used. This circuitry is not working properly	This code usually means a problem with either the system memory or the motherboard	Treat as an apparent memory failure. • Troubleshoot the mother board
3	Base 64K RAM failure There is a failure of some sort within the first 64 KB of system memory.	The first bank of memory probably has a bad memory chip in it somewhere. It is possible that there is a failure related to the motherboard or a system device as well	Treat as an apparent memory failure. • Troubleshoot the mother board.
4	System timer failure There is a problem with one or more of the timers used by the system to control functions on the motherboard.	This is usually a motherboard failure	Troubleshoot the mother board.

S.No.	Explanation	Diagnosis	Troubleshooting steps
5	Processor failure The system processor is generating an error condition indicating a problem with it.	There is a problem related to the processor or motherboard. Note that this doesn't mean that the processor is necessarily dead; with a dead processor the system won't boot at all (it runs the BIOS code that is used to start up the PC.)	There is a problem related to the processor or motherboard. Note that this doesn't mean that the processor is necessarily dead; with a dead processor the system won't boot at all (it runs the BIOS code that is used to start up the PC.)
6	Keyboard controller / gate A20 failure The keyboard controller is a chip on the motherboard that communicates with your keyboard. It also controls the A20 gate that provides access to the high memory area (HMA). This component is indicating a failure	This is usually a problem with either the keyboard or the motherboard	• Troubleshooting the keyboard is relatively easy; try that first. • Troubleshoot the key board controller Trouble shoot as a mother board failure
7	Virtual mode exception error Virtual mode is one of the different modes that the processor can run in. The system is reporting an error when testing this mode	There is a problem related to the processor or motherboard Note that this doesn't mean that the processor is necessarily dead, since the system won't boot at all with a dead processor.	• Troubleshoot the processor. • Troubleshoot the motherboard.
8	Display memory read/write failure The BIOS is unable to write to the frame buffer memory on the video card	This is usually caused by a problem with the video card, or the memory on the video card. It can also be a motherboard issue. Note: Unlike the other AMI beep codes, this one is "nonfatal". The system may continue to boot despite this error.	• Troubleshoot the video card. • Troubleshoot the motherboard
9	ROM BIOS checksum failure The read-only memory (ROM) containing the BIOS program (which is what is running when you turn on the PC and what generates this error) uses a checksum value as a double check that the ROM code is correct. This checksum is compared against the values in the ROM each time the PC is booted and if there is a mismatch, this code is generated	The BIOS ROM chip on the motherboard is probably faulty. It could also be another component on the motherboard.	Troubleshoot the motherboard. It is possible to replace just the BIOS ROM chip but often replacing the motherboard will make more sense for cost and simplicity reasons.
10	CMOS shutdown register read/write error A component of the motherboard is producing an error interacting with the CMOS memory that holds the BIOS settings.	There is likely a problem with the motherboard.	Troubleshoot the motherboard.
11	**Cache memory error** The system has attempted to verify the operation of the secondary (level 2) cache and has encountered an error	This usually means a problem with the system cache. It may also be a more general problem with the motherboard.	• Troubleshoot the secondary cache • Troubleshoot the motherboard.

S.No.	Explanation	Diagnosis	Troubleshooting steps
12	Memory or video problem The system is producing constant beeping in no specific pattern, or a fast "ringing" sound.	The memory is more likely--the system complains long and loud if it can't find any usable memory, as there is no way to even start the boot process when this is the case. The motherboard itself could also be the problem.	Troubleshoot the system memory. • Troubleshoot the video card. • Troubleshoot the motherboard.
13	Memory problem There is a failure of some sort related to the system memory.	The first bank of memory probably has a failure of some sort; this is usually just a physical problem such as an incorrectly inserted module, but may also mean a bad memory chip in a module. It is possible that there is a failure related to the motherboard or a system device as well.	Treat as an apparent memory failure. • Troubleshoot the motherboard.
14	Video error The BIOS is unable to access the video system in order to write any error messages to the screen.	This is usually caused by a problem with the video card, or the memory on the video card. It can also be a motherboard issue	Troubleshoot the video card. • If the video card is not at fault, troubleshoot the motherboard.
15	Video error The BIOS is unable to access the video system in order to write any error messages to the screen	This is usually caused by a problem with the system memory, or possibly the video card. The memory is more likely--the system complains long and loud if it can't find any usable memory, as there is no way to even start the boot process when this is the case. The motherboard itself could also be the problem.	Troubleshoot the system memory. • Troubleshoot the video card. • Troubleshoot the motherboard.

Introduction of Tablet and their troubleshooting techniques

Objective: At the end of this lesson you shall be able to
- **define tablet, parts and their troubleshooting techniques.**

Computer Tablet introduction

A tablet is a wireless, portable personal computer with a touchscreen interface. The tablet form factor is typically smaller than a notebook computer, but larger than a smartphone. (Fig 1)

A tablet PC also known as a tablet computer or simply tablet is a smaller version of a laptop computer and a larger version of a smartphone. All tablets feature a touchscreen interface, allowing users to engage with the device using touch commands and easily access many applications without needing an external keyboard or mouse.

That said, users can connect an external keyboard or mouse to a tablet. In fact, many users prefer to work with an external input device for gaming, to create documents, access websites and do other tasks on a tablet.

Unlike many laptops, a tablet is a highly portable device, making it easy to carry and transport. And compared to a smartphone, tablets feature a larger form factor and larger screens, those providing a larger and clearer display experience. Tablets also provide greater storage capacity and a longer battery life compared to smartphones.

Like both laptops and smartphones, tablets are built to work in online and offline modes. Depending on the model and country of operation, tablets are compatible with most wireless and cellular data networks.

Image of tablet computer

Fig 1

Block diagram of tablet (Fig 2)

Tablet computer ports and keys (Fig 3)

Fig 3

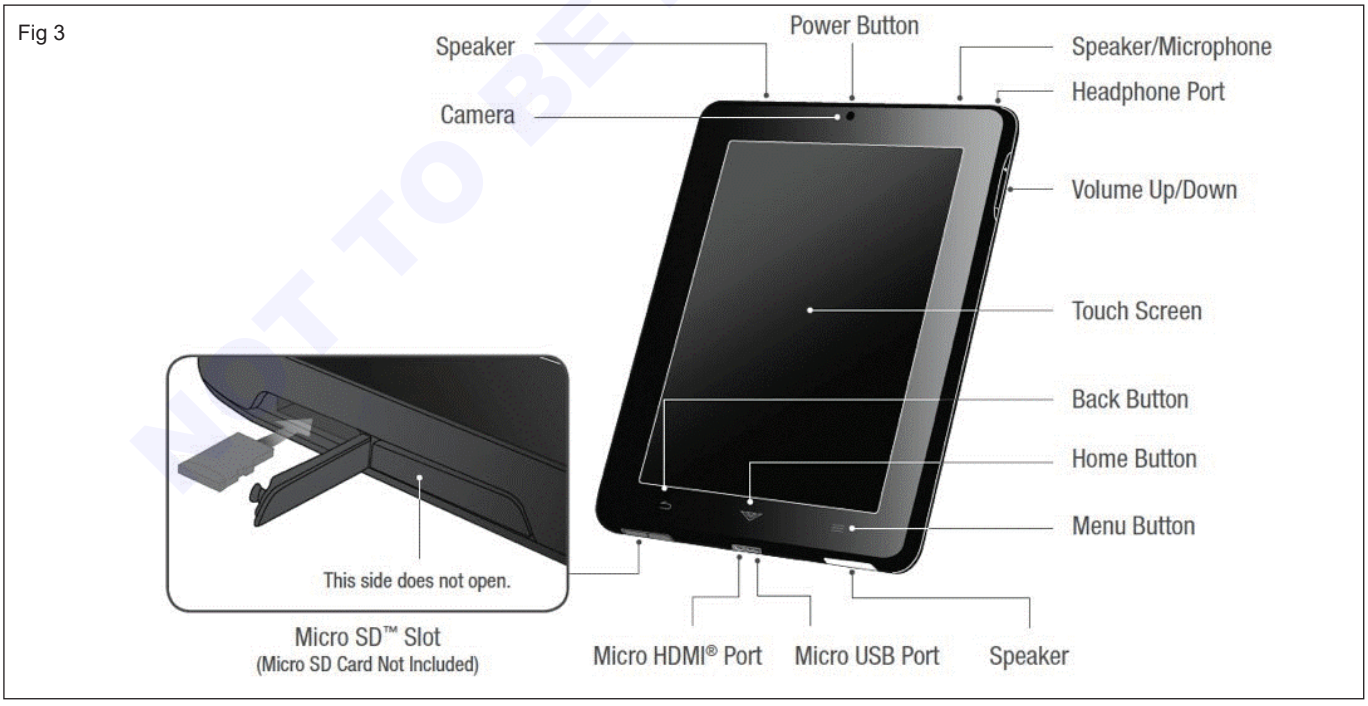
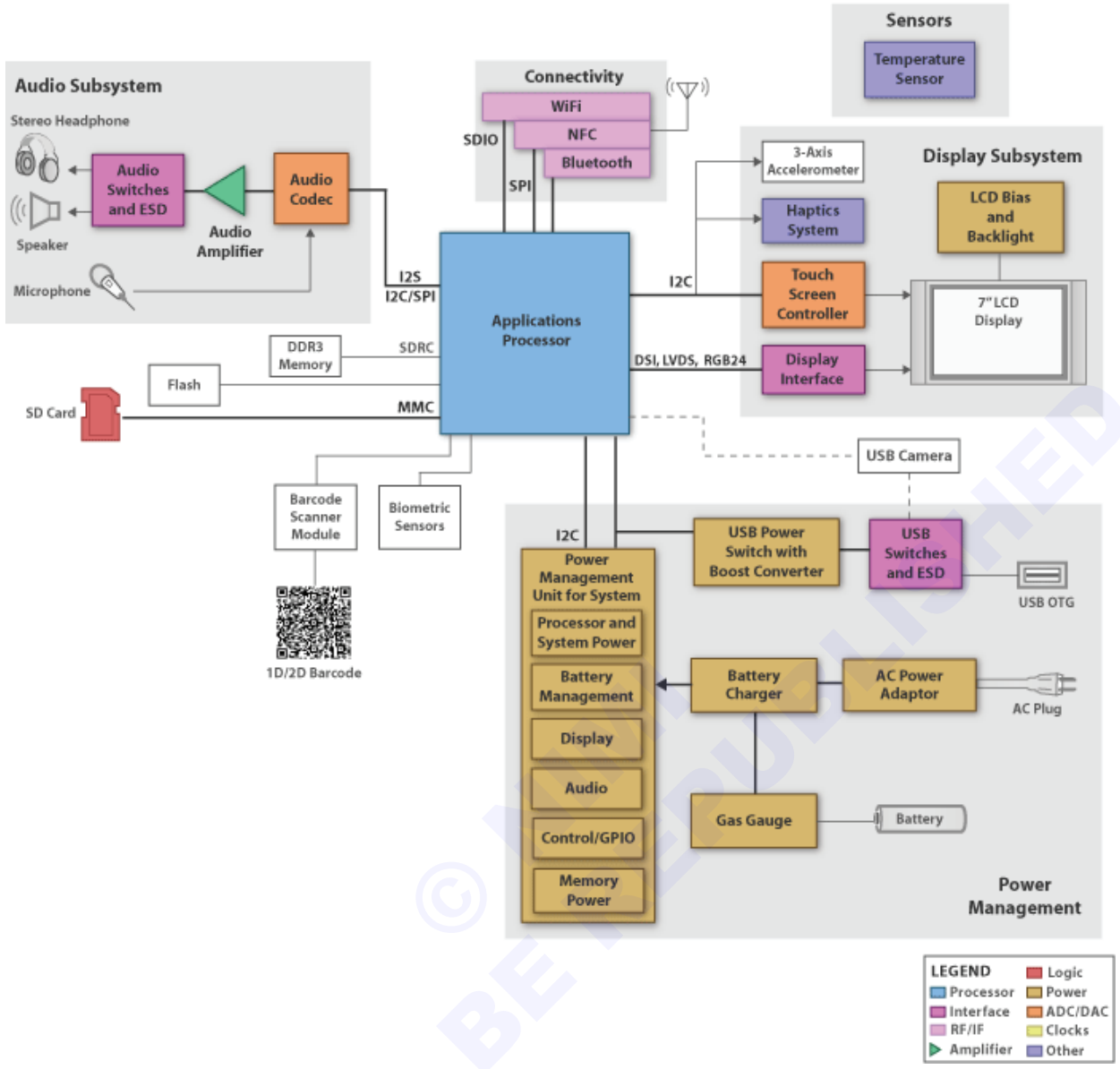


Fig 2



Parts of a tablet PC

- Touchscreen
- LCD – liquid crystal display
- Motherboard
- Rechargeable battery, and, certainly,
- Tablet casing, which, is usually composed of two parts – the rear panel, and the front panel, holding the touchscreen. (Fig 4)

The touchscreen is the input device responding to finger tips that allows the user to communicate with the device in a user-friendly manner. The growing popularity of the mobile device touchscreens has eliminated conventional mechanic keyboard while provided the tablets with bigger screens, as well as made web surfing substantially simple, thus increasing multimedia characteristics of the devices.

LCD – liquid crystal display

The most frequent problem of tablet LCDs will always be mechanical damage, in other words – the screens that suffer of fractures. Should you have experienced such problem, our store will always help you. In our store you can find the variety of LCDs for tablets supplied in various sets: LCDs separately, LCDs with touchscreens, as well as LCDs with binding frames.

Mother board:

Definition of the Motherboard is also known as a mainboard, planar board or logic board, system board, mobo or MB. It links all the individual parts of a computer together and also, allows the CPU to access and control these separate parts. (Fig 5)

A motherboard provides the electrical connections by which the other components of the system communicate. Unlike a backplane, it also contains the central processing unit and hosts other subsystems and devices.

Fig 4

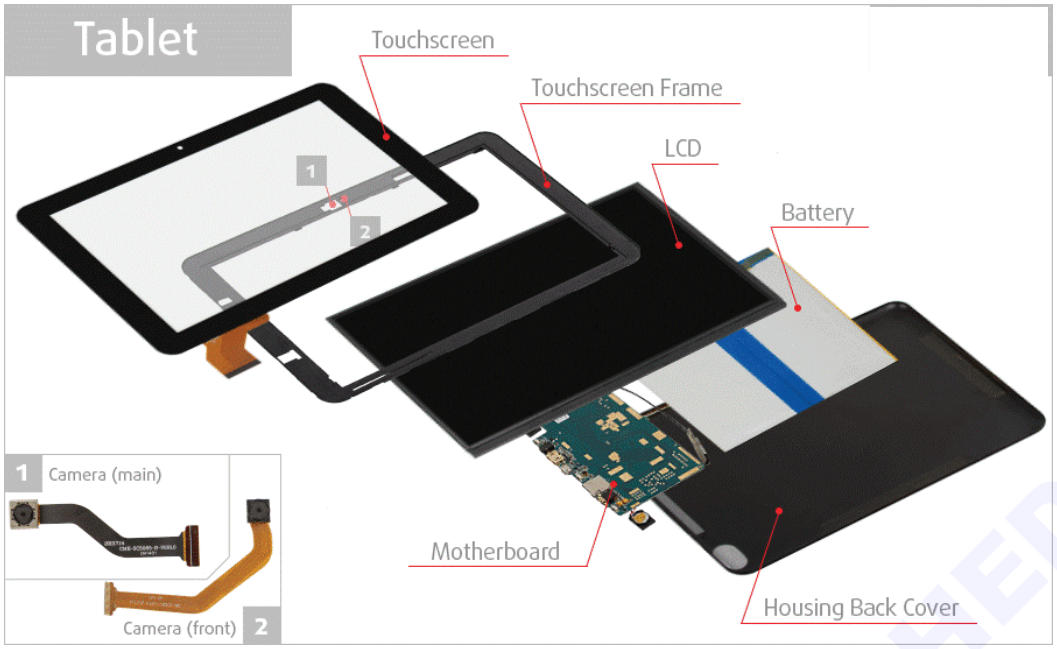
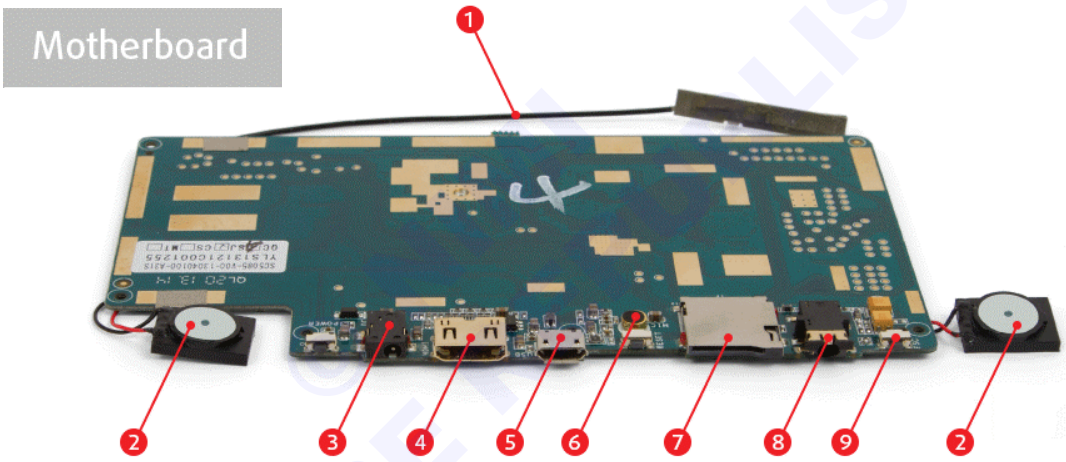


Fig 5



Parts of tablets motherboard:

1 **Coaxial cable:** These cables are used for connecting antenna and motherboard that are usually soldered together or connected with a special connector.

2 **Speaker (buzzer):** The small size speaker, which main purpose is playing tunes, speech, movie soundtracks, games sound as well as any other sounds reproduced by your device.

3 **Charge connector:** Some manufacturers install this unit separately to clear up some space for the USB connector, when the operation of the device is necessary during the charging process, and, in some cases, charging may be conducted only through micro-USB port (Item No.5 on the illustration)

4 **Mini-HDMI connector:** This unit is specifically designed to transmit video signals to other devices, such as TV set, computer display or projector.

5 **Micro-USB connector:** The connector which is typically used to connect external keyboard, mouse, memory card, as well as used to connect tablet to PC and for other purposes.

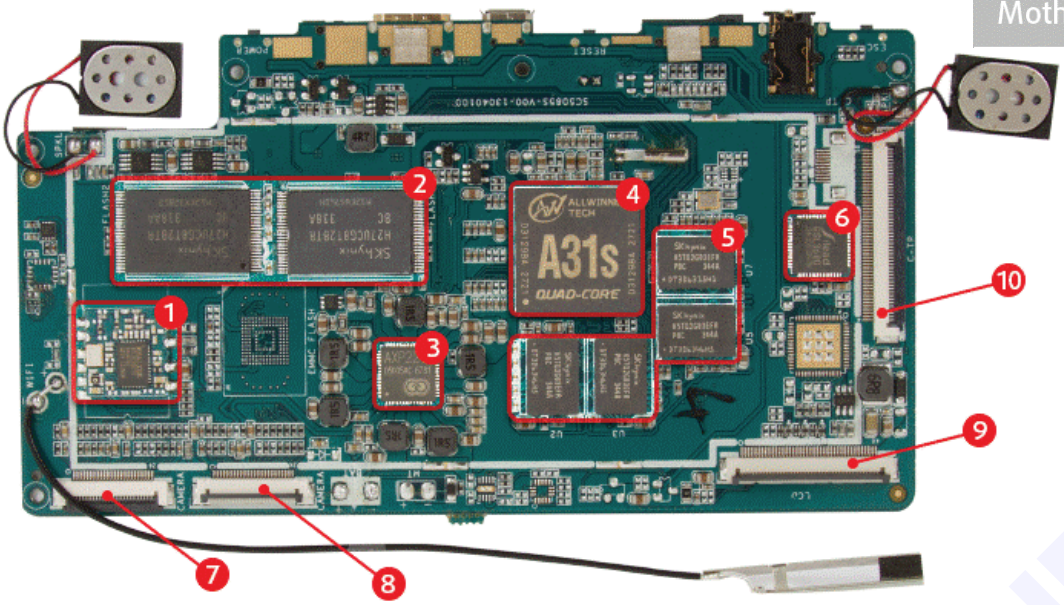
6 **Microphone:** This device is used to convert mechanical (sonic) waves into electric signals to record or transmit your speech.

7 **Memory card connector:** Typically, this unit is used to increase memory volume for data storage. Looks similar to the SIM-card connector. This module is missing on the disassembled tablet body shown on the picture.

8 **Handsfree connector:** Holding a tablet to your ear is so much inconvenient, that is why, you may opt to use external headset with a microphone.

9 **Tablet power button:** The other side of the motherboard hosts various electric elements, micro electric circuits and connectors for LCD, touchscreen, and cameras. Micro electric circuit, in other words, microelectronic integrated circuit or chip (microchip) – is the miniature electronic circuit, printed on a semiconductor substrate or seal, and is usually installed into the undismountable casing. (Fig 6)

Fig 6



1 Bluetooth operation module, Wi-Fi and FM-radio units.

2 ROM – read only memory, which stores information saved by user, photo, video, documents and programs.

3 Power management chip, in other words, power supply unit, designed for charging tablet as well as conducting power to other internal components.

4 CPU – central processing unit, which is basically the “brain” of the device that computes data with performing arithmetical and logic operations as well as operates other devices. The main characteristics of the device are processor speed and productivity. Another important feature is the CPU’s power consumption.

5 RAM – random access memory unit, that is, basically, working memory. This memory type is designed to provide short-time storage for variable data while CPU performs operations on the data. This is the place to keep all the running programs and their data.

6 Touchscreen controller. This micro electric circuit, with the algorithm recorded in it, allows the CPU to perform floating point operations and converts them into digital code read by the CPU. Also, there are cases where micro-controller may be attached directly to the touchscreen's flat cable.

7 Primary camera connector.

8 Front camera connector.

9 Display connector.

10 Touchscreen connector.

The tablets with mobile network support also have an amplifier, while the rather expensive models even have video processors.

The device's portability is provided, first and foremost, by a rechargeable battery.

Rechargeable batteries are different in their chemical makeup, voltage, capacity and size. We offer the variety of the rechargeable batteries for tablets.

The rear panel

The rear panel design defines comfortable holding in hands, mechanical crash resistance of the device, and, of course, the device’s overall appearance.

Testing of Various parts with Multimeter:

Testing Components on PCB boards with multimeters is important in the Fault Finding of Mobile Phones. In this testing method, SMD components like Resistor, Capacitor, Diode, and Coil are tested for fault.

While Testing these components, one should keep in mind that the Red Probe of the multimeter should be placed on the ground and the Black probe of the multimeter will be the testing point.

Generally, 99% of capacitor & 70% of Diode would be in parallel connection. Likewise, 99% of Coil and 95% of Resistor would be in Series connection. Most of the PCB board would be configured in the above ratio.

During testing, It is very important to know whether the SMD component is connected in Parallel or Series.

During testing (Red probe on the ground and black probe as testing lead) of components connected in a series circuit, the multimeter will give a value above 250 ohms on both sides of the SMD component (Coil, Resistor).

Likewise, for Parallel Circuit, the multimeter will give a value above 250 ohms on one side and would get beep sound (ground) on the other side of the SMD Component (Capacitor).

If you get a beep sound (ground) on both sides of the component, then check all the components in the

particular section and then remove each component and check for short.

Note: If you get a value less than 200 ohms, the entire SMD component in the particular section needs to be checked.

Various hardware problems:

Check the power button: Ensure that the power button is not stuck or damaged. Use a different charger: Try a similar voltage third-party charger if the original charger doesn't work correctly. Try hard reset: Hold the power and volume down buttons for 10-2

Common Tablet Problems And Solutions

There are many tablet problems, and you can use different approaches to fix the issue. It will enable you to fix any tablet problem before visiting any repair shop. Here are some of the common tablet problems and their solutions:

Battery not charging

Users experience changes in the battery charging process, either it slows down or does not charge completely. In some cases, it's not charging as usual. In such cases, you examine the battery or check any hardware-related issues.

If you can confirm your battery has issues, all you need to do is to purchase a new one. Other recommendations you can take include the following:

- Check the charging ports and remove any dirt that may prevent direct contact between the charger and the power source.
- Confirm that the USB cable and adapters have no issues.
- Ensure the power source is on.
- Avoid using the tablet to perform different activities while charging.
- Use a different cable to charge the phone to see if the problem persists.
- For hardware issues, visit us for repair services.

Overheating

The tablet gets very hot when you use it for a long time without rest. Others overheat when you connect them to the charger and start using them while charging. Many users reported cases of their battery exploding due to overheating, causing many worries.

It's a usual scenario, but it can worsen when it overheats and turns off. When you experience such behavior, look at your battery to ensure it's okay. If you have no idea how to check if the battery is ok, visit the nearest technician for more consultation.

Unresponsive touchscreen

The tablet touchscreen becomes unresponsive when you try to use or touch it. Most users find it hard on which direction to take as they feel it's more technical. We have several steps one can take before asking or visiting any technician.

Some of the troubleshooting tips one can take include:

- Remove all the sim cards and other cards and turn off the tablet. It helps the system in resolving the issues.
- Download and install a screen calibration application from the Google App store to improve the screen responsiveness.
- Contact the technician if the two solutions above do not solve the problem.

Slow performance issues

After using a tablet for a while, it becomes slow, giving the users stress. It can also happen if you use the same tablet for longer. Malware and viruses can also slow them down and the activities we use the tablet for, i.e., playing games, watching movies, and browsing.

Some of the actions one can take to improve performance include:

- Uninstall all the applications you are not using anymore and delete all the unnecessary files to increase the device storage.
- Install antivirus software to detect and clean any malware and protect your tablet from further infections that slow down its performance.
- Clear all the application's cache to provide more storage.
- Analyze all the applications running in the background and the resources they consume. If you feel some consume a lot of space, you can disable them.

The device fails to turn on when you want to use it. It's widespread, and there are solutions to try:

Remove the battery from the device for a short period, reinsert it, and try turning it on again.

Hold the volume down and power buttons for 10 seconds to force a restart. If it fails, connect it to power for around 40 minutes to fix the current battery drain issues.

Restart the tablet using safe mode.

Tablet not connecting to WiFi

Most tablet WIFI issues are mainly due to network issues, not the tablet alone, as many expect. One can take several steps to fix the WIFI issue. Some of the solutions one can try include.

Check device settings like GPS locations, parental controls, wifi not turned on, and third-party blocking.

Forget all the WIFI networks and reconnect again.

Confirm the distance from where you are browsing to the router is short.

Contact your Internet Service Provider

Camera issues

When you open your tablet camera and try to take a picture or record a video for your social media handles or memory, it's not working. Restart the device and try to take a picture to see if it solves the issue.

If the problem persists, open the camera application. Go to the storage data and clear all the cached data. After doing this, restart the application and try taking another picture.

The last method to fix the camera issue is to confirm the camera permissions. If it allows the user to have access to the device camera. For most users, a restart fixes the problem.

Cracked screen

The screen cracks when you hit your tablet on a hard surface, or it falls on the ground. It makes it hard to use the tablet again. Visit our repair shop to help you replace the screen to avoid further damage.

Tablet not connecting to PC

When users want to transfer some files from the tablet to the computer, they face several issues making the transfer fail. You can fix this by doing the following:

Enabling USB debugging on your device.

Try connecting the tablet with a different cable.

Check the computer USB ports to ensure they are in good condition.

Tablet keyboard issues

Tablet users cannot survive without keyboards. They use them in most activities, i.e., sending and replying to messages, browsing, and navigating the device. The keyboard reaches a point, and it stops working.

Some of the common methods of solving the issue include:

Remove all the third-party keyboard applications installed and use the default one.

Close all the applications running in the background and optimize the battery and other settings.

Check any pending updates and install them

Causes of Common Tablet Problems

There are many causes of tablet problems. You can avoid these issues by being very keen on the tablet's behavior. Some of the common causes include:

Use of faulty USN cables and charging ports.

Having pending software updates.

Attack of computer viruses and malware on your system.

Issues with the Internet Service Provider.

Insufficient storage on your device.

Installation of third-party applications.

Running of background applications.

5 Check for background processes

Some apps may run background processes that consume significant system resources, leading to overheating. Close any unnecessary background apps or use a task manager to manage running processes.

6 Clean the tablet's cents and ports

Dust and debris accumulation can hinder proper ventilation, leading to overhealing. Gently clean the vents and ports of your tablet using a soft cloth or compressed air. If your tablet continues to overheat despite taking these steps, we recommend consulting a professional tablet repair technician. They can diagnose any hardware-related issues, such as a malfunctioning fan or thermal management system, and provide appropriate solutions to resolve the problem.

Flashing a tablet

Flashing an Android phone is a complex process that involves installing a new firmware or operating system on your device. This can be necessary if you want to update to a newer version of Android, fix software issues, remove a virus, or even install a custom ROM.

Best 8 Android Flashing Software

- Top 1: DroidKit – Android Phone Toolkit (Recommend)
- Top 2: System Repair for Android.
- Top 3: Android Repair Master.
- Top 4: Smartphone Flash Tool.
- Top 5: Odin Flashing Tool.
- Top 6: Flashing Utility.
- Top 7: Kingo Root.
- Top 8: Cyber Flashing.

Mobile flashing software

Android Flash Tool is a web-based tool that lets you flash an Android build to your device for development and testing. Note: Android Flash Tool is easier to use than the fastboot flashall command, but supports fewer reference devices.

The disadvantages of flashing a phone

Disadvantages: Warranty concerns: Installing a custom ROM may void the warranty of the device, as it involves modifying the original software. Security risks: Custom ROMs may not receive official security updates, potentially leaving the device vulnerable to security threats.

Update android tablets

Updating Android tablets running on OS version Marshmallow (6.0), Lollipop (5.0-5.1), and KitKat (4.4) are a bit different from the Android tablets running on the previous version (Jelly Bean). Follow these below-given steps to update these devices:

1 Launch your Android tablet's Settings applications that look like a gear icon.

2 Scroll the Settings screen and tap on the About device.

3 Now, hit download updates manually; if there are any updates available for your device, install them.

Update Android Tablets Running on Jelly Bean version

To update the Android tablets running on Android Jelly Bean (4.1 to 4.3) version, follow the below-given steps.

1 Open the Settings applications of your tablet device, which looks like a gear icon on the home screen.

2 Scroll the Settings screen and tap on the About device.

3 Tap on the Software update.

4 Finally, update your device.

Update Android Tablet by rooting process

Rooting Android tablets let you navigate deeper inside the device sub-system that is normally blocked for end-users. Once you root your device (Android tablet), you can customize anything that Android allows. You can install and update the latest version of Android OS on your Android tablets.

It is suggested to keep a backup of your tablet device so that you can revert the rooting process if your device does not support an upgraded version. If the Android OS version you are updating on your device is not compatible, the backup will help you revert to the device's original settings.

1 Search for the rooting software for PC that supports your Android tablet on your desktop browser. Select the one you trust and is compatible with your tablet from the search result.

2 Download and install the rooting software on your PC. Once the installation of the application gets complete, launch it.

3 Now, connect your Android tablet with your computer with the help of the USB cable that comes with your tablet.

4 The application automatically detects your tablet. Now click on the Root button to start the rooting process. Follow the on-screen instructions to finish the rooting process successfully.

5 Restart your tablet, and you will find that the device is running on the newer Android version you installed.

Unlock a Locked Tablet

There are four key ways to lock a tablet

- **Pattern:** You selected a pattern drawn by swiping between a grid of nine on-screen dots. To unlock the tablet, you'll need to swipe the same pattern.
- **PIN:** A pincode is a string of four or more numbers. To unlock a tablet with a pin, you'll need to select the same numbers in the same order they were when the tablet was originally set up.
- **Password (Passcode on iPad):** Instead of numbers, a password can contain four or more letters or numbers. This could be a memorable word, date, place, or person. To unlock a tablet with a password, you need to input the same password used to set up the device.
- **Biometrics:** Some tablets offer finger print or face recognition logins. To unlock the device, you'll need to use the same finger in the same orientation as it was when added, or show the same face as the person who set up the device.

  To be able to unlock the tablet, you'll need to use the method used when setting up the device.

Unlock Android Tablet If I Forgot the Pattern Lock

If you have forgotten the pattern to unlock your Android tablet, your first port of call should be to try everything you can to remember it. If you have written it down somewhere, try to find it.

If you really can't remember the pattern on a Samsung tablet, you can use Samsung's Find My Mobile website, but you'll need to know your Samsung account details to login there.

Some older Android tablets can use password recovery functions, but if your tablet is only a few generations old, you'll have to factory reset it.

Unlock a Tablet Without the Password

There is no effective way to unlock a tablet without a password. There are some third-party applications which purport to offer that ability, but you should treat any such claims with extreme caution as you risk giving access to your data to the software's developers.

Without the pattern or password, you'll need to factory reset the Android tablet.

When it's set back up again, you could always consider turning off Android's lock screen feature to avoid any problems like this again, but doing so is a severe security risk

Concept IOS

Apple iOS stands for iPhone operating system and is designed for use with Apple's multitouch devices. The mobile OS supports input through direct manipulation and responds to various user gestures, such as pinching, tapping and swiping.

Features of IOS

It is the operating system that powers Apple's iPhones today. The iOS has evolved over the years and today integrates features and functionalities like multitasking, cloud syncing, augmented reality, and machine learning capabilities.

Concept of android

Android OS is a Linux-based mobile operating system that primarily runs on smartphones and tablets. The Android platform includes an operating system based upon the Linux kernel, a GUI, a web browser and end-user applications that can be downloaded.

Concept of Ice cream Sandwich

The default home screen of Ice Cream Sandwich displays a persistent Google Search bar across the top of the screen, a dock across the bottom containing the app drawer button in the middle, and four slots for app shortcuts alongside it. Folders of apps can be made by dragging an app and hovering it over another.

Concept of jellybeans

Android Jelly Bean (Android 4.1, 4.2, 4.3) is the codename given to the tenth version of the Android mobile operating system developed by Google, spanning three major point releases (versions 4.1 through 4.3).

Android Jelly Bean is a version of the Android operating system (OS) for mobile phones, tablet PCs and other supported handheld devices. Android Jelly Bean was released in June 2012 as a successor to Android Ice Cream Sandwich. Android Jelly Bean is also known as Android 4.1/4.2.

Concept of PhoneGap

PhoneGap is an open-source framework for quickly building cross-platform mobile apps using HTML5, Javascript, and CSS. Building applications for each device–iPhone, Android, Windows Mobile, and more requires different frameworks and languages.

Introduction of Internet and E-mail

Objectives: At the end of this exercise you shall be able to
- **define world wide web and website**
- **define web browsing and search engines**
- **concept of favorites folder**
- **define electronic mail and their applications.**

World Wide Web

The World Wide Web commonly referred to as WWW, W3, or the Web is a system of interconnected public webpages accessible through the Internet. The Web is not the same as the Internet, the Web is one of many applications built on top of the Internet.

Website: (A collection of similar web pages linked together via hyperlinks.)

A website is a collection of linked web pages (plus their associated resources) that share a unique domain name. Each web page of a given website provides explicit links most of the time in the form of clickable portions of text that allow the user to move from one page of the website to another.

Web Page: A text file produced in any markup language, such as HTML, is referred to as a web page. Hypertext, simple text, sound, photos, videos, and links to other pages are all included on the web page (hyperlinks).

URL: Each website's main page has its own unique address. Uniform Resource Locator is the name given to this one-of-a-kind address.

Web Browser

A software application used to access information on the World Wide Web is called a Web Browser. When a user requests some information, the web browser fetches the data from a web server and then displays the webpage on the user's screen. Web Browser is a common term which is frequently used by people while discussing the Internet. However, the exact definition of a web browser is known by few only. Browsers are computer programs that search for, access, and display various websites on the Internet. Mozilla Firefox, Chrome, and so forth.

Today web browsers are easily accessible and can be used on devices like computer, laptops, mobile phones, etc. but this evolution of making browsers available for easy use took many years.

The most recent major entrant to the browser market is Chrome, first released in September 2008. Chrome's take-up has increased significantly year by year, by doubling its usage share from 8% to 16% by August 2011. This increase seems largely to be at the expense of Internet Explorer, whose share has tended to decrease from month to month. In December 2011, Chrome overtook Internet Explorer 8 as the most widely used web browser but still had lower usage than all versions of Internet Explorer combined. Chrome's user-base continued to grow and in May 2012, Chrome's usage passed the usage of all versions of Internet Explorer combined. By April 2014, Chrome's usage had hit 45%. Internet Explorer was deprecated in Windows 10, with Microsoft Edge replacing it as the default web browser.

The primary purpose of a web browser is to bring information resources to the user ("retrieval" or "fetching"), allowing them to view the information ("display", "rendering"), and then access other information ("navigation", "following links"). This process begins when the user inputs a Uniform Resource Locator (URL), for example http://en.wikipedia.org/, into the browser. The prefix of the URL, the Uniform Resource Identifier or URI, determines how the URL will be interpreted. The most commonly used kind of URI starts with http: and identifies a resource to be retrieved over the Hypertext Transfer Protocol (HTTP). Many browsers also support a variety of other prefixes, such as https: for HTTPS, ftp: for the File Transfer Protocol, and file: for local files. Prefixes that the web browser cannot directly handle are often handed off to another application entirely. For example, mailto: URIs are usually passed to the user's default e-mail application, and news: URIs are passed to the user's default newsgroup reader.

In the case of http, https, file, and others, once the resource has been retrieved the web browser will display it. HTML and associated content (image files, formatting information such as CSS, etc.) is passed to the browser's layout engine to be transformed from markup to an interactive document, a process known as "rendering". Aside from HTML, web browsers can generally display any kind of content that can be part of a web page. Most browsers can display images, audio, video, and XML files, and often have plug-ins to support Flash applications and Java applets. Upon encountering a file of an unsupported type or a file that is set up to be downloaded rather than displayed, the browser prompts the user to save the file to disk.

Information resources may contain hyperlinks to other information resources. Each link contains the URI of a resource to go to. When a link is clicked, the browser navigates to the resource indicated by the link's target URI, and the process of bringing content to the user begins again.

Features

Available web browsers range in features from minimal, text-based user interfaces with bare-bones support for HTML to rich user interfaces supporting a wide variety of file formats and protocols. Browsers which include additional components to support e-mail, Usenet news, and Internet Relay Chat (IRC), are sometimes referred to as "Internet suites" rather than merely "web browsers".

All major web browsers allow the user to open multiple information resources at the same time, either in different browser windows or in different tabs of the same window. Major browsers also include pop-up blockers to prevent unwanted windows from "popping up" without the user's consent.

Privacy and security

Most browsers support HTTP Secure and offer quick and easy ways to delete the web cache, cookies, and browsing history.

Standards support

Early web browsers supported only a very simple version of HTML. The rapid development of proprietary web browsers led to the development of non-standard dialects of HTML, leading to problems with interoperability. Modern web browsers support a combination of standards-based and de facto HTML and XHTML, which should be rendered in the same way by all browsers.

Extensibility

A browser extension is a computer program that extends the functionality of a web browser. Every major web browser supports the development of browser extensions.

Types of Web Browsers

All web browsers are application programs that are developed to access information on World Wide Web. Although the primary application of all the web browsers is the same, they differ from each other in more than one aspect.

The distinguishing areas are:

- Platform: Linux, Windows, Mac, BSD and other Unix
- Protocols: FTP, SFTP, SAMBA, HTTP, IMAP, etc.
- Graphical User Interface (GUI)
- Layout Engine: Amaya, Gecko, Trident, KHTML, WebKit
- Mobile Compatibility
- HTML5 Support
- Open Source
- Proprietary

Internet Explorer (Fig 1)

It was developed by Microsoft in 1994 and released in 1995 as a supportive package to Microsoft Windows line of operating systems. According to statistics, its usage share from 1999 to 2003-04 was around 95%.

Fig 1

Features: There are regular Microsoft updates that IE supports. Favicon allows an image to be used as a bookmark. It supports Integrated Windows Authentication.

Mozilla Firefox (Fig 2)

Fig 2

It is owned by Mozilla Corporation and was the result of experimentation. 'Mozilla Firefox' was officially announced in February 2004. It was earlier named Phoenix, Firebird, and eventually Firefox. It is the second-most famous browser after Internet Explorer, as there were around 100 million downloads within a year of its release. Until November 2008, 700 million downloads were recorded.

Features: As it is open source software, it allows everyone to access the code. It supports tabbed browsing that allows the user to open multiple sites in a single window. Session storage is also an important feature of Firefox, which allows the user to regain access to the open tabs after he has closed the browser window.

Safari (Fig 3)

Fig 3

This is a web browser from Apple Inc., which is compatible with Mac OS X, Microsoft Windows, and the iPhone OS. Safari was released by Apple in January 2003 as a public beta. It will fill an online form with the personal information by using the Auto Fill feature with the help of information that is stored in the address book or Outlook.

Features: The Safari 4 beta had many features like VoiceOver screen reader, that reads aloud everything that is on the screen, including text and web links. It also has features like CSS Canvas, LiveConnect, XML 1.0, and JavaScript support, and Cover Flow. 'Grammar Checking' is an interesting built-in feature, which performs a grammar check on the typed text and gives suggestions to correct the sentence if wrong. Also, there is a resizable web search box option available.

Opera (Fig 4)

Fig 4

This browser was developed by Opera Software in 1996. It is a well-known browser that is mainly used in Internet-activated mobile phones, PDAs, and smartphones. Opera Mini and Opera Mobile are the browsers used in smartphones.

Features: It also has some common functions like zoom and fit-to-width, content blocking, tabs and sessions, download manager with BitTorrent, and mouse gestures.

Google Chrome (Fig 5)

Fig 5

This web browser was developed by Google. Its beta and commercial versions were released in September 2008 for Microsoft Windows. The browser versions for Mac OS X also developed on 20. The browser options are 5 x 6 x 7 x 8 x etc. very similar to that of Safari, the settings locations are similar to Internet Explorer 7, and the window design is based on Windows Vista.

Features: The main standout feature is the malware and phishing warning that the browser suggests when the user wants to browse a site. Also, there is a user tracking option available with Chrome.

Search Engines

A search engine is a software program that helps people find the information they are looking for online using keywords or phrases. Search engines are able to return results quickly—even with millions of websites online—by scanning the Internet continuously and indexing every page they find. (Fig 6)

Fig 6

As of January 2022, Google is by far the world's most used search engine, with a market share of 90.6%, and the world's other most used search engines were Bing, Yahoo!, Baidu, Yandex, and DuckDuckGo.

Now, YouTube is the world's second-largest search engine after Google.

A web search engine is a type of website that helps computer user find information on the Internet. It does this by looking through other web pages for the text the user wants to find. The software that does this is known as a search engine.

To use a search engine it is must enter at least one keyword in to the search box. Usually an on-screen button must be clicked on to submit the search. The search engine looks for matches between the keyword(s) entered and its database of websites and words.

Search engines are some of the most advanced websites on the web. They use special computer code to sort the web pages on SERPs. The most popular or highest quality web pages will be near the top or the list. When a user type words into the search engine, it looks for web pages with those words. There could be thousands, or even millions, of web pages with those words. Using more keywords or different keywords improves the results of searches.

Google, Yahoo!, Ask.com, Forestle and Bing are popular search-engine websites. Some older services include Webcrawler, Lycos, and Alta Vista. A search service may also include a portal with news, games, and more information besides a search engine.

A search engine operates in the following order:

1 Web crawling

2 Indexing

3 Searching

Web search engines work by storing information about many web pages, which they retrieve from the HTML markup of the pages. These pages are retrieved by a Web crawler (sometimes also known as a spider) - an automated Web crawler which follows every link on the site.

Most Web search engines are commercial ventures supported by advertising revenue and thus some of them allow advertisers to have their listings ranked higher in search results for a fee. Search engines that do not accept money for their search results make money by running search related ads alongside the regular search

engine results. The search engines make money every time someone clicks on one of these ads.

Search engine categories

Web search engines

Search engines that are expressly designed for searching web pages, documents, and images were developed to facilitate searching through a large, nebulous blob of unstructured resources. They are engineered to follow a multi-stage process: crawling the infinite stockpile of pages and documents to skim the figurative foam from their contents, indexing the foam/buzzwords in a sort of semi-structured form (database or something), and at last, resolving user entries/queries to return mostly relevant results and links to those skimmed documents or pages from the inventory.

Database search engines

Searching for text-based content in databases presents a few special challenges from which a number of specialized search engines flourish. Databases can be slow when solving complex queries (with multiple logical or string matching arguments). Databases allow pseudo-logical queries which full-text searches do not use. There is no crawling necessary for a database since the data is already structured. However, it is often necessary to index the data in a more economized form to allow a more expeditious search.

Mixed search engines

Sometimes, data searched contains both database content and web pages or documents. Search engine technology has developed to respond to both sets of requirements. Most mixed search engines are large Web search engines, like Google. They search both through structured and unstructured data sources. Take for example, the word 'ball.' In its simplest terms, it returns more than 40 variations on Wikipedia alone. Pages and documents are crawled and indexed in a separate index. Databases are indexed also from various sources. Search results are then generated for users by querying these multiple indices in parallel and compounding the results according to "rules."

Google Tips and Tricks Every Student Should Know

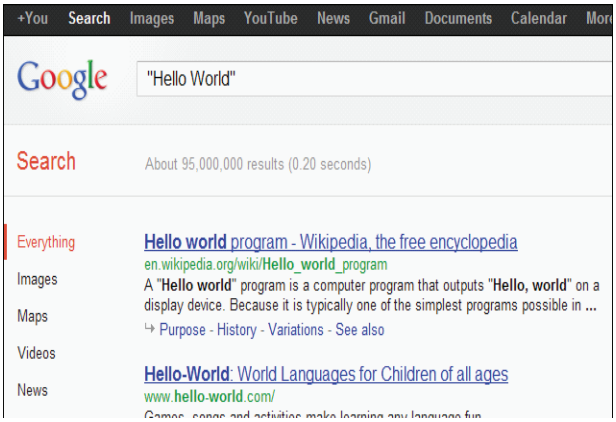
Google is a powerful tool, but it is missing out on a lot of that power if it is just type words into it. Master Google and find the best results faster with these search tricks. Many of Google's search operators aren't very well-known.

Exact words and phrases

One of the most basic and widely known search tricks is using quotation marks to search for an exact phrase. For example, perform the following search will only get pages that contain the word "Hello" followed by the word "World."(Fig 7)

"Hello World"

Fig 7

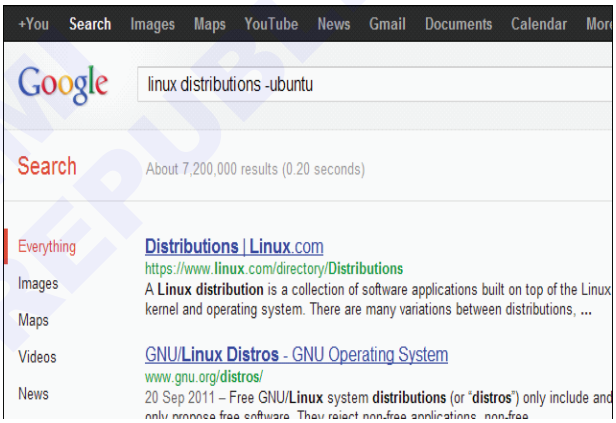


Excluding a Word

The minus sign allows to specify words that shouldn't appear in the results. For example, if it is looking for pages about Linux distributions that don't mention Ubuntu, use the following search:

linux distributions -ubuntu (Fig 8)

Fig 8

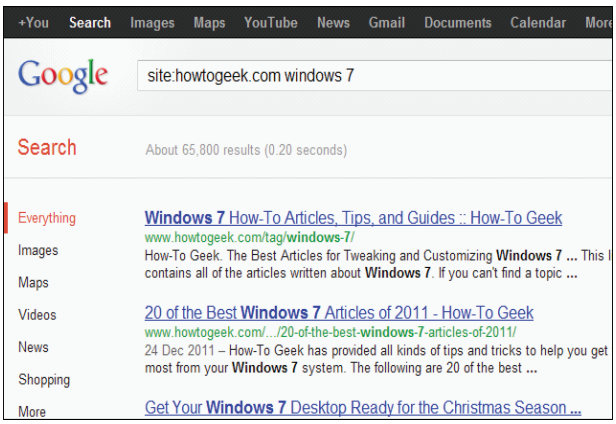


Site search

The site: operator allows performing a search in a specific site. For example looking for information on Windows 7 on How-To Geek. Use the following search (Fig 9)

site:howtogeek.com windows 7

Fig 9

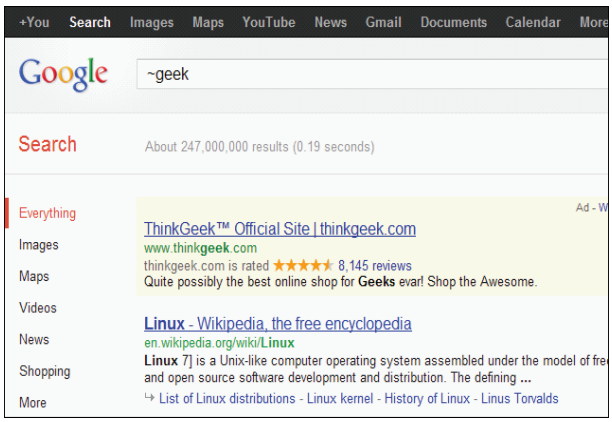


Use the site: operator to specify a domain. For example, looking for high-quality references use site:.edu to only pull up results from .edu domains.

Related Words

The tilde (~) operator is the opposite of enclosing a single word in quotes - it searches for related words, not just the word that typed. For example to search a word similar to “geek”: (Fig 10)

Fig 10



Apparently, “Linux” is the most similar word to geek, followed by “Greek.” “Nerd” comes in third.

The Wildcard

The asterisk (*) is a wildcard that can match any word. For example, to see what companies Google has purchased and how much they paid, use this search:

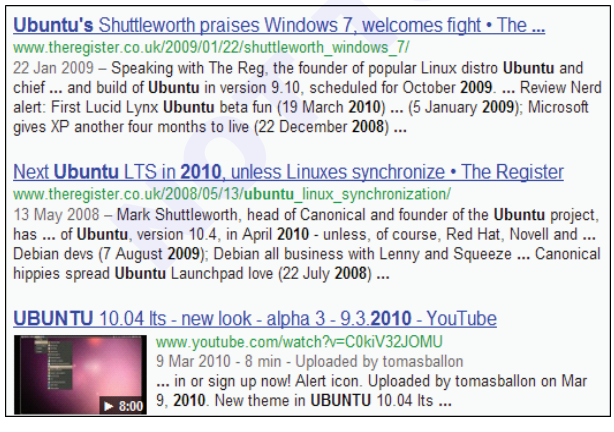
“google purchased * for * dollars”

Time Ranges

A little-known search operator allows to specify a specific time range. For example, use the following search to find results about Ubuntu from between 2008 and 2010: (Fig 11)

ubuntu 2008..2010

Fig 11

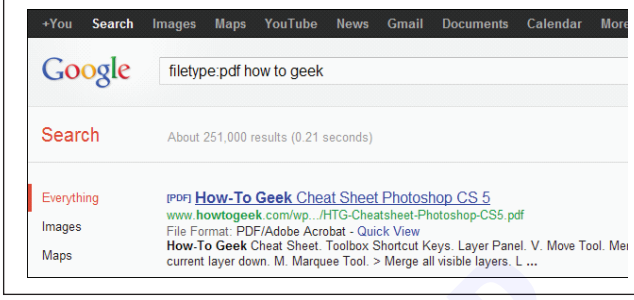


File type

The filetype: operator allows searching for files of a specific file type. For example, to search for only PDF files use the following search (Fig 12).

filetype:pdf how to geek

Fig 12

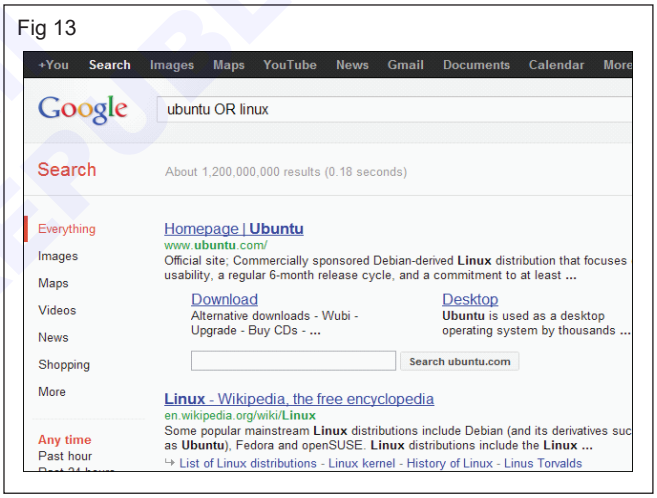


One word or the other

The “OR” operator allows to find words that contain one term or another. For example, using the following search will pull up results that contain either the word “Ubuntu” or the word “Linux.” The word “OR” must be in uppercase (Fig 13).

ubuntu OR linux

Fig 13

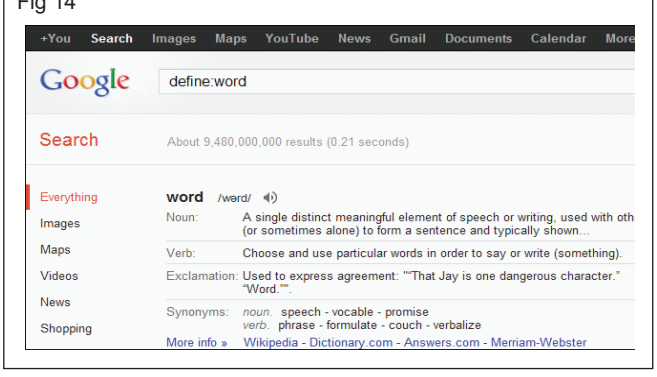


Word definitions

Want to see a word and its definition. Use the following search trick (Fig 14)

define:word

Fig 14

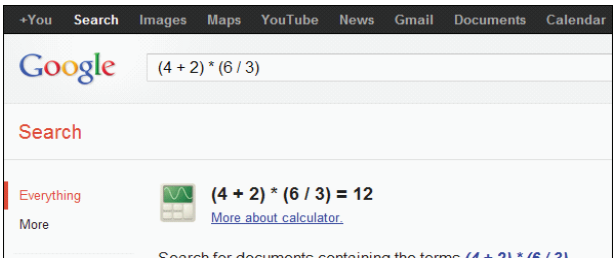


Calculator

Use Google instead of pulling one out or launching a calculator app. Use the +, -, * and / symbols to specify arithmetic operations. Use brackets for more complicated expressions. Here's an example (Fig 15)

(4 + 2) * (6 / 3)

Fig 15

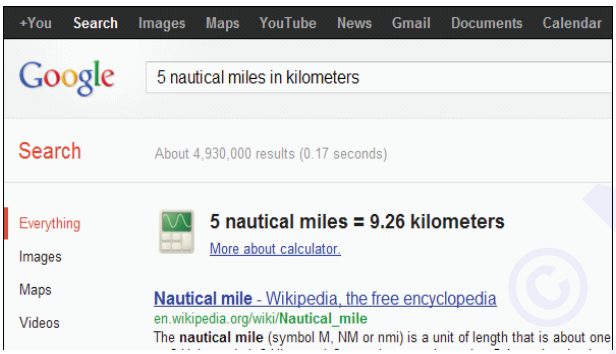


Unit conversions

The calculator can also convert between units. Just type "X [units] in [units]". Here's an example (Fig 16):

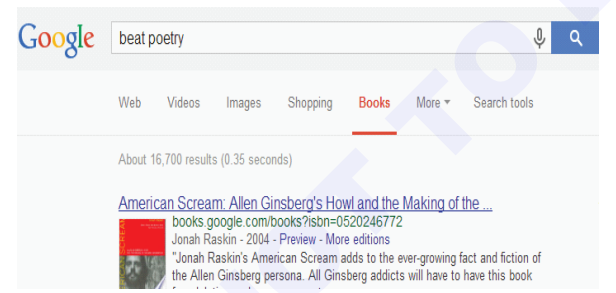
5 nautical miles in kilometers

Fig 16



Search Google books and use Google scholar (Fig 17)

Fig 17



Head to books.google.com to start researching the topic or use Google's advanced book search for options like book language, author, publication dates, and more. In the search results, click on "Search tools" to filter books by ones that are available with a preview, select books or magazines, and filter or sort by date. Public domain books can be downloaded as PDF, and out of copyright or books with author/publisher permission are fully viewable. Search within books too, and have the search phrase highlighted, as well as add books to the library for future reference. Additionally, when the search on a title, Google's book overview page will list popular passages, a word cloud, bibliographic information, and other reference information.

Favorites folder

At the top of the message list, the title of the folder you're viewing appears along with a star. If only the outline of the star appears it means the folder isn't in your Favorites list. Select the star to fill it in and the folder will be added to your Favorites.

What is the importance of creating a favorites folder?

Bookmarks and favorites are important features in web browsing because they allow users to easily save and access their most frequently visited websites.

To add a favourite to the personal Favourites in Internet Explorer:

1 Visit the web site whilst connected to the Internet.

2 Select the Favourites pull down menu or press the Favourites button.

3 Choose Add To Favourites.

4 A dialog box appears asking to choose which Favourites folder to add the URL to (or to create a new folder).

5 Select the appropriate folder and press OK.

6 The URL that is in Address Panel is added to the Favourites.

To return to a previously-bookmarked favourite:

1 Select Favourites from the pull down menu or press the Favourites button.

2 Navigate to the particular web site title that wish to visit.

3 Click on the Web site title.

4 IE now attempts to retrieve that web site.

Saving bookmarks or favorites in Google Chrome

On the right side of the address bar, click the star icon.

It could look like this or .

Otherwise do one of the following:

1 Go to the Chrome menu > Bookmarks > Bookmark this page.

2 Go to the web address bar at the top of the page and find the lock or the page . Drag either one into the bookmarks bar.

3 Press Ctrl+D or ⌘+D.

Show or hide the bookmarks bar

To turn the bookmarks bar on or off, follow these steps:

1 In the top-right corner of the browser window, click the Chrome menu .

2 Select Bookmarks > Show Bookmarks Bar.

Also use the keyboard shortcuts Ctrl+Shift+B (Windows and Chrome OS) and ⌘-Shift -B (Mac).

Favorite Folder Locations

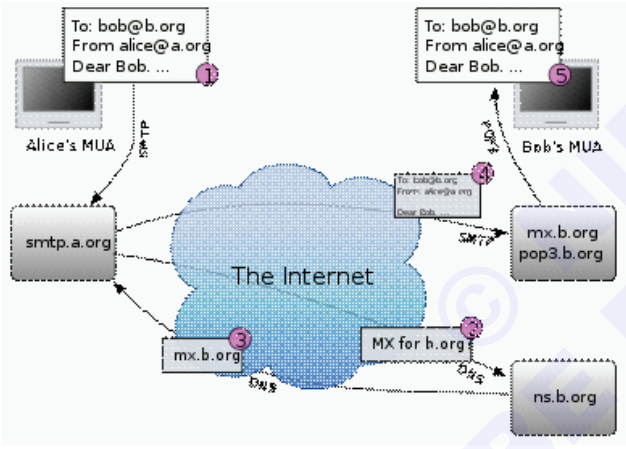
The full path to the Favorites folder in later versions of Windows is "C:\Users(username)\Favorites\".

Electronic mail

An Internet email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

Email is an information and communications technology. It uses technology to communicate a digital message over the Internet. Users use email differently, based on how they think about it. There are many software platforms available to send and receive. Popular email platforms include Gmail, Hotmail, Yahoo! Mail, Outlook, and many others. (Fig 18)

Fig 18



Network-based email was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is now carried by the Simple Mail Transfer Protocol (SMTP). In the process of transporting email messages between systems, SMTP communicates delivery parameters using a message envelope separate from the message (header and body) itself.

The diagram in the below shows a typical sequence of events that takes place when sender Alice transmits a message using a mail user agent (MUA) addressed to the email address of the recipient.

1 The MUA formats the message in email format and uses the submission protocol, a profile of the Simple Mail Transfer Protocol (SMTP), to send the message to the local mail submission agent (MSA), in this casesmtp.a.org.

2 The MSA determines the destination address provided in the SMTP protocol (not from the message header), in this case bob@b.org. The part before the @ sign is the local part of the address, often the username of the recipient, and the part after the @ sign is a domain name. The MSA resolves a domain name to determine the fully qualified domain name of the mail server in the Domain Name System (DNS).

3 The DNS server for the domain b.org (ns.b.org) responds with any MX records listing the mail exchange servers for that domain, in this case mx.b.org, a message transfer agent (MTA) server run by the recipient's ISP.

4 smtp.a.org sends the message to mx.b.org using SMTP. This server may need to forward the message to other MTAs before the message reaches the final message delivery agent (MDA).

5 The MDA delivers it to the mailbox of user bob.

6 Bob's MUA picks up the message using either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP).

Using e-mail is rather straightforward. Once an account created, just select the option that says something like "new e-mail message" or "create a new message". That probably prompted with three boxes (called fields):

- **To:**
- **Subject:**
- **Body:** (sometimes the body doesn't actually say body, it's just the big area where to type the actual message.)

In the To: field type the complete e-mail address of the person who will receive the e-mail, type anything in the subject and body, although the length of the subject is limited. Usually the subject to just a few words describing the content of the body of the e-mail message. There are options for attachments and forwards, add files by using the attachment option, forward (make a copy) of a message that is received from someone and mail it to someone else with the forward option.

There are fields for CC: and BCC: close to the To: field. CC stands for carbon copy. To send a message to multiple people, add the extra people in the CC: field (usually separate the e-mail addresses by commas). BCC stands for blind carbon copy. BCC works just like a carbon copy, except the e-mail addresses typed in the BCC do not show up to the other recipients.

Email address

An email address such as John.Smith@example.com is made up of a local part, an @ symbol, then a case-insensitive domain part. Although the standard specifies the local part to be case-sensitive, in practice the mail system at example.com may treat John. Smith as equivalent to john.smith and mail systems often limit their users' choice of name to a subset of the technically valid characters. In some cases they also limit which addresses it is possible to send mail to.

The general format of an email address is localpart@domain, and a specific example is jsmith@example.org. An address consists of two parts. The part before the @ sign (localpart) identifies the name of a mailbox. This is

often the username of the recipient, e.g., jsmith. The part after the @ symbol is a domain name that represents the administrative realm for the mail box, e.g., a company's domain name, example.com.

An email message also contains a message envelope that contains the information for mail routing. To indicate the message recipient, an email address also may have an associated display name for the recipient, which is followed by the address specification surrounded by angled brackets, for example: John Smith <john.smith@example.org>.

Addressing an Email

When sending an email, it have three field choices: "to", "cc", and "bcc". Here is how to use each field:

- **To:** enter the email addresses of the people the email is targeted to
- **Cc:** enter the email addresses of the people you want to know about the email (remember that everyone will see their names)
- **Bcc:** enter the email addresses of the people you want to know about the email but not announce to everyone else that they are getting a copy

Carbon copying someone on an email is a great way to keep them in "the loop" and allows them to know what is going on without actually being involved. It can be a useful way to remind people of what happened at a meeting or to remind them to take an action on something. Carbon copying also makes the recipient aware of who else is looking at the email. This is often used in business settings to get the primary recipient (the "to" field) of the email to take the message more seriously or to let them know that it is important.

Blind carbon copying someone to an email is common to keep the recipients' privacy. One example is to use Bcc when emailing a long list of people who do not know each other like in a mailing list. Another reason to blind carbon copy someone is to keep them in the loop of a conversation without letting the other recipients (the "to" and "cc" fields) know. In business, this can be used to tattle on someone by blind carbon copying the superiors on an email thread. Blind carbon copying also prevents the "reply all" function.

While filling out an email with the following information:

- **From:** You
- **To :** John Smith
- **Cc :** Kerry Thomas, Lindy Davis
- **Bcc :** Mark Villis, Spike Moor

All of the recipients (including Mark Villis and Spike Moor) will see the following email header in their email message:

From : You

To : John Smith

Cc : Kerry Thomas, Lindy Davis

Notice that none of the recipients will know who the bcc recipients are. Both of the bcc-ed recipients will realize they were bcc-ed but neither Mark nor Spike will know who else was bcc-ed with them.

Message folders

Message folders are used to organize the email messages. That are containing inbox, outbox, sent-mail, trash, drafts and templates folders etc. These folders each have special functions:

Inbox: Where by default the new messages are seeing when checking the mail.

Outbox: Where messages are put while they are waiting to be delivered. That is outbox is what is being sent (normally if the sending fails for a reason it gets saved here and will continue to try and send it again). It is not possible to drag and drop messages here to send them.

Sent-mail: By default copies of all messages that have sent are put into this folder.

Trash: By default all messages that have deleted are moved into this folder.

Drafts: Contains messages that are started to edit but then saved to this folder through Message -> Save as Draft.

Spam: Contains junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. The messages may contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments.

Address book: An address book or a name and address book (NAB) is a book or a database used for storing entries called contacts. Each contact entry usually consists of a few standard fields (for example: first name, last name, company name, address, telephone number, e-mail address, fax number, mobile phone number).

Email client's "address book" enables addition of email addresses to the contact list quickly and without error. Address book should store all of the frequently used email addresses, enabling to select from a list instead of having to re-type the addresses each time to send an email. This is the fastest way to address a message, and more importantly ensures that will never make a typing mistake and send the email to the wrong address.

The program recreated all of the interoffice mailing system's functionalities, including the inbox, outbox, folders, memos, attachments, address book, and more.

E mail Addressing

Some of the most popular and commonly used formats of email addresses are as follows:

- Firstname.secondname@domain.com.

Example: peter.parker@gmail.com

Subject:

Type anything in the subject and body, although the length of the subject is limited. Usually the subject to just a few words describing the content of the body of the email message.

Inbox

Inbox is an area where you can see all the received mails.

Outbox

Outbox is an area where the outgoing messages or messages which are in process of sending or which are failed to send are stored. Sent mail − Sent mail is an area to view all the sent or successfully delivered mails.

Favorite's folders

In the context of the World Wide Web, a bookmark is a Uniform Resource Identifier (URI) that is stored for later retrieval in any of various storage formats. All modern web browsers include bookmark features. Bookmarks are called favorites or Internet shortcuts in Internet Explorer, and by virtue of that browser's large market share, these terms have been synonymous with bookmark since the first browser war. Bookmarks are normally accessed through a menu in the user's web browser, and folders are commonly used for organization. In addition to bookmarking methods within most browsers, many external applications offer bookmark management.

Use of bookmarks or favourites

There are over a billion web sites on the web and many of these have long and complicated URL's. Surfers need a way to remember where their preferred web sites can be found on the web.

Internet Explorer's Favourites and Netscape's equivalent Bookmarks are facilities that enable the users to store the URL's of web sites. This can organize the favorite URL's into folders of related links - for instance in the Favorites may have a Sports folder containing the URL's of the best sport web sites that a user have found.

When a user add a Favourite or Bookmark it is stored with the title of the web page (the title of the web page appears in the blue top border of the browser window). User can change the title that is stored in the Favourites by right clicking the Favourite, and selecting Rename, then overtyping the original title. This will not affect the title on the actual web page. To return to a previously bookmarked web site is a simple matter of selecting Favourites (or Bookmarks) and clicking the link to the site want to visit.

Internet Explorer favourites

There are two main ways to accessing the Favourites in IE - using the Favourites pull down menu, or using the Favourites button. The Favourites button toggles on and off. When it is on, it permanently displays the Favourites list alongside the left of the browser window, as well as providing options to add to, and organise the Favourites list.

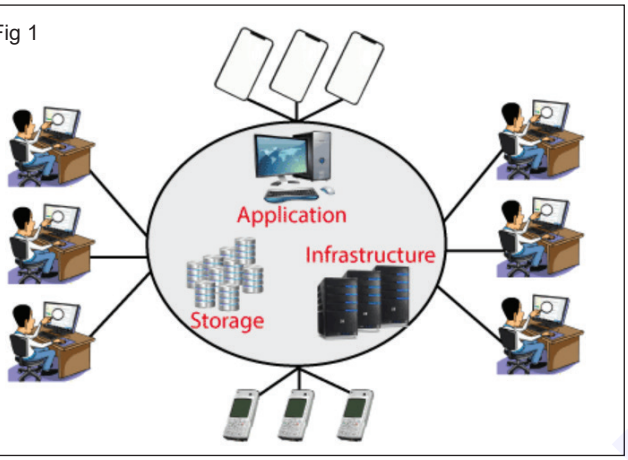
Cloud Computing & Cyber Security

Objectives: At the end of this exercise you shall be able to
- **concept of Cloud computing and their service providers**
- **concept of Cyber security, Cyber laws and IT Act and importance of privacy and techniques.**

Introduction to Cloud Computing

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet). (Fig 1)

Fig 1



Cloud Computing provides an alternative to the on-premises datacentre. With an on-premises datacentre, we have to manage everything, such as purchasing and installing hardware, virtualization, installing the operating system, and any other required applications, setting up the network, configuring the firewall, and setting up storage for data. After doing all the set-up, we become responsible for maintaining it through its entire lifecycle.

The cloud environment provides an easily accessible online portal that makes handy for the user to manage the compute, storage, network, and application resources. Some cloud service providers are in the following figure. (Fig 2 & 3)

Fig 2

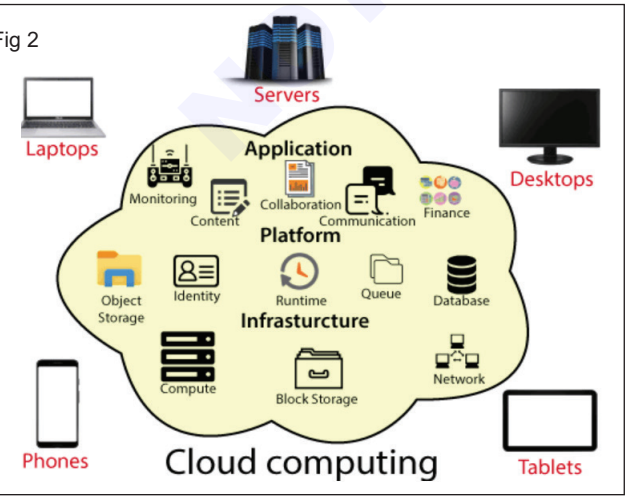


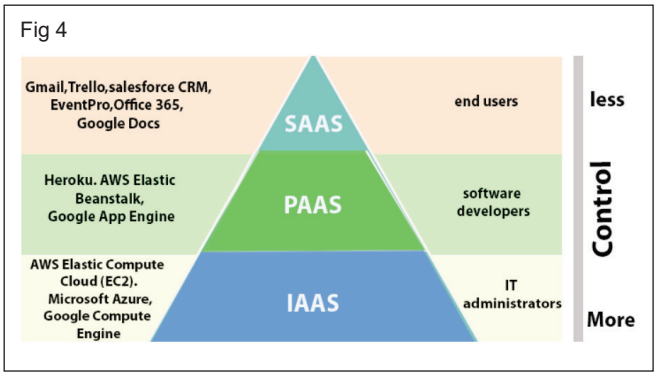
Fig 3

Advantages of cloud computing

- **Cost**: It reduces the huge capital costs of buying hardware and software.
- **Speed**: Resources can be accessed in minutes, typically within a few clicks.
- **Scalability**: We can increase or decrease the requirement of resources according to the business requirements.
- **Productivity**: While using cloud computing, we put less operational effort. We do not need to apply patching, as well as no need to maintain hardware and software. So, in this way, the IT team can be more productive and focus on achieving business goals.
- **Reliability**: Backup and recovery of data are less expensive and very fast for business continuity.
- **Security**: Many cloud vendors offer a broad set of policies, technologies, and controls that strengthen our data security.

Types of Cloud Computing services: (Fig 4)

Fig 4



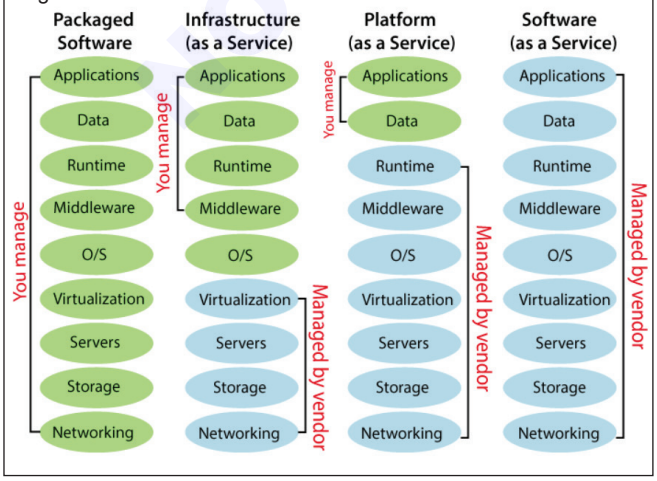
- **Public Cloud:** The cloud resources that are owned and operated by a third-party cloud service provider are termed as public clouds. It delivers computing resources such as servers, software, and storage over the internet.
- **Private Cloud**: The cloud computing resources that are exclusively used inside a single business or organization are termed as a private cloud. A private cloud may physically be located on the company's on-site datacentre or hosted by a third-party service provider.
- **Hybrid Cloud**: It is the combination of public and private clouds, which is bounded together by technology that allows data applications to be shared between them. Hybrid cloud provides flexibility and more deployment options to the business.

1 **Infrastructure as a Service (IaaS)**: In IaaS, we can rent IT infrastructures like servers and virtual machines (VMs), storage, networks, operating systems from a cloud service vendor. We can create VM running Windows or Linux and install anything we want on it. Using IaaS, we don't need to care about the hardware or virtualization software, but other than that, we do have to manage everything else. Using IaaS, we get maximum flexibility, but still, we need to put more effort into maintenance.

2 **Platform as a Service (PaaS)**: This service provides an on-demand environment for developing, testing, delivering, and managing software applications. The developer is responsible for the application, and the PaaS vendor provides the ability to deploy and run it. Using PaaS, the flexibility gets reduce, but the management of the environment is taken care of by the cloud vendors.

3 **Software as a Service (SaaS)**: It provides a centrally hosted and managed software services to the end-users. It delivers software over the internet, on-demand, and typically on a subscription basis. E.g., Microsoft One Drive, Dropbox, WordPress, Office 365, and Amazon Kindle. SaaS is used to minimize the operational cost to the maximum extent. Fig 5 shown as difference between the cloud services.

Fig 5



Create an account in Google cloud:

1 In the Google Cloud console, go to the Create service account page.

Go to Create service account

The remaining steps will appear automatically in the Google Cloud console.

2 Select a Google Cloud project.

3 Enter a service account name to display in the Google Cloud console.

The Google Cloud console generates a service account ID based on this name. Edit the ID if necessary. You cannot change the ID later.

4 Optional: Enter a description of the service account.

5 If you don't want to set access controls now, click Done to finish creating the service account. To set access controls now, click Create and continue and continue to the next step.

6 Optional: Choose one or more IAM roles to grant to the service account on the project.

7 When you are done adding roles, click Continue.

8 Optional: In the Service account users role field, add members that can impersonate the service account.

9 Optional: In the Service account admins role field, add members that can manage the service account.

10 Click Done to finish creating the service account.

After you create a service account, grant one or more roles to the service account so that it can act on your behalf.

Also, if the service account needs to access resources in other projects, you usually must enable the APIs for those resources in the project where you created the service account.

Introduction to Cyber Security

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Some other definitions of cybersecurity are

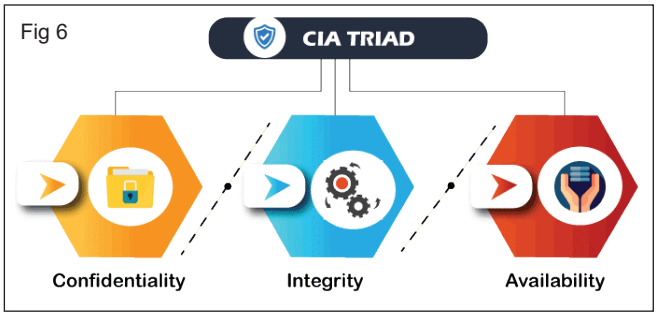
"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

Cyber Security Goals

Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated. (Fig 6)

Fig 6



We can break the CIA model into three parts: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.

Others

Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party, and either hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

Distributed cloud

A cloud computing platform can be assembled from a distributed set of machines in different locations, connected to a single network or hub service. It is possible to distinguish between two types of distributed clouds: public- resource computing and volunteer cloud.

Public-resource computing

This type of distributed cloud results from an expansive definition of cloud computing, because they are more similar to distributed computing than cloud computing. Nonetheless, it is considered a sub-class of cloud computing, and some examples include distributed computing platforms such as BOINC and Folding@ Home.

Volunteer cloud

Volunteer cloud computing is characterized as the intersection of public-resource computing and cloud computing, where a cloud computing infrastructure is built using volunteered resources. Many challenges arise from this type of infrastructure, because of the volatility of the resources used to built it and the dynamic environment it operates in. It can also be called peer-to-peer clouds, or ad-hoc clouds. An interesting effort in such direction is Cloud@Home, it aims to implement a cloud computing infrastructure using volunteered resources providing a business-model to incentivize contributions through financial restitution.

Intercloud

The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based. The focus is on direct interoperability between public cloud service providers, more so than between providers and consumers (as is the case for hybrid- and multi-cloud).

Multicloud

Multicloud is the use of multiple cloud computing services in a single heterogeneous architecture to reduce reliance on single vendors, increase flexibility through choice, mitigate against disasters, etc. It differs from hybrid cloud in that it refers to multiple cloud services, rather than multiple deployment modes (public, private, legacy).

Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

Cloud engineering

Cloud engineering is the application of engineering disciplines to cloud computing. It brings a systematic approach to the high-level concerns of commercialization, standardization, and governance in conceiving, developing, operating and maintaining cloud computing systems. It is a multidisciplinary method encompassing contributions from diverse areas such as systems, software, web, performance, information, security, platform, risk, and quality engineering.

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

- **Network Security**: It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security**: It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage,

writing source code, validation, threat modeling, etc., before a program or device is deployed.

- **Information or Data Security**: It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management**: It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security**: It involves processing and making decisions on handling and securing data assets.
- **Mobile Security**: It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security**: It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning**: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education**: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

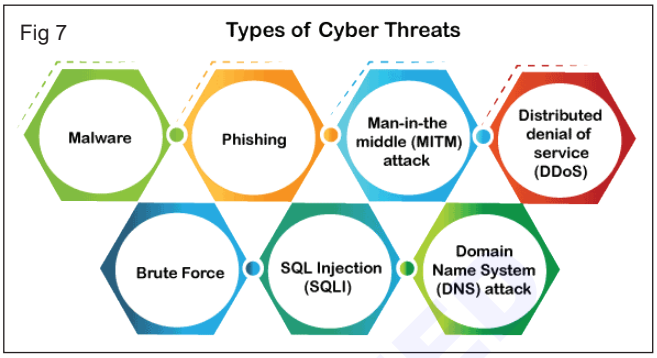
Importance of Cyber Security

Today we live in a digital era where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical infrastructure such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use devices connected to the Internet as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access or exposure that could have negative consequences. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vandalism.

Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, it is essential to have an excellent cybersecurity strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive business and personal information.

Types of Cyber Security Threats (Fig 7)

Fig 7



A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general. The cyber community defines the following threats available today:

Malware

Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The following are the important types of malware created by the hacker:

- **Virus**: It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.
- **Spyware**: It is a software that secretly records information about user activities on their system. For example, spyware could capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.
- **Trojans**: It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.
- **Ransomware**: It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.
- **Worms**: It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.
- **Adware**: It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this

program is to generate revenue for its developer by showing the ads on their browser.

- **Botnets**: It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Domain Name System (DNS) attack

A DNS attack is a type of cyberattack in which cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It is a severe cybersecurity risk because the DNS system is an essential element of the internet infrastructure.

Cyber Law

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

Importance of Cyber Law

1 It covers all transactions over the internet.

2 It keeps eye on all activities over the internet.

3 It touches every action and every reaction in cyberspace.

Introduction to IT act

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce. The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime. The original Act contained 94 sections, divided into 13 chapters and 4 schedules.

- Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.
- The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.
- It also gives legal recognition to digital signatures.
- The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies.

The main provision of IT Act 2000

The original act addressed electronic documents, e-signatures, and authentication of those records. It also enacted penalties for security breach offenses including damaging computer systems or committing cyber terrorism.

Importance of IT law in India

Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online.

Features of IT Act 2000

- All electronic contracts created through secure electronic channels were legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records and conjointly digital signatures are in place

Introduction of Computer Networks

Objectives: At the end of this lesson you shall be able to

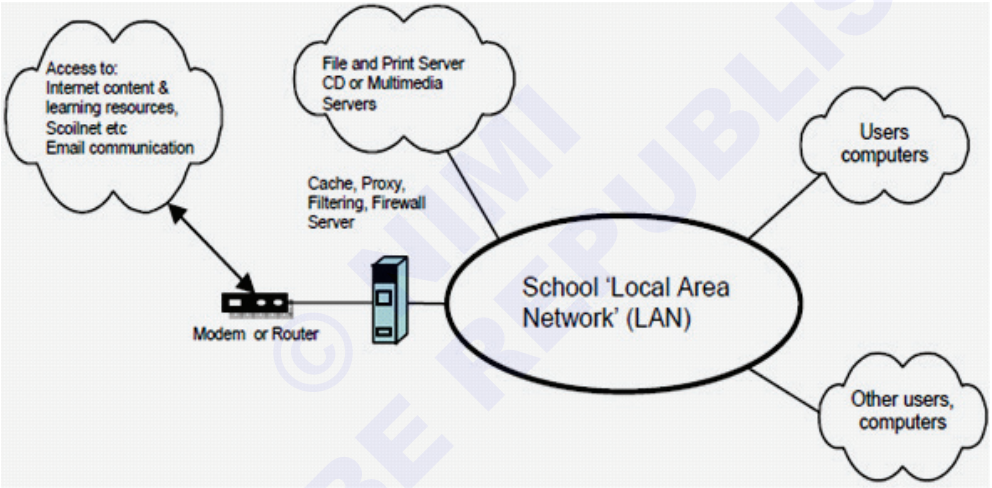
- **define Computer networks and their application and types**
- **list out the types of Topologies**
- **define Internet, Ethernet, WI-FI, Bluetooth, Mobile Networking and Wired & Wireless Networking**
- **explain Peer to Peer and Client server network**
- **list out the difference between Internet and Intranet.**

Introduction to computer network

Computer networking refers to the study and analysis of the communication process among various computing devices or computer systems that are linked or networked together to exchange information and sharing resources. Let us see the various concept of computer network.

Today computer networks are everywhere. You will find them in homes, offices, factories, hospital, leisure centers etc. A network is any interconnected group of people or things capable of sharing meaningful information with one another. All data networks consist of nodes, which refers to any computer or digital device using the network and links, the physical connections (either wired or wireless) that carry messages between nodes. (Fig 1)

Fig 1



Advantage of networking

- File sharing
- Hardware sharing
- Application sharing
- Internet access
- Centralized software management
- Data security and Management
- Saving Disk space
- Performance Enhancement
- Entertainment
- Remote Access

Network technologies

Computer networks can be logically classified into:

1 Peer to Peer networks

2 Client server networks

Peer to peer networks

A peer-to-peer network is a technology that allows you to connect two or more computers to one system. This connection allows you to easily share data without having to use a separate server for your file-sharing. Each end-computer that connects to this networks become a 'peer' and is allowed to receive or send files to other computers in its network. This enable you to work collaboratively to perform certain tasks that need group attention, and it is also allows you to provide services to another peer.

Client server networks

A client server computer network model is made-up of client computers and server computers. Now we need to understand the terms "client computer" and "server computer". (Fig 2)

Client computer

A computer which is seeking any resource from another computer, is a client computer. For example: Downloading a file from a File Server, Browsing Internet etc. (Fig 3)

Fig 2

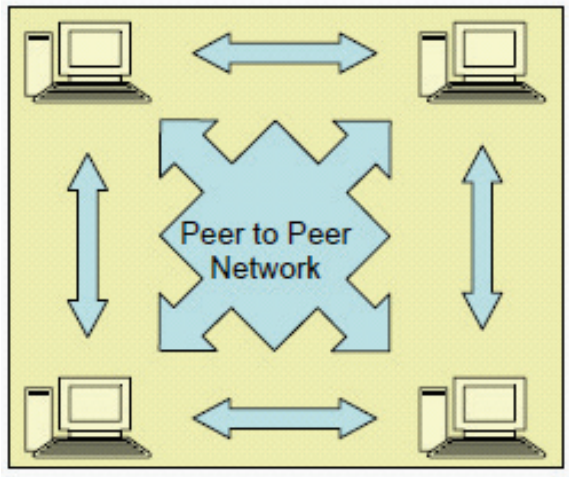
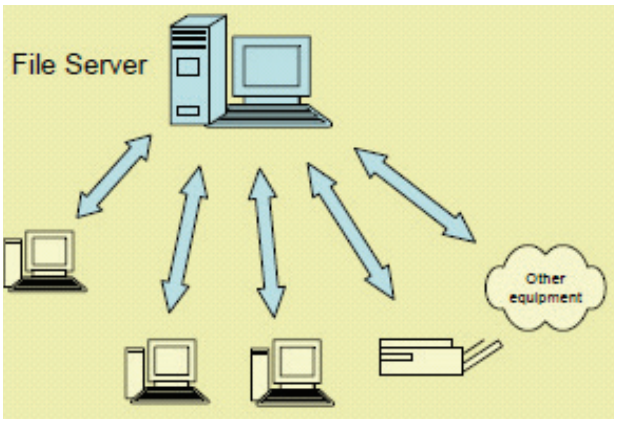


Fig 3



Sever computer

If a computer has a resource which is served to another computer, it is a server computer. A server computer is installed with appropriate Operating system and related software to serve the network clients with one or more services.

In a client server network, high-end servers, installed with the Network Operating System (Server Operating System) and the related software, serve the clients continuously on a network, by providing them with specific services upon request. The Client – Server network model is widely used network model.

Table 1

Comparison between peer-to-peer and client/server networks Peer-to-Peer networks vs Client/Server networks

Peer-to-Peer Networks	Client/Server Networks
Easy to set up.	More difficult to set up.
Less expensive to install.	More expensive to install.
Can be implemented on a wide range of operating systems.	A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking.
More time consuming to maintain the software being used (as computers must be managed individually.	Less time consuming to maintain the software being used (as most of the maintenance is managed from the server).
Very low levels of security supported or none at all. These can be very cumbersome to setup, depending on operating system being used.	High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings.
Ideal for networks with less than 10 computers.	No limit to the number of computers that can be supported by the network.
Does not require a server.	Requires a server running a server operating system.
Demands a moderate level of skill to administer the network.	Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system.

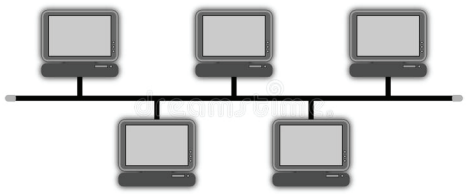
Network topologies

The way in which you connect a computer into a network is known as topology. There are five topologies. They are

1 Bus
2 Ring
3 Star
4 Tree
5 Hybrid
6 Mesh

Bus Topology (Fig 4)

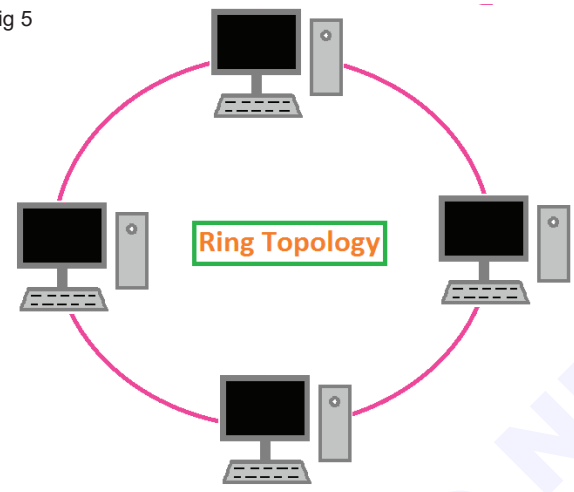
Fig 4



Bus topology is a network type in which every computer and device is connected to a single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in the bus topology.

Ring topology (Fig 5)

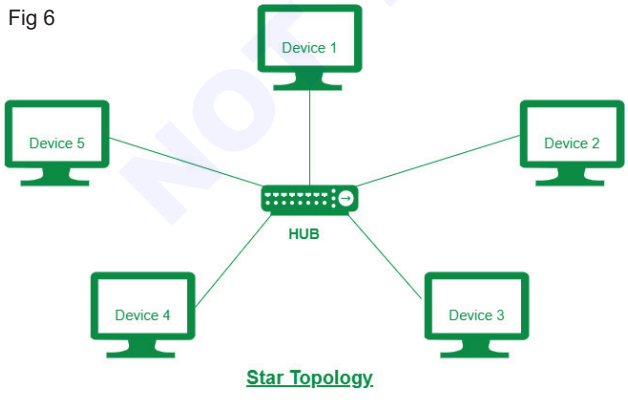
Fig 5



A network topology in which every node has exactly two branches connected to it. It features a logically closed loop. Data packets travel in a single direction around the ring from one network device to the next. All messages travel through a ring in the same direction (effectively either clock wise or counter clock wise). A failure in any cable or device breaks the loop and can take down the entire network.

Star topology (Fig 6)

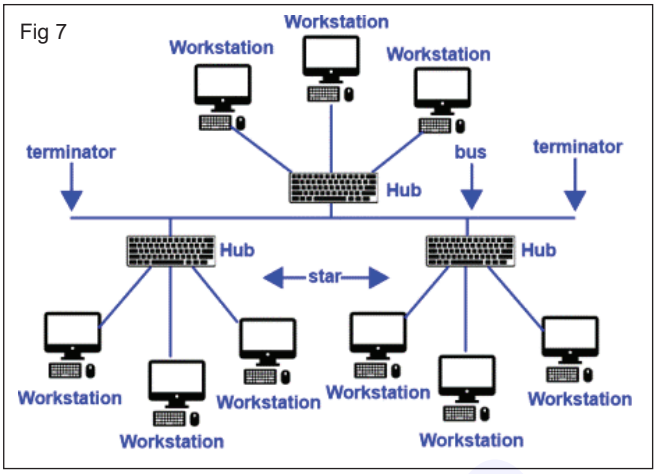
Fig 6



In a star topology each node has a dedicated set of wires connecting it to a central network hub. Since all traffic passes through the hub, the hub becomes a central point for isolating network problems and gathering network statistics.

Tree topology (Fig 7)

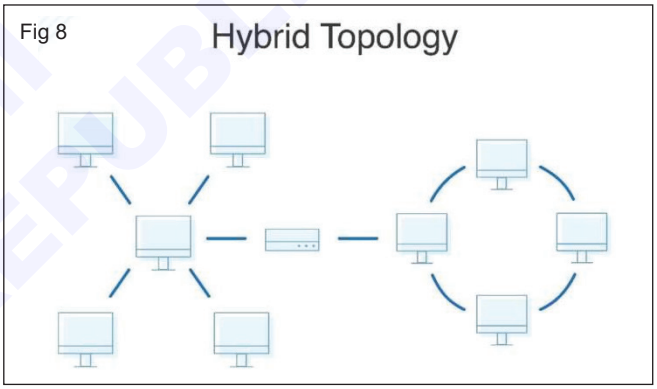
Fig 7



In computer networking, tree topology is a type of network topology that resembles a tree. In a tree topology, there is one central node (the “trunk”), and each node is connected to the central node through a single path. Nodes can be thought of as branches coming off of the trunk.

Hybrid topology (Fig 8)

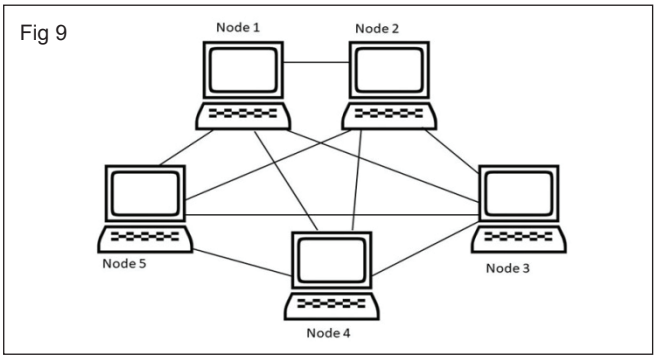
Fig 8



A combination of two or more topology is known as hybrid topology. For example, a combination of star and mesh topology is known as hybrid topology.

Mesh topology (Fig 9)

Fig 9



A network topology in which there are at least two nodes with two or more paths between them. Messages sent on a network can take any of several possible paths from source to destination. Same WAN like the internet employ Mesh routing.

Types of networking

There are mainly three types of computer networks based on their size:

1 Local Area Network (LAN)

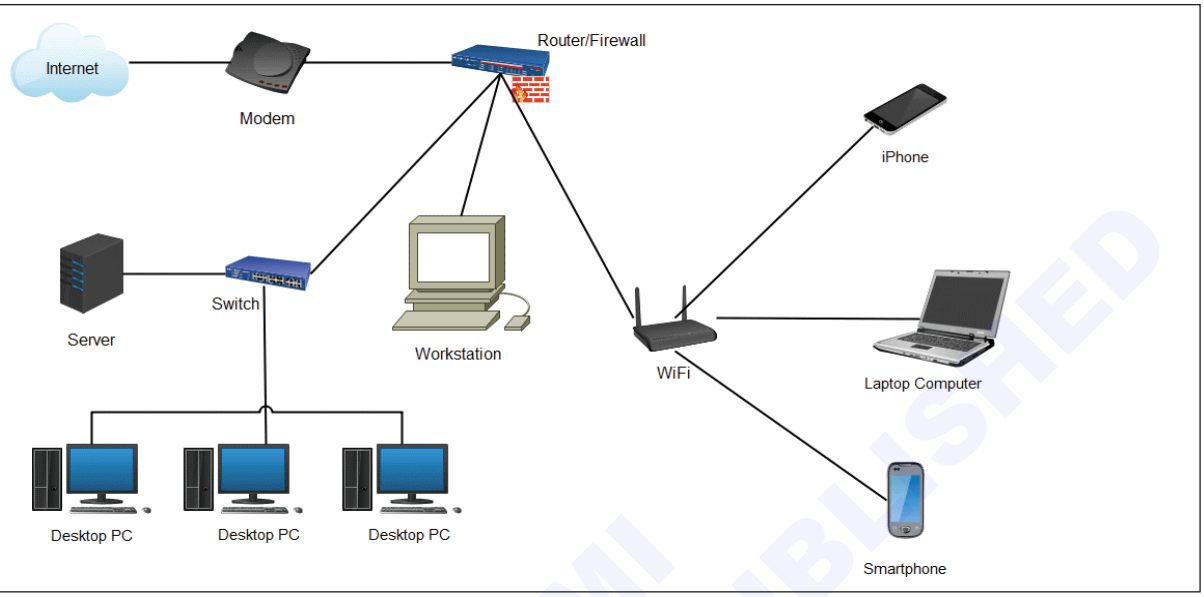
2 Metropolitan Area Network (MAN)

3 Wide Area Network (WAN)

Local area network (LAN)

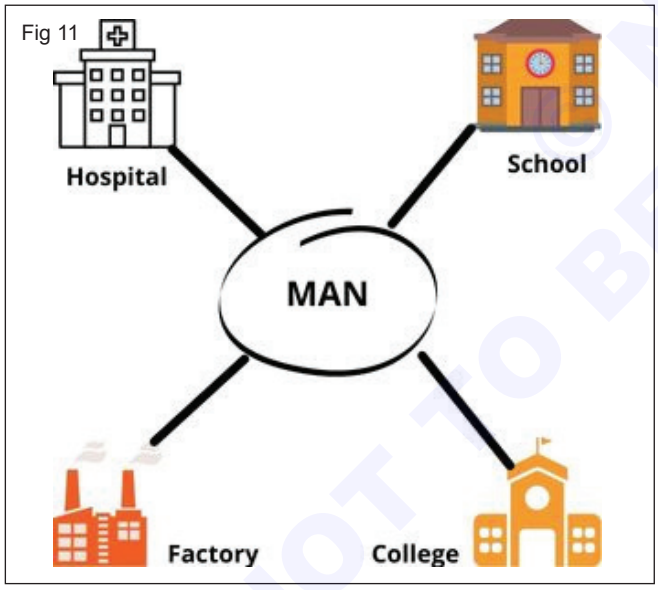
Local Area Network is a group of computers connected with each other in a small place such as School, Hospital, Apartment etc. LAN due to their small size considered faster, their speed can range anywhere from 100 to 1000 Mbps. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection. (Fig 10)

Fig 10



Metropolitan area network (MAN) (Fig 11)

Fig 11

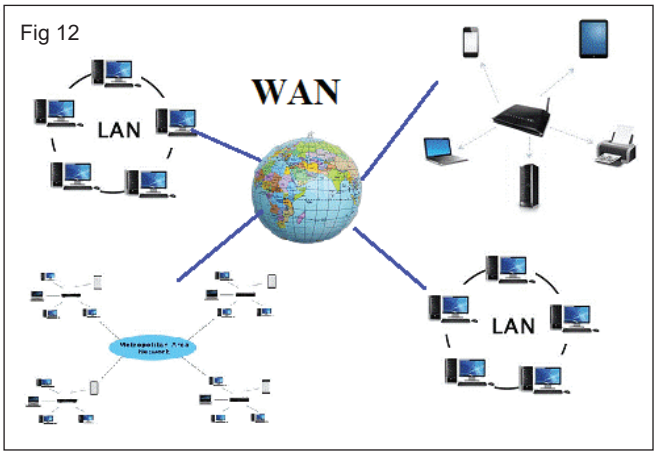


MAN network covers larger area by connecting LANs to a larger network of computers with each other through telephone lines. The size of the Metropolitan Area Network is larger than LANs and smaller the WANs, a MAN covers the larger area of a city or town. MAN speed ranges up to 100 Mbps.

Wide area network (WAN) (Fig 12)

Wide Area Network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover a country, continent or even a whole world. Internet connection is an example of WAN. The speed of WAN can range anywhere from 10 to 20 Mbps.

Fig 12



Comparison between LAN, MAN and WAN

LAN	MAN	WAN
LAN is referred to as local area networks	MAN is referred to as metropolitan area networks	WAN is referred to as wide area networks.
Ownership of LAN is private	Ownership of MAN can be public or private	Ownership of WAN might not be owned by one organization
LAN s transmit data at high Speeds.	The speeds of transmissions of MAN is average.	WAN s transmit data at low speeds.
LAN propagation delays are Short.	MAN propagation delays are moderate.	WAN propagation delays are quite long.
LAN s tend to be less congested	MANs tend to be more congested	WAN is more congested than MAN.
LAN s maintenance and design are easy.	MAN s maintenance and design are more difficult than LAN.	WAN ' s maintenance and design are also more difficult than LAN as well as MAN.
LAN has more fault tolerance	MAN has less fault tolerance	WAN has also fault tolerance.

INTERNET

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

Advantages of Internet

- An internet connection provides many people with ability to work from home or have a virtual office.
- Can provide online education to the student with the help of the Internet.
- With internet, one is able to access information quickly and easily
- The internet improves internal communications through emails, connected calendars and chat services specifically designed to improve business communications.

INTRANET

An intranet is a private network that is contained with an enterprise. Typical intranet for a business organization consists of many interlinked local area networks (LAN) and use any Wide Area Network (WAN) technology for network connectivity. The main purpose of an intranet is to share company information and computing resources among employees. Intranet is a private internetwork, which is usually created and maintained by a private organization. The content available inside Intranet are intended only for the members of that organization (usually employees of a company).

Advantages of Intranet

- It reduces emails and meetings
- Improve employee engagement and knowledge sharing
- Helps an organization to build an internal collaborative culture.
- Increases productivity in an organization
- With use of intranet, there is reduced incidences and errors
- Enhances centralized access to information.

Extranet

An extranet can be viewed as part of a company's intranet that is extended to users outside the company like suppliers. Vendors, partners, customers, or other business associates. Extranet is required for normal day to day business associates. For example, placing purchase order to registered vendors, billing & invoices, payments related activities, joint venture related activities, product brochures for partners, discounted price lists for partners etc.

ETHERNET

Ethernet is defined as a networking technology that includes the protocol, port, cable, and computer chip needed to plug a desktop or laptop into a local area network (LAN) for speedy data transmission via coaxial or fiber optic cables.

Ethernet is used to connect devices in a network and is still a popular form of network connection. For local networks used by specific organizations, such as company offices, school campuses and hospitals. Ethernet is used for its high speed, security and reliability.

Wi –Fi

Wi-Fi (Wireless Fidelity) networks are used commonly and these connect every possible device together. Wi-Fi has been developed to facilitate wireless local area networking in the 2.4GHz or 5.2GHz bands. There are issues related to security threat in Wi Fi, but the same can be prevented using the several security measures that are available. The common security methods include WEP, WPA and WPA2. (Fig 13)

However Wi-Fi is a trade marked phrase that refers to IEEE 802.11x standards.

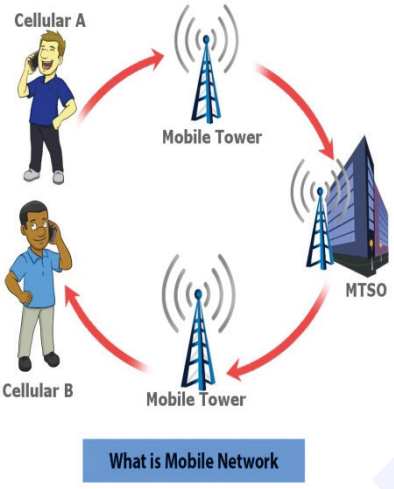
Fig 13

BLUETOOTH

Bluetooth is a short range wireless communication technology, which uses radio waves to transmit information. It is a high speed and low power communication technology to connect gadgets wirelessly without requiring cable connection. It is used for exchanging data between fixed and mobile devices/ computers over short distances. It works well in a short distance for the devices to stay connected, when the range extends it fails to maintain connectivity. The range and transmission speeds of Bluetooth are lower than Wi-Fi.

Mobile Networking (Fig 14)

Fig 14

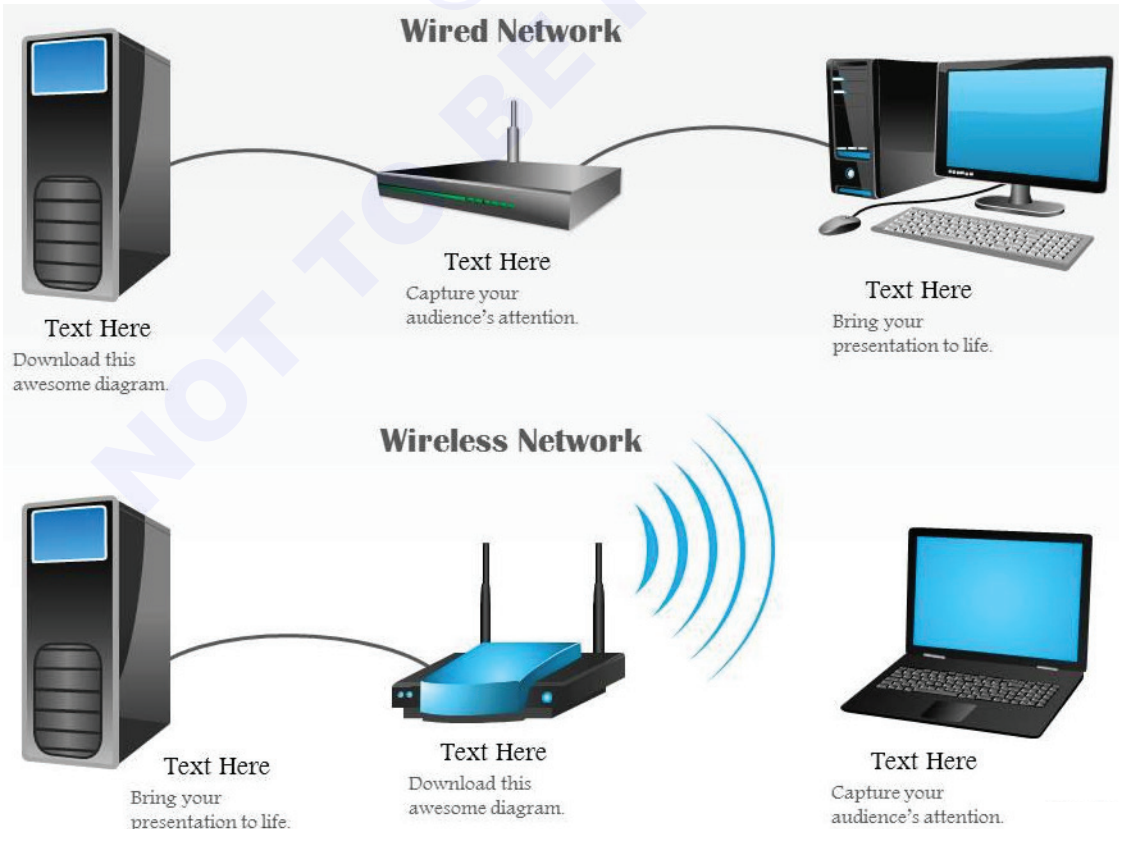


A cellular network or mobile network is a telecommunications network where the link to and from end nodes is wireless and the network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station.

The mobile phone network enables wireless communication using mobile devices, such as mobile phones, smart phones or tablets. Mobile phone networks provide the necessary infrastructure and are operated by mobile phone providers.

Wired and Wireless Networking (Fig 15)

Fig 15



A wired network is one where the devices in the network are connected using cables. Most wired networks are Ethernet networks. Wireless networks use radio waves to connect devices. There are a range of wireless technologies, but the most common are Wi-Fi and Bluetooth.

Wired LANs tend to be much faster, more reliable, provide better security, and deliver more bandwidth than their wireless counterparts. Easier to troubleshoot - Wired LANs are typically much easier to monitor and troubleshoot.

Difference between Internet, Intranet and Extranet

Internet	Intranet	Extranet
It is a global system of interconnected computer network.	It is a private network specific to an organization.	It is a private network that uses public network to share information with suppliers and vendors.
Not regulated by any authority.	It is regulated by an organization.	It is regulated by multiple organization.
Thus content in the network is accessible to everyone connected.	Thus content in the network is accessible only to members of organization.	The content in the network is accessible to members of organization & external members with access to network.
It is largest in terms of number of connected devices.	It is small network with minimal number of connected devices.	The number of devices connected is comparable with Intranet
It is owned by no one.	It is owned by single organization.	It is owned by single/multiple organization.
It is means of sharing information throughout the world.	It is means of sharing sensitive information throughout organization.	It is means of sharing information between members and external members.
Security is dependent of the user of device connected to network.	Security is enforced via a firewall.	Security is enforced via a firewall that separates internet & extranet.
Example: What we are normally using is internet.	**Example:** TCS using internal network for its business operations.	**Example**: HP and Intel using network for business related operations.
Users can access Internet anonymously.	Users should have valid username/ password to access Intranet.	Users should have valid username/ password to access Extranet.
Internet is unregulated and uncensored.	But Intranet is regulated by the organization policies.	Extranet is also regulated by contractual agreements between organizations.

Communication Media & Connectors

Objectives: At the end of this lesson you shall be able to
- **define communication media and connectors**
- **list out the types of network cables and connectors**
- **explain the color codes for CAT5 cable.**

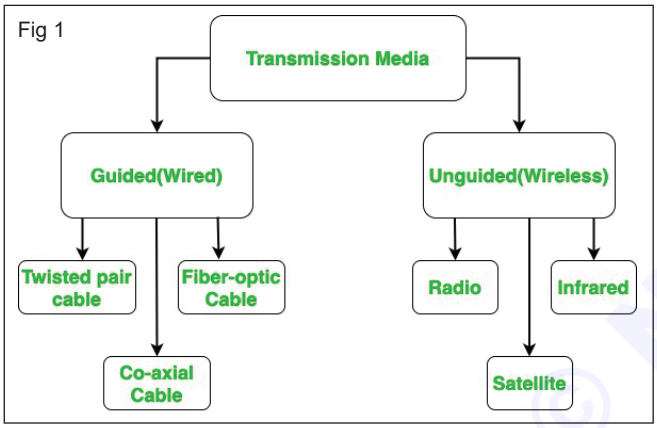
Communication media and Connectors

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e., it is the channel through which data is sent from one place to another. Transmission media is broadly classified into the following types: (Fig 1)

1 Guided Media

2 Unguided Media

Fig 1



Guided Media

It is also referred to as wired or bounded transmission media. Signals being transmitted are directed and confined in the narrow pathway by using physical links.

Features

- High speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided media:

- Coaxial cable
- Twisted pair cable
- Optical Fiber cable

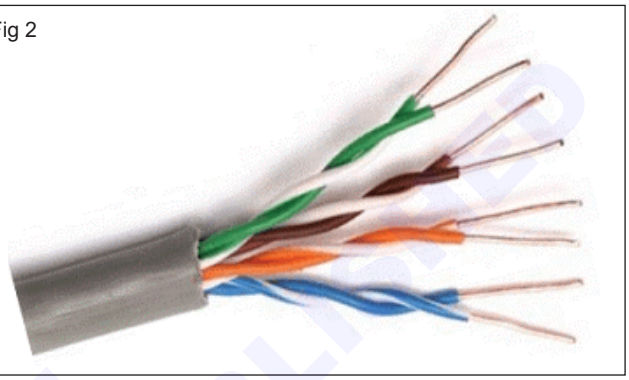
Twisted Pair Cable

It consists of two separately insulated conductor wires wound about each other. Generally several such pairs are bundled together in a protective sheath. They are the most widely used Transmission media.

Types of Twisted-Pair Cables

Unshielded Twisted Pair (UTP) (Fig 2)

Fig 2



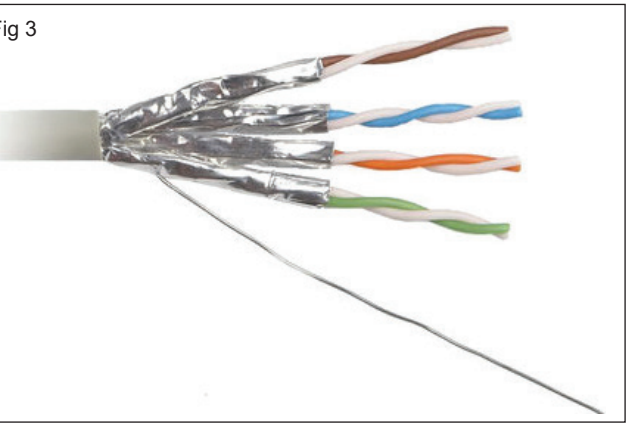
This type of cable has the ability to block interference and does not depend on physical shield for this purpose. It is used for telephonic applications.

Advantages

- Least expensive
- Easy to install
- High speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

Shielded Twisted Pair (STP) (Fig 3)

Fig 3



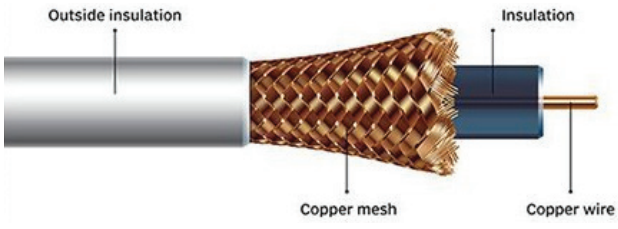
This type of cable consists of a special jacket to block external interference. It is used in fast data rate Ethernet and in voice and data channels of telephone lines.

Advantages

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

Coaxial Cable (Fig 4)

Fig 4



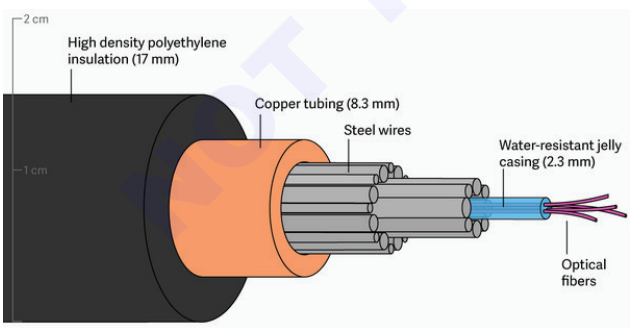
It has an outer plastic covering 2 parallel conductors each having a separate protection cover. The coaxial cable transmits information in two modes. Baseband mode (dedicated cable bandwidth) and broadband mode (cable bandwidth is split into separate ranges). Cable TV and analog television networks widely use Coaxial cables.

Advantages

- High bandwidth
- Better noise immunity
- Easy to install and expand
- Inexpensive

Fiber Optical Cable (Fig 5)

Fig 5



It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded a core made up of glass or plastic covering called the cladding. It is used for the transmission of large volumes of data. The cable can be unidirectional or bi directional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Unguided Media

Radio waves

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency range 3KHz to 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. Further categorized as Terrestrial and Satellite.

Infrared

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency range 300GHZ to 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Connectors

RJ 45 (Registered Jack - 45) (Fig 6)

Fig 6

Registered jack specifications are related to the wiring patterns of the jacks, rather their physical characteristics. The term RJ 45 has also come to refer to a range of connectors for Ethernet jacks. An 8pin/8position plug or jack is commonly used to connect computers onto Ethernet based local area networks. Two wiring schemes T568A and T568B are used to terminate the twisted pair cable onto the connector interface.

RJ 11 (Registered Jack 11) (Fig 7)

Fig 7

Media Type	Maximum segment length	Speed	Cost	Advantages	Disadvantages
UTP	100 m	10 Mbps - 1000 Mbps	Least expensive	Easy to install; widely available and widely used	Susceptible to interference; can cover only a limited distance.
STP	100 m	10 Mbps - 100 Mbps	More expensive than UTP	Reduced crosstalk; more resistant to EMI than thinnet or UTP	Difficult to work with; can cover only a limited distance.
Coaxial	500 m (Thicknet) 185 m (Thinnest)	10 Mbps - 100 Mbps	Relatively inexpensive, but more costly than UTP	Less susceptible to EMI interference than other types of copper media	Difficult to work with (Thicknet); limited bandwidth; limited application (Thinnet); damage to cable can bring down entire network
Fiber-optic	10 km and farther (single-mode) 2 km and farther (multimode)	100 Mbps - 100 Gbps (single mode) 100 Mbps - 9.92 Gbps (multimode)	Expensive	Cannot be tapped, so security is better; can be used over great distances; is not susceptible to EMI; has a higher data rate than coaxial & twisted-pair cable	Difficult to terminate

RJ 11 connector used in analog telephony to connect the phone instrument and the cable. Now it is mostly used to connect to modems and is still used in landlines. It is a 4 slot connector and has six pins, which means you cannot fit it into the RJ 45 slot.

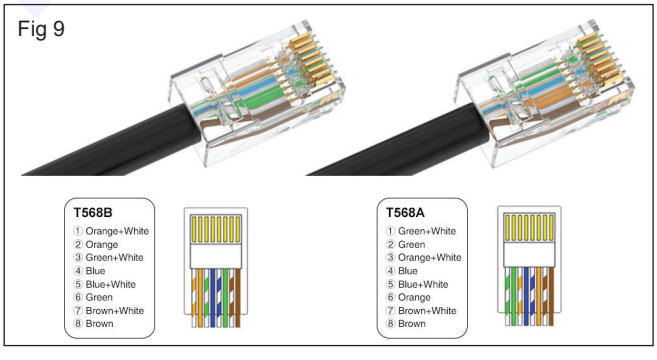
BNC (Bayonet Neill Concelman) connector (Fig 8)

Fig 8

The BNC connector is a miniature quick connect/ disconnect radio frequency connector used for coaxial cable. It is designed to maintain the same characteristics impedance of the cable, with 50 ohm and 75 ohm types being made.

Color codes of T568A and T568B CAT5 cables (Fig 9)

Fig 9



Straight through cable

Straight Through Cable is used for connecting a LAN port to a computer, hub or switch. It is an 8 wired patch cable. It is also used when connecting a PC to a switch and also for connecting router to a hub, or a printer to the router etc. Its main purpose is to connect a host to the client.

Cross over Cable

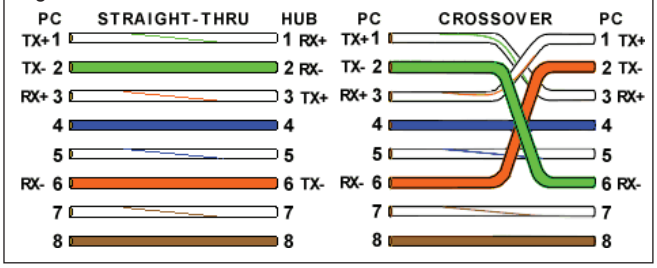
Crossover cables are planted to connect two hosts together. The cables are crossed wired to let the two computers or hosts get connected directly. It can also be said that primarily Crossover Cables are used when like or same devices are intended to be connected. The

pairs of wires crisscross each other which makes the communication path for the two devices to communicate at the same time. Crossover cables are extensively used for connecting a computer with a computer, switch with a switch, and router with a router, hub with a hub and computer with a router. They overturn the receiving and transmission signals.

The updating technology has made devices with integrated auto sensing technology which helps them to build the crosses pairs when required. (Fig 10)

For example:

Fig 10



Pin number designations

There are pin number designations for each color in T-568B and T-568A.

T-568B			T-568A	
Pin	**Color**	**Pin Name**	**Color**	**Pin Name**
1	Orange stripe	Tx+	Green stripe	Rx+
2	Orange	Tx-	Green	Rx-
3	Green stripe	Rx+	Orange stripe	Tx+
4	Blue	Not used	Blue	Not used
5	Blue stripe	Not used	Blue stripe	Not used
6	Green	Rx-	Orange	Tx-
7	Brown stripe	Not used	Brown stripe	Not used
8	Brown	Not used	Brown	Not used

RJ45 color-coded scheme

RJ45 cables have 8 color-coded wires, and the plugs have 8 pins and conductors. Eight wires are used as 4 pairs, each representing positive and negative polarity. The most commonly used wiring standard for 100baseT is T-586B standard described above. Prior to EIA 568A and 568B standards, the color-coded scheme was used to wire RJ45 cables. The table below depicts pin and color schemes used in traditional and standardized setup.

The most commonly recognized registered jack is the RJ11. This is a modular connector wired for one telephone line, using the center two contacts of six available positions, and is used for single-line telephones in homes and offices in most countries. RJ14 is similar to RJ11 but is wired for two lines and RJ25 has three lines. RJ61 is a similar registered jack for four lines.

The RJ45(S) jack is rarely used, but the designation RJ45 commonly refers to any 8P8C modular connector for application in computer networking (Ethernet).

Pin	Colored scheme	T-568B (Common)	T-568A
1	Blue	Orange stripe	Green stripe
2	Orange	Orange	Green
3	Black	Green stripe	Orange stripe
4	Red	Blue	Blue
5	Green	Blue stripe	Blue stripe
6	Yellow	Green	Orange
7	Brown	Brown stripe	Brown stripe
8	White (or Grey)	Brown	Brown

The officially recognized types of registered jacks are listed in the following table:

Code	Connector	Usage
RJA1X	225A adapter	Connector for a modular plug to a four-prong jack
RJA2X	267A adapter	Connector for splitting one modular jack to two modular jacks
RJA3X	224A adapter	Connector for adapting a modular plug to a 12-prong jack
RJ2MB	50-pin micro ribbon	2-12 telephone lines with make-busy arrangement
RJ11(C/W)	6P2C	Establishes a bridged connection for one telephone line (6P4C if power on second pair)
RJ12(C/W)	6P6C	Establishes a bridged connection for one telephone line with key telephone system control ahead of line circuit
RJ13(C/W)	6P4C	Similar to RJ12, but behind the line circuit
RJ14(C/W)	6P4C	For two telephone lines (6P6C if power on third pair)
RJ15C	3-pin weatherproof	For one telephone line for boats in marinas
RJ18(C/W)	6P6C	For one telephone line with make-busy arrangement
RJ21X	50-pin micro ribbon	For up to 25 lines
RJ25(C/W)	6P6C	For three telephone lines
RJ26X	50-pin micro ribbon	For multiple data lines, universal
RJ27X	50-pin micro ribbon	For multiple data lines, programmed
RJ31X	8P8C	Allows an alarm system to seize the telephone line to make an outgoing call during an alarm. Jack is placed closer to the network interface than all other equipment. Only 4 conductors are used.
RJ32X	8P8C	Like RJ31X, this wiring provides a series tip and ring connection through the connecting block, but is used when the customer premises equipment is connected in series with a single station, such as an automatic dialer.
RJ33X	8P8C	This wiring provides a series tip and ring connection of a KTS line ahead of the line circuit because the registered equipment requires CO/PBX ringing and a bridged connection of the A and A1 lead from behind the line circuit. Tip and ring are the only leads opened when the CPE plug is inserted. Typical usage is for customer-provided automatic dialers and call restrictors.
RJ34X	8P8C	Similar to RJ33X, but all leads are connected behind the line circuit.
RJ35X	8P8C	This arrangement provides a series tip and ring connection to whatever line has been selected in a key telephone set plus a bridged A and A1 lead.
RJ38X	8P4C	Similar to RJ31X, with a continuity circuit. If the plug is disconnected from the jack, shorting bars allow the phone circuit to continue to the site phones. Only 4 conductors are used.
RJ41S	8P8C, keyed	For one data line, universal (fixed loop loss and programmed)
RJ45S	8P8C, keyed	For one data line, with programming resistor
RJ48C	8P4C	For four-wire data line (DSX-1)
RJ48S	8P4C, keyed	For four-wire data line (DDS)
RJ48X	8P4C with shorting bar	For four-wire data line (DS1)
RJ49C	8P8C	For ISDN BRI via NT1
RJ61X	8P8C	For four telephone lines
RJ71C	50-pin micro ribbon	12 line series connection using 50-pin connector (with bridging adapter) ahead of customer equipment. Mostly used for call sequencer equipment.

Introduction to data communication

Objectives: At the end of this lesson you shall be able to
- **define data transmission**
- **define analog and digital signals**
- **explain the types of data transmission mode.**

Data Communications

When we communicate, we are sharing information. This sharing can be local orremote. Between individuals, local communication usually occurs face to face, whileremote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (teleis Greek for “far”).

The word data refers to information presented in whatever form is agreed upon bythe parties creating and using the data.

Data communications are the exchange of data between two devices via someform of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combinationof hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1 **Delivery -** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2 **Accuracy -** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3 **Timeliness -** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

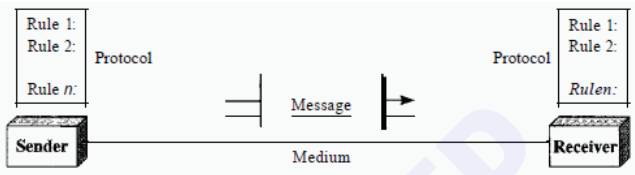
4 **Jitter -** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Components

A data communications system has five components (Fig 1).

1 **Message -** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Fig 1



2 **Sender -** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

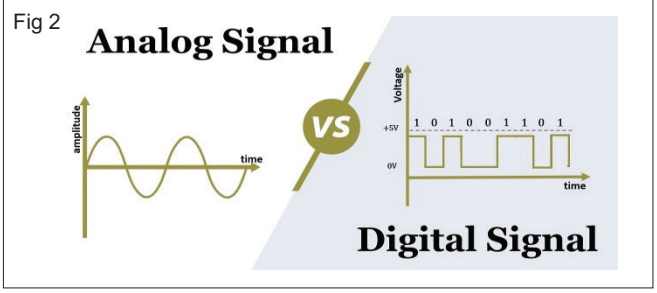
3 **Receiver -** The receiver is the device that receives the message. It can be a computer workstation, telephone handset, television, and so on.

4 **Transmission medium -** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5 **Protocol -** A protocol is a set of rules that govern data communications. 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.

Analog and Digital Signal (Fig 2)

Fig 2



Analog and digital signals are the types of signals carrying information. The major difference between both signals is that the analog signals have continuous electrical signals, while digital signals have non-continuous electrical signals.

An analog signal is signals and wavelengths transmitted over communications lines such as the sound of a voice over the phone line. With computers, a dial-up modem is an example of a device that takes digital data and converts it to an analog signal to transmit over phone lines.

A digital signal is a signal that represents data as a sequence of discrete values. A digital signal can only take on one value from a finite set of possible values at a given time. With digital signals, the physical quantity representing the information can be many things: Variable electric current or voltage.

Analog signals are represented by a sine wave and digital as square waves. Analog signals when compared to digital signals are continuous and more accurate. Digital signals are less expensive, negligible distortion, have a faster rate of transmission.

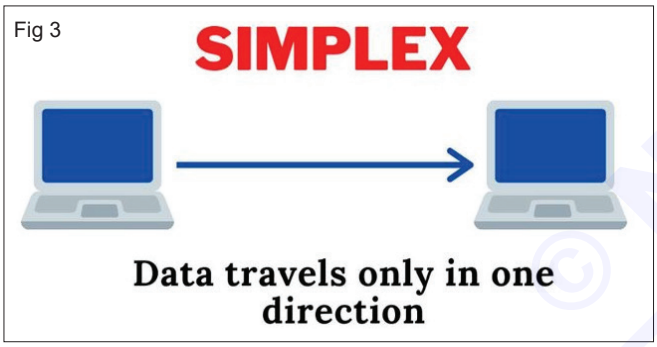
Data Transmission

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode:

- Simplex mode
- Half - Duplex mode
- Full - Duplex mode

Simplex Mode (Fig 3)

Fig 3

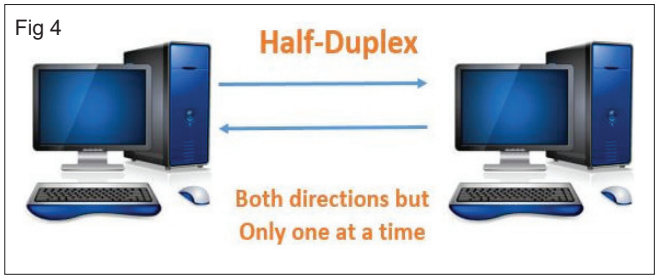


In Simplex mode, the communication is unidirectional. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

Half – Duplex Mode (Fig 4)

Fig 4



In half duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half - duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkie in which message is sent one at a time and messages are sent in both the directions.

Full – Duplex Mode (Fig 5)

Fig 5

In Full – duplex mode, both stations can transmit and receive simultaneously. In full – duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, Example: Telephone , this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving or the capacity is divided between signals travelling in both directions.
- Full- duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided the two directions.

Difference between Simplex, Half Duplex and Full Duplex

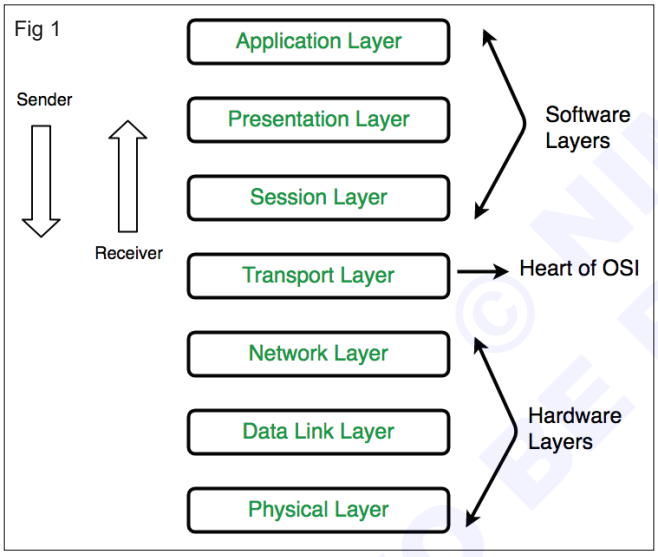
Simplex mode	Half duplex mode	Full duplex mode
A unidirectional communication.	A two way directional communication but one at a time.	A two way communication simultaneously.
Sender can send the data but that sender can't receive the data.	Sender can send the data and also can receive the data but	Sender can send the data and also can receive the data simultaneously.
Provides less performance than half duplex and full duplex mode.	Provides less performance than full duplex mode	Provides better performance than Simplex and Half duplex mode.
Example: Keyboard and Monitor	Example: Walkie- Talkie	Example: Telephone

OSI Model

Objectives: At the end of this lesson you shall be able to
- **define OSI model**
- **list out the name of the layers in OSI model**
- **explain the working principle of each layer.**

OSI Model - 7Layers

The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which provides a standard for different computer systems to be able to communicate with each other. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last. Each layer of the OSI model handles a specific job and communicates with the layers above and below itself. The seven layers of the OSI model can be defined as follows, from bottom to top: (Fig 1)



The Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

The Data link layer

The data link layer facilitates data transfer between two devices on the same network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra network communication.

The Network Layer

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination, this is known as routing.

The Transport Layer

Layer 4 is responsible for end to end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume. It's also responsible for flow control and error control.

Flow determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

The Session Layer

This layer is responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources. The session layer also synchronizes data transfer with check points.

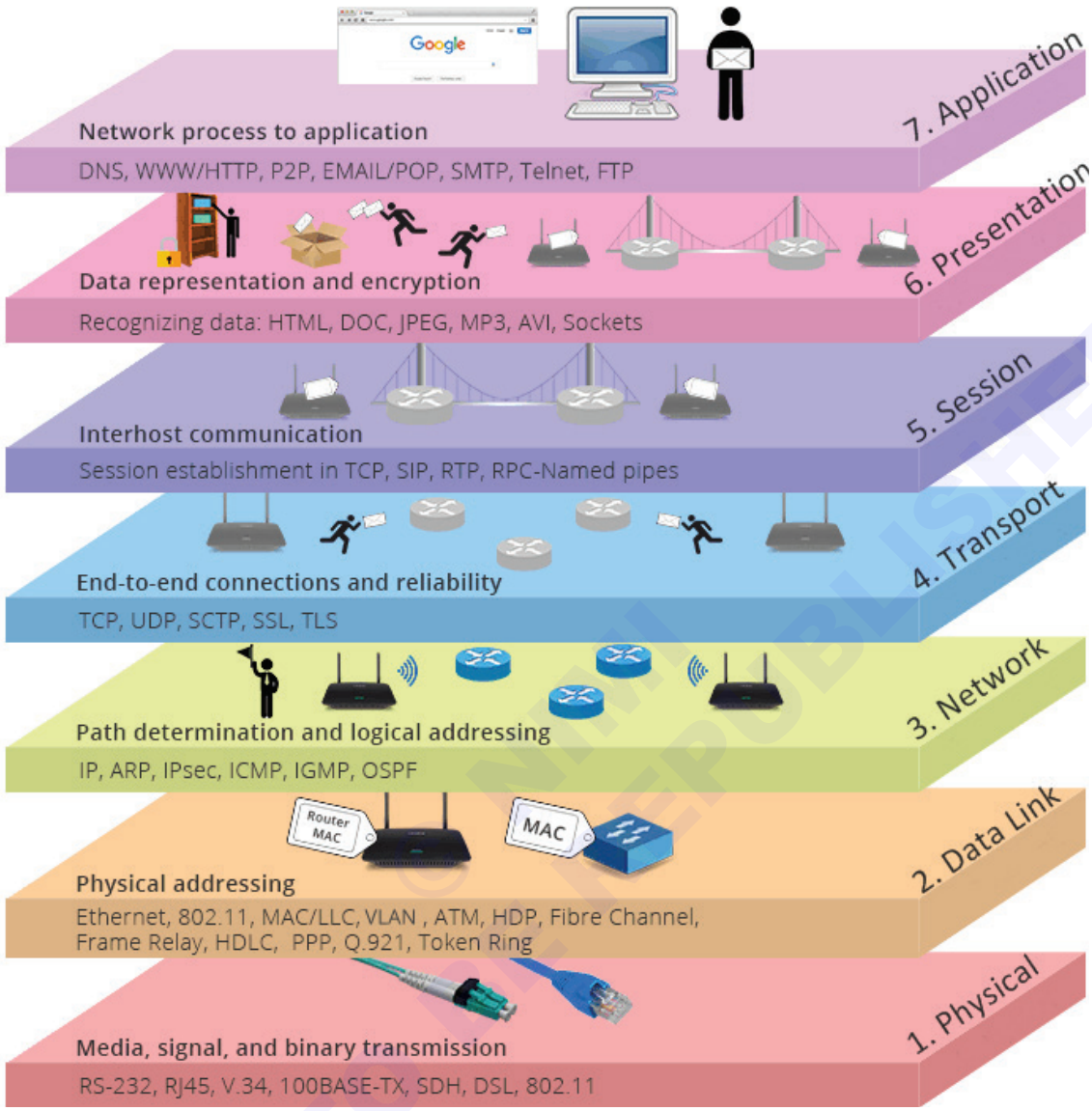
The Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer, the presentation layer is responsible for translation, encryption, and compression of data. If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with

unencrypted, readable data. Finally, the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

Data transformation stages (Fig 2)

Fig 2



The Application Layer: This is the only layer that directly interacts with data from the user. Software applications link web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer, rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

How data flows through the OSI model?

In order for human readable information to be transferred over a network from one device to another, the data must travel down the seven layers of the OSI model on the sending device and then travel up the seven layers on the receiving end.

Advantages of OSI model

The OSI model helps users and operators of computer networks:

- Determine the required hardware and software to build their network.
- Understand the communicate the process followed by components communicating across a network.
- Perform troubleshooting by identifying which network layer is causing an issue and focusing efforts on that layer.

OSI Model and Communication between Systems

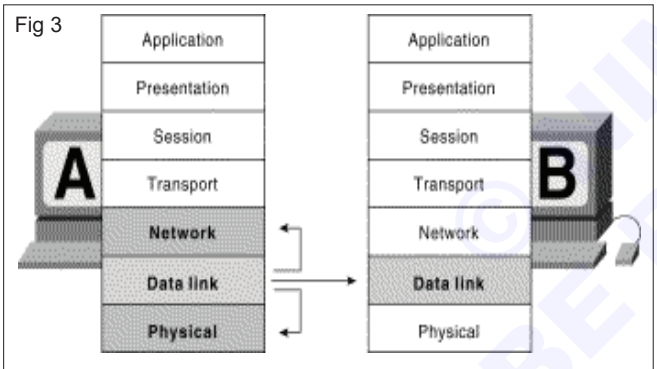
Information being transferred from a software application in one computer system to a software application in another must pass through the OSI layers. For example, if a software application in System A has information

to transmit to a software application in System B, the application program in System A will pass its information to the application layer (Layer 7) of System A. The application layer then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

Interaction between OSI Model Layers

A given layer in the OSI model generally communicates with three other OSI layers: the layer directly above it, the layer directly below it, and its peer layer in other networked computer systems. The data link layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B. Fig 3 illustrates this example.

Fig 3



OSI model layers communicate with other layers

The OSI model helps network device manufacturers and networking software vendors

- Create devices and software that can communicate with products from any other vendors, allowing open interoperability.
- Define which parts of the network their products should work with.
- Communicate to users at which network layers their product operates – for example, only at the application layer or across the stack.

TCP/IP Model – 4 Layers

It stands for Transmission Control Protocol / Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are,

1 Process / Application layer

2 Host –to –Host / Transport layer

3 Internet layer

4 Network Access / Link layer

The Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. It helps you to define details of how data should be sent using the Network. It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, fiber or twisted pair cables. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Internet Layer

An internet layer is a second layer of TCP/IP layers of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer till they reach the destination irrespective of the route they take. The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks. Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer - management protocols that belong to the network layer are:

- Routing protocols
- Multicast group management
- Network layer address assignment.

Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error free and in sequence. Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation. The transport layer also offers an acknowledgement of the successful data transmission and sends the next data in case no errors occurred. TCP is the best known example of the transport layer.

Importance functions of Transport Layers

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.

- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Application Layer

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model. Example of the application layer is an application such as file transfer , email, remote login, etc.

The functions of the Application Layers

- Application layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services.

Advantages of the TCP/IP model

- It helps you to establish up a connection between different types of computers.
- It operates independently of the operating system
- It supports many routing protocols
- It enables the internet working between the organizations.
- TCP/IP model has a highly scalable client server architecture.
- It can be operated independently.
- Supports a number of routing protocols.
- It can be used to establish a connection between two computers.

Disadvantages of the TCP/IP model

- TCP/IP is a complicated model to set up and manage
- The transport layer does not guarantee delivery of packets.
- Replacing protocols in TCP/IP is not easy
- It has no clear separation from its services, interfaces and protocols.

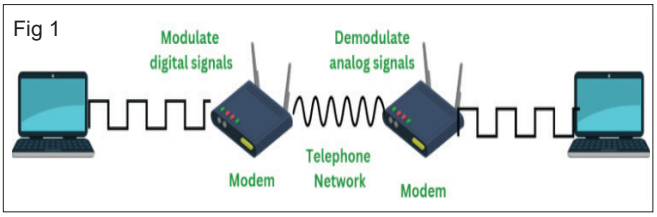
Network Components

Objectives: At the end of this lesson you shall be able to
- **define of Network components and their types, applications and advantages**
- **define IP Routing in Network RIP IGRP.**

MODEM

A portmanteau of “Modulator – Demodulator” is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line can transmit only analog data. (Fig 1)

Fig 1



The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices Modulator and Demodulator. The modulator converts digital data into analog data is being send by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.

Whenever a user uploads data from a computer on the internet, the modem takes in the digital signal from your computer and then, converts these signals into analog signals. Analog signals can be easily accessed by telephone networks. When computers try to download data from the internet, the modem takes the analog signal over the telephone and converts that signal into a digital signal. The digital signal is accessible by the computer.

Types of Modem

There are following different types of Modem

1 Cable Modems

Cable modems help in establishing communication between computer and ISP over landline connection. These modems allow the access to high-speed data with the help of a cable TV (CATV) network. Such modems are external devices connected to your PC with the help of a standard 10 BASE-T Ethernet card and twisted pair wiring.

2 Telephone Modems

These modems are network devices that allow data communication between two computers over voice-grade telephone lines. Telephone modems convert bits to analog signals for transmission through physical channels. These also convert the analog signals in the local loops into bits that are understandable by a computer.

3 Dial Modems

These modems convert the data between analog form (used on the telephone lines) and digital form (used on the computers). These networking devices plug into computer at one end and a telephone line at another end. These modems can transmit the data at a maximum rate of 56000 bits/sec. Whenever you have connected to a network with the help of dial up modem, it relays distinctive handshaking sounds between the remote modem and your device. This sound helps in verifying if the connection is working.

4 Satellite Modems

These modems provide an internet connection with the help of satellite dishes. They transfer input bits into output radio signals. It then executes the vice versa. These modems are more reliable for providing an internet network in comparison with other modems.

5 Digital Subscriber Line (DSL)

DSL are used for transmission of the digital data over telephone lines. These modems offer high-speed internet connection through telephone lines. Two types of DSL modem include asymmetric and symmetric DSL that use existing telephone wiring within your home wiring. Due to the use of existing wiring, these modems are cost-effective.

Applications of Modems

Initially, these devices were used for either sending faces or for connecting the user with the internet. These days, modems have more than just two applications. These include the following:

1 **Data transfer**: Dial modems provide secure connections for smoothly transferring the data. These come along with the redial functionality in case a call is dropped.

2 **Reliable backup**: Modems act as a backup in the absence of stable broadband or server connection. With modems, data can be retrieved and servers can be configured even if the status of the broadband connection is not known.

3 **Remote management**: These networking devices can be installed at remote or sensitive locations. Along with that, modems help in remotely controlling certain applications. This helps in a quick resolution to issues that will otherwise require physical assessment.

Advantages of Modem

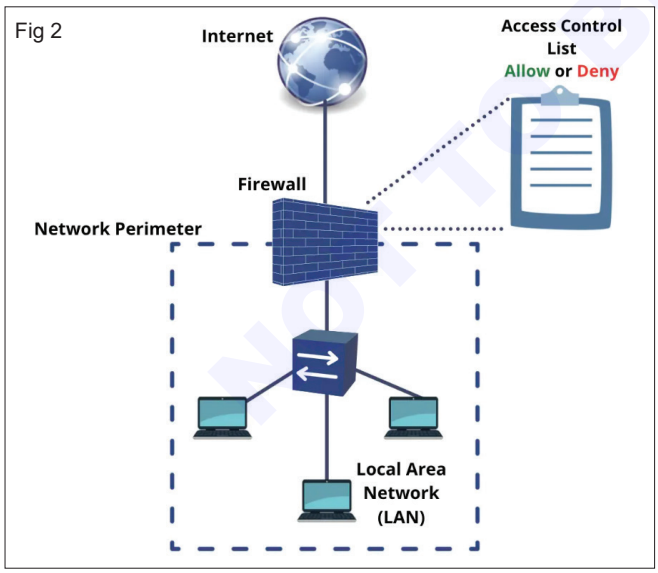
Modems have the following characteristics:

- Modems are useful in converting digital signals into analog signals.
- They help in connecting the devices to the internet.
- Only a limited number of systems can be connected to the internet through a modem.
- Modems are prone to cyber-attacks which reduces the probability of secure transmission.
- The cost of a modem is dependent on the number of features it offers. More inclusion of features will lead to an increase in the cost of modem.
- Modems slow down when it is connected to a hub.
- They are unable to track traffic between the LAN and the internet.
- Modems require RJ11 Jack to communicate with telephone lines and RJ45 for connection with computers.
- For modems to work, device drives must be installed in the operating system for configuration and communication.
- These devices must be configured with an Internet Service Provider (ISP) and computer for using the internet.

Firewall

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. (Fig 2)

Fig 2



A firewall is a type of cybersecurity tool used to filter traffic on a network. Firewalls can separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having unique pros and cons.

Out of the three firewall types, a proxy firewall is the most secure. The concept works the same as using a middleman to receive sensitive materials, inspecting them at a secure location, then delivering them to you once they are declared "safe."

Types of Firewall

Stateless packet-filtering firewall

A packet filtering firewall is the oldest form of firewall. These firewalls live on the edge of a perimeter security-based network and require manual inputs from a security professional to s-et the parameters for traffic without any learning capabilities. An administrator creates an access control list (ACL) to either allow or deny packets from certain internet protocol (IP) addresses. It's essentially a "dumb" firewall.

What makes these firewalls "stateless" is the lack of any packet inspection, source logging, or validation capabilities. The problem with stateless packet-filter firewalls is the implied trust that's given to IP addresses allowed by administrators. While these firewalls block traffic from denied sources, not all threats originate from malicious addresses.

In some cases, trusted addresses can be hijacked and used to pass along malicious traffic through your perimeter security — all under the nose of a stateless packet filter. Think of this like a trusted mail carrier passing along a package with a bomb in it without building security knowing.

Stateful inspection firewalls

If you're looking for an upgrade from 1990s capabilities, that would be the stateful inspection firewall.

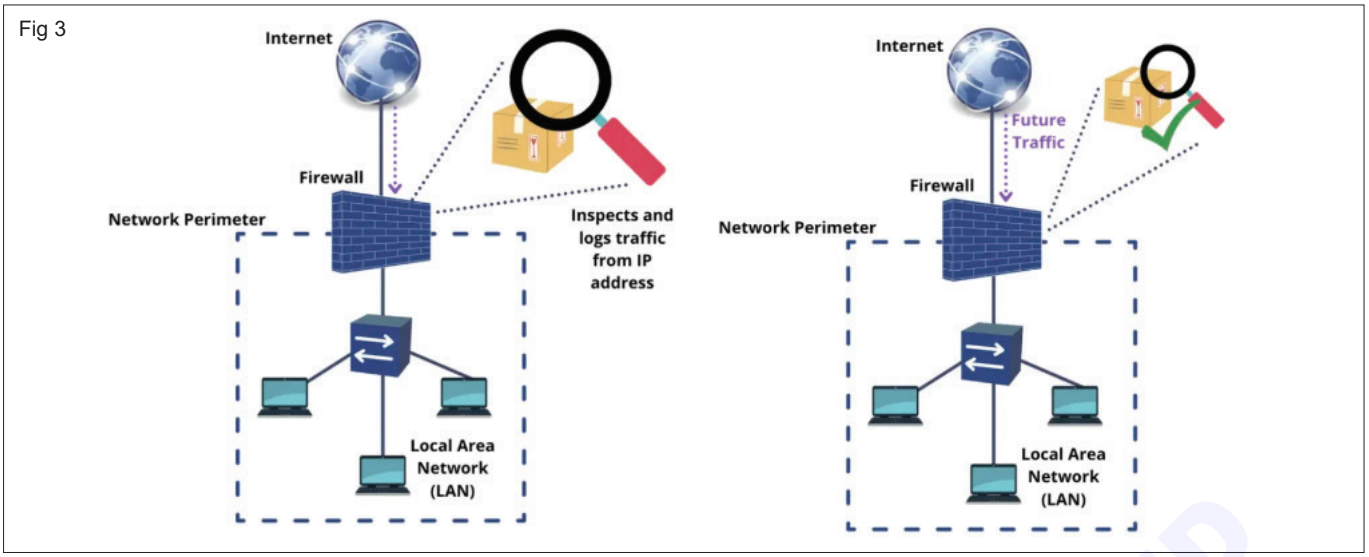
This firewall type is "stateful" because while it does use access control lists to regulate incoming and outgoing packets, the firewall also inspects packet traffic, logs the relevant data — originating address, packet type, destination, and so on — and compares future traffic against that log to validate it. (Fig 3)

This firewall operates under the concept of "this traffic was safe before, so if it's the same, it's safe now." While this is an upgrade from using simple ACLs, this type of firewall is prone to two specific vulnerabilities.

The first issue is that stateful inspection firewalls are process-intensive and tend to bottleneck traffic due. This makes them potential targets for distributed denial-of-service (DDOS) attacks.

The second issue is that their inspection is still limited. This makes it possible for hijacked traffic through the firewall so long as the traffic type isn't unexpected. This makes stateful firewalls vulnerable to "man-in-the-middle" (MITM) attacks where hackers intercept the connection and begin sending altered packets of the same type back through the firewall. Your firewall won't know that the traffic is malicious since it'll look like it's coming from an expected source.

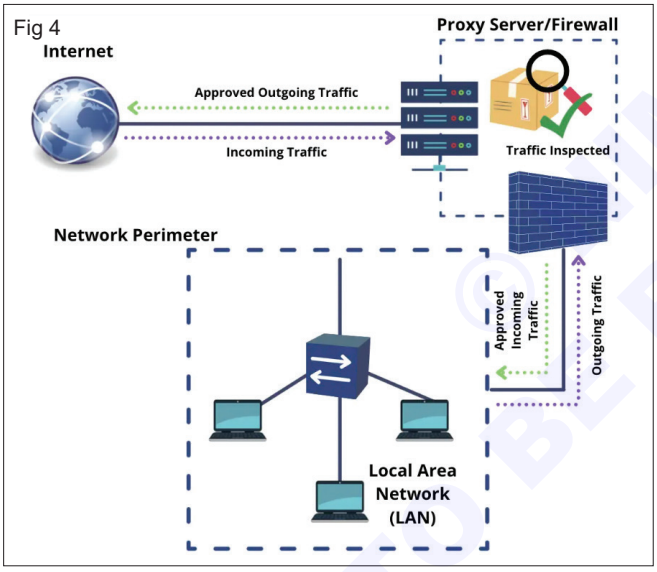
Fig 3



Proxy firewalls

Out of the three firewall types, a proxy firewall is the most secure. The concept works the same as using a middleman to receive sensitive materials, inspecting them at a secure location, then delivering them to you once they are declared "safe." (Fig 4)

Fig 4



Instead of allowing traffic to reach the network perimeter before it's inspected, a proxy firewall filters packets through a server with a firewall installed:

Most proxy firewalls employ security capabilities not shared by the last two, such as:

- **Deep packet inspection (DPI):** DPI searches for signatures of malware, outgoing sensitive data, and monitors for restricted content, such as unmanaged virtual private network (VPN) traffic or inappropriate websites.
- **Sandboxing:** The biggest benefit of a proxy firewall is the distance it creates between threats and your network. This creates a "sandboxing" capability that allows threats to play out in a safe environment that only harms the specific firewall it contacts. Most security infrastructures create redundant proxy firewalls that take over in case one is down.
- **Traffic validation:** Like standard stateful firewalls, proxy firewalls also use administrative tools like ACLs and logging to validate traffic from recognized sources.

Firewalls Are Moving to the Cloud

As businesses rapidly shift to the cloud, the demands on the old network perimeter are too much for a standard firewall. Packet filters and stateful firewalls aren't enough to protect networks, data, and devices from the long list of external and internal threats that exist today.

That's why firewalls are becoming firewalls as a service (FWaaS). These new firewalls converge with other technologies, such as secure web gateways (SWG), zero-trust architectures, cloud access security brokers (CASB), and other security functions, into a new paradigm known as secure access service edge (SASE) architecture.

This convergence makes firewalls more effective at inspecting traffic and protecting your assets and data from new threats that would otherwise evade your standard packet-filtering firewall.

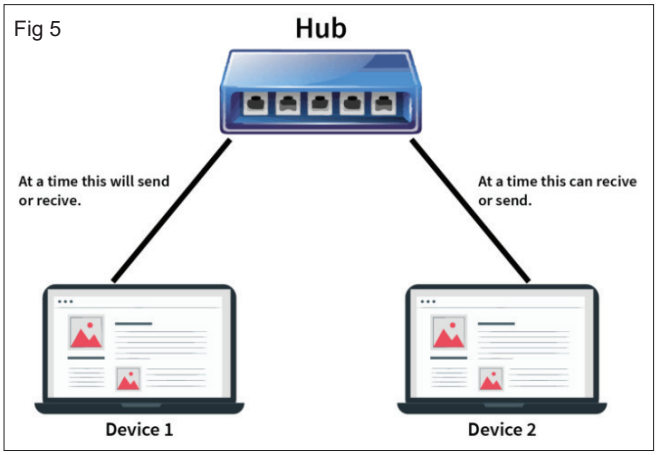
HUB

A hub is a networking device that is used to connect multiple devices in a network. Hub works at the physical layer and broadcasts data to all the ports except the port from which the data is being broadcasted. Hub stores various ports, such that when a packet arrives at one port it is copied to other ports. (Fig 5)

A hub receives data and then sends it in full to all connected devices (hosts). All ports of the hub operate at the same speed and are located in a collision domain (which includes all connected network devices).

Hub works in half-duplex mode. This device sends and receives data as electrical signals or binary bits. The diagram below shows the half-duplex mode of a hub:

Fig 5



Types of Hub

There are two types of hubs. They are mentioned below:

1 **Active hub**: This hub uses electricity and is capable of regenerating binary signals and amplifying analog signals. Hence this can also be used as a repeater.

2 **Passive hub**: This does not use electricity hence it doesn't have the capability of regeneration or amplification. It just transmits the data.

Applications of Hub

- These are used by various organizations to provide connectivity.
- They are also used in small networks like home networks.
- They are also used for network monitoring.

Advantages of Hub

- **Connectivity**: This allows the clients to connect to a network so that they can share and have conversations.
- **Cost**: Hubs are cheap compared to switches.
- **Area Coverage**: Only Active hubs can be used as repeaters to increase the area coverage of a network as they have a power source that can be used to amplify the signals. Passive hubs can't be used for the same.

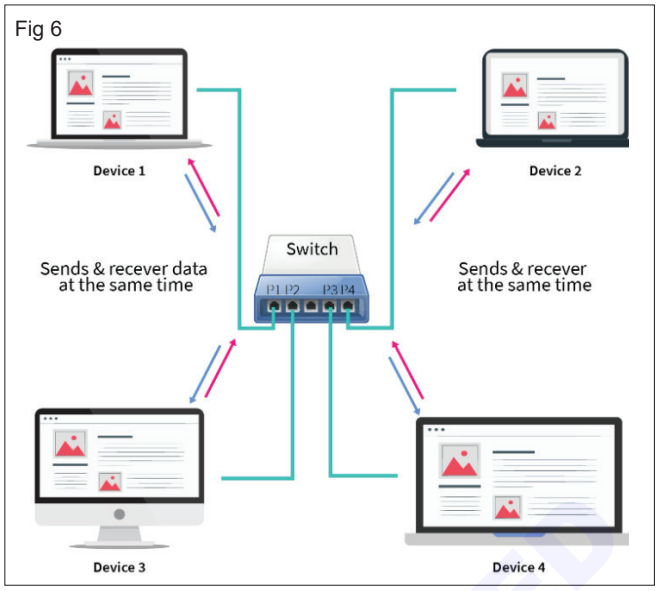
Switch

Switch is also a networking device that works on the data link layer of the OSI model. This is used to connect various devices together in a computer network. The switch enables connection setting and termination based on the need for connection. (Fig 6)

The device stores the MAC address of all the devices connected to it. To store this it maintains a table where the port number is mapped to the MAC address of the device connected to that port.

This device first broadcasts to the MAC address of all the devices connected to the switch and then multicast or unicast depending on the requirement. The first time a switch receives a data frame from a device connected to it, it broadcasts it to all the devices connected to its port except the port on which it received the data frame.

Fig 6



When the device that was supposed to receive the data gets the data, it sends an acknowledgment. Using this acknowledgement it maps that device with the port on the switch. Switch also provides packet filtering. In this way, the Mac address table is filled.

Switch works in full duplex mode. In this, the number of collision domains is equal to the number of ports present in the device.

Since there are a lot of collision domains collisions are very less. Generally, a switch has 16 to 48 ports. This device sends and receives data in the form of a data packet called frame and packet.

The diagram below shows the full-duplex mode of a switch.

Types of Switch

The types of switches are given below:

- **Unmanaged switches**: These switches are used in homes and small businesses. There is no need to configure these switches. It can be instantly used.
- **Managed switches:** These switches are used in large companies and organizations. There is a need for configuration in setting the precision control and the highest level of security. These switches are very costly but at the same time are scalable. Managed switches are also of two types:
- **Smart switches:** This offers basic security level management features. Hence called partially managed switches. These are used in fast LANs which support gigabits of data transfer.
- **Enterprise managed switches:** These switches have the ability to fix, copy, transfer, and display network configurations, web interface, SNMP (Simple Network Management Protocol), and command line interface. These are used in organizations having a large number of ports, switches, and nodes. Nodes are devices on a network that can both receive and communicate data.

- **LAN switches:** These switches are used to reduce network congestion or bottleneck by distributing data only to the intended recipient. These are also known as ethernet switches.
- **PoE switches:** PoE stands for Power Over Ethernet. These switches allow devices to use power and receive data on the same cable simultaneously. Hence simplifying the cabling process.

Applications of Switch

- It is used to manage the flow of data across the network.
- These are used to connect devices together physically on the same computer network.
- They are used to connect components of LAN.
- These are managed switches that are used in large organizations to manage security and flow of data.

Advantages of Switch

- **Bandwidth:** Switches increase the available bandwidth of the network.
- **Performance:** They improve the performance of the network.
- **Collision domains:** Switches create a collision domain for each connection hence there are very few collisions in switches.
- **Traffic management:** Switches use port-to-MAC mapping to manage network traffic.
- **VLANs (virtual LAN):** Supports VLANs that help in logical segmentation of ports.
- **Configurations:** Switch provides configurations of security and precision.

Key Difference Between Hub and Switch

The main difference between a hub and a switch is in how they handle data traffic within a network. Hubs, considered less intelligent, indiscriminately broadcast data to all connected devices, causing congestion and inefficiency as all devices receive the data, regardless of whether it's intended for them or not. On the other hand, switches are more intelligent; they selectively forward data only to the specific device for which it is intended, reducing network traffic and improving overall speed and efficiency. This key distinction makes switches a preferred choice in modern networks where efficient data management is crucial.

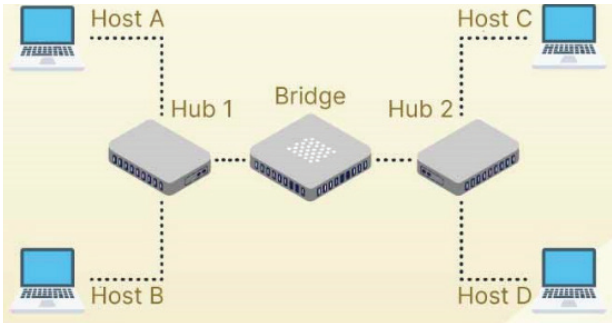
Difference Between Hub and Switch

S.No.	Hub	Switch
1	This works on the physical layer which is layer-1 of the OSI model.	This works on the data link layer which is layer-2 of the OSI model.
2	Used to connect multiple PCs in a single computer network.	Used to connect various devices on a single computer network.
3	Data is transmitted as electrical signals or bits.	Data is transmitted as frames and packets.
4	A hub also broadcasts data to all connected devices.	Switch first broadcasts and then performs unicast or multicast based on the intended recipient.
5	Operates in half-duplex transmission mode.	Operates in full-duplex transmission mode.
6	Has only one collision domain.	The number of collision domains equals the number of ports in the switch.
7	Encounters a lot of collisions.	There are no collisions in a full-duplex switch.
8	Considered non-intelligent as it doesn't use MAC addresses.	An intelligent device that uses MAC addresses to send data only to the intended recipient.
9	Lacks tables for storing MAC addresses.	Stores MAC addresses in CAM (Content Addressable Memory) tables.
10	A passive device that doesn't actively process data.	An active device that processes and forwards data intelligently.
11	Supports transfer speeds of 10 Mbps.	Supports transfer speeds ranging from 10/100 Mbps to 1 Gbps and beyond.
12	Limited in scalability and network size.	More scalable, making it suitable for larger networks and diverse setups.
13	Simpler and cost-effective but less efficient.	Efficient in managing network traffic and offers better performance but is relatively costly.

Bridges

A bridge is a network device that connects multiple sub-networks to create a single network. It provides interconnection with other computer networks that use the same protocol. Through a bridge, multiple LANs can be connected to form a larger and extended LAN. (Fig 7)

Fig 7



A bridge is a network device that connects multiple sub-networks to create a single network. It provides interconnection with other computer networks that use the same protocol. Through a bridge, multiple LANs can be connected to form a larger and extended LAN. This function of creating a single aggregate network from multiple network segments is called network bridging. It works in the data link layer, which is the second network layer in the OSI model.

Functions of Bridges

Now, let us take a look at the functions of bridges:

- Store MAC address in PC that is used in the network for reducing network traffic.
- Divide local area networks into multiple segments.
- Connects multiple networks to ensure communication between them.
- Connects LAN segments into a single network.
- Recognizes areas where data is to be sent and on which device it will be sent.
- Maintains MAC address table to discover new segments.
- Used in load filtering of network traffic by separating it into segments or packets

Advantages of Bridges

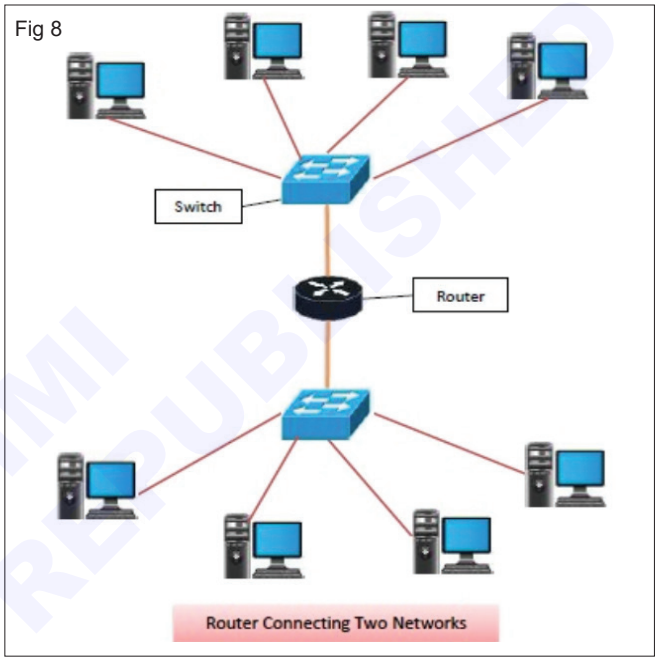
Bridges are smart network devices that have the following advantages:

- Improve the performance of bridges by segmenting large busy networks into multiple smaller and interconnected networks.
- Cost-effective as they are simple and inexpensive.
- Increases available bandwidth to individual nodes as lesser network nodes share collision domain.
- Reduces network congestion by dividing LAN into multiple smaller segments.
- Bridges are smart networking devices that can be used as repeaters to extend a network. They have many benefits as well as disadvantages. Based on the requirement of your system and network, you should choose a network device that can fulfill them.

Routers

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route. (Fig 8)

Fig 8



Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs, bridges, and switches.

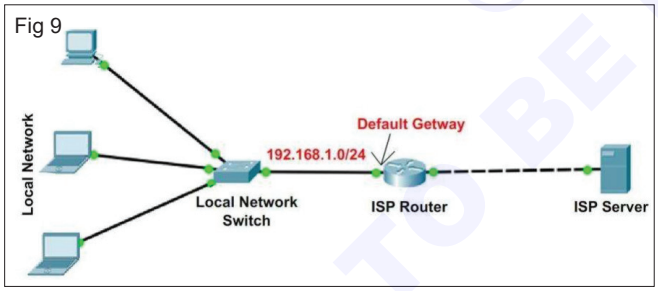
Types of Routers

A variety of routers are available depending upon their usages. The main types of routers are −

- **Wireless Router −** They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers −** They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers −** They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers −** They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
- **Brouters −** Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Gateways (Fig 9)

Fig 9



- A device that can bridge several network structure is called a gateway. Thus gateways can link two dissimilar LANs. The major difference between gateways and routers is that routers operate at the OSI model's network layer. In contrast, gateways operate from the lowest to the topmost layer, i.e., the application layer to the OSI model's network layer.
- Gateways and routers are used correspondingly. It can change data packets from one protocol structure to another before forwarding them to connect two different networks. Hence it incorporates a protocol conversion function at the application layer.
- A gateway is a connecting device that can relate to multiple networks. They perform at the application layer of the OSI model. They manage messages, locations, and protocol conversion to deliver a packet to its terminal between two connections.
- The main disadvantage of the gateway is that gateways are slow because they need to perform intensive conversions.

Characteristics of Gateways

- It can support complete protocol transformation from one proprietary computer network technology to other technology. It means ethernet to token ring or FDDI or some different model or protocol instead of encapsulation.
- It needs higher layers of the OSI model, possible by layer 7, the application layer. IBM SNA, DECnet, Internet TCP/IP and other protocols can be transformed from connection to connection.
- Unlike bridges and routers, gateways work casually due to protocol conversion. Therefore, they can generate bottlenecks of the blockage during the time of peak operation.

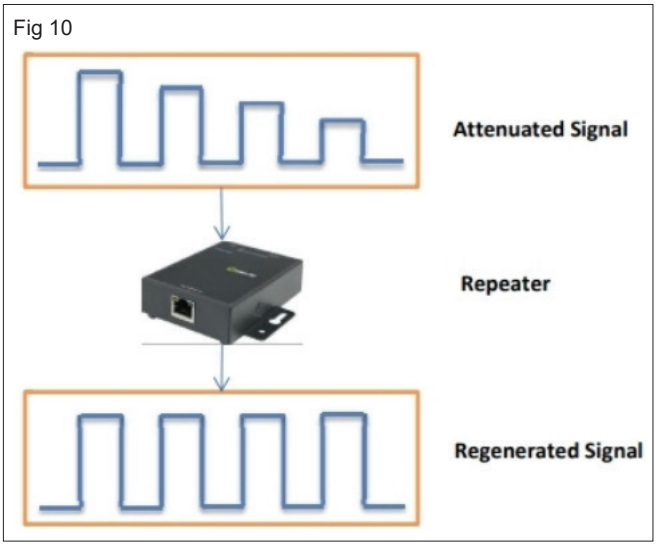
Advantages of Gateways

- It can connect the devices of two several networks having a different design.
- It is an intelligent tool with filtering capabilities.
- It has control over both collisions and the advertisement area.
- It needs a full-duplex mode of connection.
- It can make data translation and protocol conversion of the data packet according to the destination network's requires.
- It is used to encapsulate and decapsulate the data packets.
- It has enhanced security over any other network relating device.

Repeaters

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. (Fig 10)

Fig 10



When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- Analog Repeaters − They can only amplify the analog signal.
- Digital Repeaters − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- Wired Repeaters − They are used in wired LANs.
- Wireless Repeaters − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- Local Repeaters − They connect LAN segments separated by small distance.
- Remote Repeaters − They connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Transceivers

A transceiver is a combination transmitter/receiver in a single package. While the term typically applies to wireless communications devices, it can also be used for transmitter/receiver devices in cable or optical fiber systems.

The main functionality of this electronic device is to transmit, as well as receive, different signals.

In local area networks, the transceiver is a part of the network interface card. It can both transmit signals over the network wire and detect electrical signals flowing through the wire. However, some types of networks require an external transceiver.

In wireless communication devices, like smartphones and cordless telephones, the transceiver is built into the mobile device.

Access point

An access point (AP) is a term used for a network device that bridges wired and wireless networks. Consumer APs are often called a "wireless routers" because they typically also serve as both internet routers and firewalls. Commercial and industrial APs tend towards minimal network routing capabilities and rarely have firewalls.

Most APs connect wireless networks using the Wi-Fi standard; however, modern commercial and industrial APs increasingly offer support for the Bluetooth and Thread wireless standards, as well. This allows commercial and industrial APs to support both human-centric and Internet of Things (IoT) devices.

Table

Network devices summary

Device	Function/Purpose	Key points
Hub	Connects devices on a twisted-pair network	A hub does not perform any tasks besides signal regeneration.
Switch	Connects devices on a twisted-pair network	A switch forwards data to its destination by using the MAC address embedded in each packet.
Bridge	Divides networks to reduce overall network traffic	A bridge allows or prevents data from passing through it by reading the MAC address.
Router	Connects networks together	A router uses the software configured network address to make forwarding decisions.
Gateway	Translates from one data format to another	Gateways can be hardware or software based. Any device that translates data formats is called a gateway.
CSU/DSU	Translates digital signals used on a LAN to those used on a WAN	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.

Device	Function/Purpose	Key points
Network card	Enables systems to connect to the network	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
ISDN terminal adapter	Connects devices to ISDN lines	ISDN is a digital WAN technology often used in place of slower modem links. ISDN terminal adapters are required to reformat the data format for transmission on ISDN links.
WAP	Provides network capabilities to wireless network devices.	A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.
Modem	Provides serial communication capabilities across phone lines.	Modems modulate the digital signal into analog at the sending end and perform the reverse function at the receiving end.
Transceiver	Coverts one media type to another, such as UTP to fiber.	A device that functions as a transmitter and a receiver of signals such as analog or digital.
Firewall	Provides controlled data access between networks.	Firewalls can be hardware or software based and are an essential part of a networks security strategy.

IP Routing in Network RIP IGRP

It is used by routers to exchange routing data within an autonomous system. IGRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks.

Routing Information Protocol (RIP) is a distance vector protocol that uses hop count as its primary metric. RIP defines how routers should share information when moving traffic among an interconnected group of local area networks.

IGRP and RIP are close cousins: both are based on the Bellman-Ford Distance Vector (DV) algorithms. DV algorithms propagate routing information from neighbor to neighbor; if a router receives the same route from multiple neighbors, it chooses the route with the lowest metric.

RIP stands for Routing Information Protocol. OSPF stands for Open Shortest Path First. IGRP stands for Interior Gateway Routing Protocol. EIGRP stands for Enhanced Interior Gateway Routing Protocol.

IP Routing

IP Routing is refers to a set of protocols to determine the best path that an IP Packet can follow in order to travel across multiple networks from its source to its destination. The set of protocols run together at the Network Layer to help hosts and routers route IP packets. IP Routing will involve too many network devices to accomplish an IP Packet's Routing. Switches, Firewall, and Routers - all of them will be involved to Route the IP Packet.

Network layer deals with one major protocol to route packets.

Network layer defines set of functions based on one major logical protocol. There are two versions of this logical protocol where other layer 3 functions revolve. IPv4 and IPv6, both define network layer routing functions, but with different details for each. Here focuses on IPv4. Internet Protocol (IPv4), and as a Layer 3 protocol, focuses on routing or guiding the IP packets that carry the data from the upper layers as source device to the destination device using Dotted Decimal Notation - known by Logical Addressing or IP Addressing System, then IPv4 Routing handle the Packets to the Data-Link for Framing and finally physical layer for transmitting frames as bit stream.

Required components for IPv4 Routing

1 The Router itself - the Hardware Piece

2 Router Operating System - Internet Operating System (IOS)

3 IP Addressing System based on Dotted Decimal Notation

4 Routing Protocols - such OSPF or EIGRP creates and maintains an Internet Road Map using IP Addressing System as reference Points

Now, Routers can guide what called "IP Packet" to reach its final destination is using an Internet Road Map built by OSPF or EIGRP using IPv4 Addressing System.

IP Routing vs GPS Routing

If GPS Routing Guides Human to drive from point A to point B, then IP Routing Guides Routers to Route IP Packets from point A to point B. If Human understand how to use GPS Road Map, then Routers running Routing Protocols such OSPF or EIGRP understand how to use Internet Road Map.

Routing Protocols

Create, maintain, and present to the Router an Internet Road Map using IP Addressing System similar to GPS Map Reference Points. Every Router loaded with the required components understand IP Routing Internet

MAP. Routers can be dedicated Hardware like Cisco or Software base running in Linux box using the same exact Routing Protocols to create, maintain, and present Internet MAP for the Router to use.

A Road MAP system like GPS device won't really care which method you would use to reach point B, rather, it cares how to represent the right and the closest path to reach point B; it's up to you to choose which moving method to use, you can walk, fly, ride a bus, car, or train, hence, different Layer! So, Network Layer uses a Universal logical Protocol called either IPv4 or IPv6 to manage the IP Addressing System; Routing Protocols in the other hand such OSPF and EIGRP Create and Maintain an Internet Road MAP using the IP Addressing System as Reference Points called: Public IP Addresses.

IPv4 or IPv6 logical addresses are used to route packets from point A to point B across different types of networks regardless of their physical structure type. Imagine that your job is to route people from point A to point B as tourist guide, what will always concern you the most is your MAP accuracy and not how the people will be riding or walking from point A to Point B. There will be another guy (A Data-Link Protocol) who would instruct the tourist to dress special shoes maybe at certain areas and to ride a special car maybe (Physical Cabling) to tour around special Mountain areas.

Finally IPv4 manage Logical Addressing or IP Addressing combined with Routing Protocols such OSPF or EIGRP is similar to GPS System combined with Satellite geographical reference points, but it guides IP Packets instead of Humans.

How routers pick the best route from their IP routing table?

Router's logic uses a database table called IP Routing Table, to route Packets from Public IP Address to another Public IP Address, or from Network to Network; the routing table lists IP addresses as groups or blocks, called IP Networks (referring to Classful Addressing) or IP Subnets (referring to Classless Addressing) and some of these addresses were directly learned due to directly and physically connected Networks, and some were learned using Dynamic and Multicasting Routing Protocols such OSPF or EIGRP.

IP routing table can be filled as follows:

1 **Static Route Entries:** Routing tables can be filled manually by the Network Engineer.

2 **Directly Connected Route Entries:** Physically connected links entries automatically get populated by the router once you configure the IP address on the interface.

3 **Dynamic Route Entries:** Routing Protocol such OSPF or EIGRP is used to shout and inform all neighbors' routers about its directly connected routes

*One of the main and major jobs of the any Routing Protocol is: to dynamically shout and Multicast the physically connected routes to other routers, so they can fill their Routing Table with Entries to build an Internet MAP.

RIP overview

Routing Information Protocol uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. Cisco IOS software sends routing information updates every 30 seconds, which is termed advertising. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

The Cisco implementation of RIP Version 2 supports plain text and Message Digest 5 (MD5) authentication, route summarization, classless inter domain routing (CIDR), and variable-length subnet masks (VLSMs).

RIP routing updates

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a RIP routing update that includes changes to an entry, the router updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting RIP routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

Classes of IP Addressing and VLAN

Objectives: At the end of this lesson you shall be able to
- **define TCP/IP, FTP, Telnet protocols**
- **classes of IP Addressing (IPV4 and IPV6)**
- **overview of Virtual LAN**
- **concept of Translator Gateways.**

Protocols

Network protocols are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely. Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.

TCP/IP

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP is a set of standardized rules that allow computers to communicate on a network such as the internet.

TCP/IP is a data link protocol used on the internet to let computers and other devices send and receive data.

TCP/IP Utilities

The TCP/IP protocol suite includes a network/node address structure, tools for static and dynamic address assignment, name resolution services, and utilities for testing and configuration. TCP/IP utilities offer network connections to other computers, such as UNIX workstations. You must have the TCP/IP network protocol installed to use the TCP/IP utilities. Many utilities are available to troubleshoot TCP/IP connectivity problems. Most utilities are public domain and are included with the TCP/IP protocol stack provided with the operating system that you are using. This also means that the utilities may vary slightly depending on the operating system being used. For example, to view your TCP/IP setting on a Windows Server you would use “ipconfig”, whereas on a Linux box you would use “ifconfig”-each of which may support different command-line switches. Although these utilities generally provide very basic functions, they will prove to be helpful when troubleshooting network problems.

Some important TCP/IP utilities

Ping

The ping (packet Internet groper) command is used to verify the network connectivity of a computer. Ping checks the host name, IP address, and that the remote system can be reached. Ping uses the ICMP (Internet Control Message Protocol) ECHO_REQUEST datagrams to check connections between hosts by sending an echo packet, then listening for the reply packets. This command is used to test a machine’s connectivity to another system and to verify that the target system is active. Usually, using this command is the first step to any troubleshooting if a connectivity problem is occurring between two computers. This can quickly help you to determine whether a remote host is available and responsive.

Also a great way to verify whether you have TCP/IP installed and your Network Card is working.

We’ll start by Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.

Type : PING 127.0.0.1

Using Ping

- If you are using Windows NT/2000, go to the command prompt by selecting Start | Run and then type CMD. If you are using Windows 95/98/ME, go to Start | Run, and type COMMAND.
- At the command prompt, type: ping <ip address>. In this example we are pinging the IP address of 117.194.0.24
- You will get four replies back from the ping message if the system you have pinged is up and running, as shown next.
- To test your TCP/IP software stack, you can ping the loopback address by typing ping 127.0.0.1.
- If you receive four lines of information showing successes, the TCP/IP protocol is initialized and functioning. Four lines of failed transmissions will show that TCP/IP is not initialized and cannot be used to perform network transmissions. The results of a successful ping to 127.0.0.1 are shown below.

Tracert

The tracert (or traceroute) utility determines the route data takes to get to a particular destination. The ICMP protocol sends out Time Exceeded messages to each router to trace the route. Each time a packet is sent, the time-to-live (TTL) value is reduced before the packet is forwarded. This allows TTL to count how many hops it is to the destination.

For finding more options for “tracert” type “tracert /?” windows command. In unix system “traceroute” is the command instead of “tracert”. To know about traceroute type “man traceroute” in the console of unix system.

Nslookup

Nslookup utility is used to test and troubleshoot domain name servers. Nslookup has two modes. Interactive mode enables you to query name servers for information about hosts and domains, or to print a list of hosts in a domain. Non- interactive mode prints only the name and requested details for one host or domain. Non-interactive mode is useful for a single query.

To enter the interactive mode of Nslookup, type Nslookup without any arguments at a command prompt, or use only a hypen as the first argument and specify a domain name server in the second. The default DNS name server will be used if you don't enter anything for the second argument.

To use non-interactive mode, in the first argument, enter the name or IP address of the computer you want to look up. In the second argument, enter the name or IP address of a domain name server. The default DNS name server will be used if you don't enter anything for the second argument.

Nslookup works equally well in UNIX. Find out in the man page of UNIX about the command.

Ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

Among many parameters of this command three commands are very important:-

1 /all

2 /release[adapter]

3 /renew [adapter]

For /all, Ipconfig displays all of the current TCP/IP configuration values, including the IP address, subnet mask, default gateway, and Windows Internet Naming Service (WINS) and DNS configuration.

For /release and /renew, if no adapter name is specified, the IP address leases for all adapters that are bound to TCP/IP are released or renewed.

Both /renew and /release options only work on clients configured for dynamic (DHCP) addressing.

Telnet

Telnet is a network protocol used to virtually access a computer and provide a two-way, collaborative and text-based communication channel between two machines.

It follows a user command TCP/IP networking protocol that creates remote sessions. On the web, HTTP and File Transfer Protocol (FTP) enable users to request specific files from remote computers. With Telnet, users can log on as a regular user with privileges that allow them to access the specific applications and data on that computer.

IPv4 vs IPv6

IP

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

- IPv4
- IPv6

IPv4

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, 66.94.29.13

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

IPv6

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

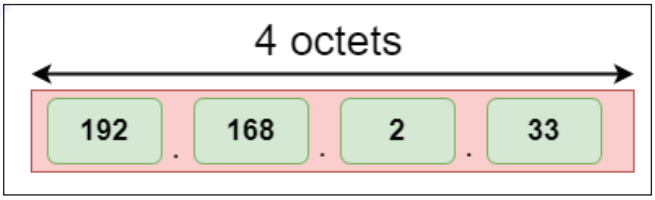
- **Dual stacking**: It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- **Tunneling**: In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation**: The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4*1038) addresses.

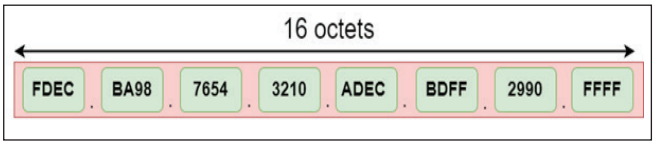
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Virtual LAN (VLAN)

A Local Area Network (LAN) was originally defined as a network of computers located within the same area. Today, Local Area Networks are defined as a single broadcast domain. This means that if a user broadcasts information on his/her LAN, the broadcast will be

received by every other user on the LAN. Broadcasts are prevented from leaving a LAN by using a router. The disadvantage of this method is routers usually take more time to process incoming data compared to a bridge or a switch. More importantly, the formation of broadcast domains depends on the physical connection of the devices in the network. Virtual Local Area Networks (VLAN's) were developed as an alternative solution to using routers to contain broadcast traffic.

In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network.

The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area.

Advantages of VLAN

VLAN's offer a number of advantages over traditional LAN's. They are:

1 Performance

In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations. For example, in a broadcast domain consisting of 10 users, if the broadcast traffic is intended only for 5 of the users, then placing those 5 users on a separate VLAN can reduce traffic.

Compared to switches, routers require more processing of incoming traffic. As the volume of traffic passing through the routers increases, so does the latency in the routers, which results in reduced performance. The use of VLAN's reduces the number of routers needed, since VLAN's create broadcast domains using switches instead of routers.

2 Formation of virtual workgroups

Nowadays, it is common to find cross-functional product development teams with members from different departments such as marketing, sales, accounting, and research. These workgroups are usually formed for a short period of time. During this period, communication between members of the workgroup will be high. To contain broadcasts and multicasts within the workgroup, a VLAN can be set up for them. With VLAN's it is easier to place members of a workgroup together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together.

However, virtual workgroups do not come without problems. Consider the situation where one user of the workgroup is on the fourth floor of a building, and the other workgroup members are on the second floor. Resources such as a printer would be located on the second floor, which would be inconvenient for the lone fourth floor user.

Another problem with setting up virtual workgroups is the implementation of centralized server farms, which are essentially collections of servers and major resources for operating a network at a central location. The advantages here are numerous, since it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building. Centralized server farms can cause problems when setting up virtual workgroups if servers cannot be placed on more than one VLAN. In such a case, the server would be placed on a single VLAN and all other VLAN's trying to access the server would have to go through a router; this can reduce performance.

3 Simplified Administration

Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Every time a user is moved in a LAN, re-cabling, new station addressing, and reconfiguration of hubs and routers becomes necessary. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated. However the full power of VLAN's will only really be felt when good management tools are created which can allow network managers to drag and drop users into different VLAN's or to set up aliases.

Despite this saving, VLAN's add a layer of administrative complexity, since it now becomes necessary to manage virtual workgroups.

4 Reduced Cost

VLAN's can be used to create broadcast domains which eliminate the need for expensive routers.

5 Security

Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion.

VLAN's working

When a LAN bridge receives data from a workstation, it tags the data with a VLAN identifier indicating the VLAN from which the data came. This is called explicit tagging. It is also possible to determine to which VLAN the data received belongs using implicit tagging. In implicit tagging the data is not tagged, but the VLAN from which the data came is determined based on other information like the port on which the data arrived. Tagging can be based on the port from which it came, the source Media Access Control (MAC) field, the source network address, or some other field or combination of fields. VLAN's are classified based on the method used. To be able to do the tagging of data using any of the methods, the bridge would have to keep an updated database containing a mapping between VLAN's and whichever field is used for tagging. For example, if tagging is by port, the database should indicate which ports belong to which VLAN. This database is called a filtering database. Bridges would have to be able to maintain this database and also to make sure that all the bridges on the LAN have the same information in each of their databases. The bridge determines where the data is to go next based on normal LAN operations. Once the bridge determines where the data is to go, it now needs to determine whether the VLAN identifier should be added to the data and sent. If the data is to go to a device that knows about VLAN implementation (VLAN-aware), the VLAN identifier is added to the data. If it is to go to a device that has no knowledge of VLAN implementation (VLAN-unaware), the bridge sends the data without the VLAN identifier.

In order to understand how VLAN's work, we need to look at the types of VLAN's, the types of connections between devices on VLAN's, the filtering database which is used to send traffic to the correct VLAN, and tagging, a process used to identify the VLAN originating the data.

VLAN Standard: IEEE 802.1Q Draft Standard

There has been a recent move towards building a set of standards for VLAN products. The Institute of Electrical and Electronic Engineers (IEEE) is currently working on a draft standard 802.1Q for VLAN's. Up to this point, products have been proprietary, implying that anyone wanting to install VLAN's would have to purchase all products from the same vendor. Once the standards have been written and vendors create products based on these standards, users will no longer be confined to purchasing products from a single vendor. The major vendors have supported these standards and are planning on releasing products based on them.

Types of VLAN's

VLAN membership can be classified by port, MAC address, and protocol type.

1 Layer 1 VLAN: Membership by Port

Membership in a VLAN can be defined based on the ports that belong to the VLAN. For example, in a bridge with four ports, ports 1, 2, and 4 belong to VLAN 1 and port 3 belongs to VLAN 2 (Table 1).

Table 1

Assignment of ports to different VLAN's

Port	VLAN
1	1
2	1
3	2
4	1

The main disadvantage of this method is that it does not allow for user mobility. If a user moves to a different location away from the assigned bridge, the network manager must reconfigure the VLAN.

2 Layer 2 VLAN: Membership by MAC Address

Here, membership in a VLAN is based on the MAC address of the workstation. The switch tracks the MAC addresses which belong to each VLAN (Table 2). Since MAC addresses form a part of the workstation's network interface card, when a workstation is moved, no reconfiguration is needed to allow the workstation to remain in the same VLAN. This is unlike Layer 1 VLAN's where membership tables must be reconfigured.

Table 2

Assignment of MAC addresses to different VLAN's

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task. Also, in environments where notebook PC's are used, the MAC address is associated with the docking station and not with the notebook PC. Consequently, when a notebook PC is moved to a different docking station, its VLAN membership must be reconfigured.

3 Layer 2 VLAN: Membership by Protocol Type

VLAN membership for Layer 2 VLAN's can also be based on the protocol type field found in the Layer 2 header (Table 3).

Table 3

Assignment of protocols to different VLAN's

Protocol	VLAN
IP	1
IPX	2

4 Layer 3 VLAN: Membership by IP Subnet Address

Membership is based on the Layer 3 header. The network IP subnet address can be used to classify VLAN membership (Table 4).

Table 4

Assignment of IP subnet addresses to different VLAN's

IP Subnet	VLAN
23.2.24	1
26.21.35	2

Although VLAN membership is based on Layer 3 information, this has nothing to do with network routing and should not be confused with router functions. In this method, IP addresses are used only as a mapping to determine membership in VLAN's. No other processing of IP addresses is done.

In Layer 3 VLAN's, users can move their workstations without reconfiguring their network addresses. The only problem is that it generally takes longer to forward packets using Layer 3 information than using MAC addresses.

5 Higher Layer VLAN's

It is also possible to define VLAN membership based on applications or service, or any combination thereof. For example, file transfer protocol (FTP) applications can be executed on one VLAN and telnet applications on another VLAN.

The 802.1Q draft standard defines Layer 1 and Layer 2 VLAN's only. Protocol type based VLAN's and higher layer VLAN's have been allowed for, but are not defined in this standard. As a result, these VLAN's will remain proprietary.

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP is available on most of the Cisco Catalyst Family products. Using VTP, each Catalyst Family Switch advertises the following on its trunk ports:

- Management domain
- Configuration revision number
- Known VLANs and their specific parameters

There are three versions of VTP, namely version 1, version 2, version 3.

The comparable IEEE standard in use by other manufacturers is GVRP or the more recent MVRP.

On Cisco Devices, VTP (VLAN Trunking Protocol) maintains VLAN configuration consistency across a single Layer 2 network. VTP uses Layer 2 frames to manage the addition, deletion, and renaming of VLANs from switches in the VTP client mode. VTP is responsible for synchronizing VLAN information within a VTP domain and reduces the need to configure the same VLAN information on each switch thereby minimizing the possibility of configuration inconsistencies that arise when changes are made.

Advantages

VTP provides the following benefits:

- VLAN configuration consistency across the layer 2 network
- Dynamic distribution of added VLANs across the network
- Plug-and-play configuration when adding new VLANs

Disadvantages

When a new switch is added to the network, by default it is configured with no VTP domain name or password, but in VTP server mode. If no VTP Domain Name has been configured, it assumes the one from the first VTP packet it receives. Since a new switch has a VTP configuration revision of 0, it will accept any revision number as newer and overwrite its VLAN information if the VTP passwords match. However, if you were to accidentally connect a switch to the network with the correct VTP domain name and password but a higher VTP revision number than what the network currently has (such as a switch that had been removed from the network for maintenance and returned with its VLAN information deleted) then the entire VTP Domain would adopt the VLAN configuration of the new switch which is likely to cause loss of VLAN information on all switches in the VTP Domain, leading to failures on the network. Since Cisco switches maintain VTP configuration information separately from the normal configuration and since this particular issue occurs so frequently, it has become known colloquially as the "VTP Bomb".

Before creating VLANs on the switch that will propagate via VTP, a VTP domain must first be set up. A VTP domain for a network is a set of all contiguously trunked switches with the matching VTP settings (domain

name, password and VTP version). All switches in the same VTP domain share their VLAN information with each other, and a switch can participate in only one VTP management domain. Switches in different domains do not share VTP information. Non-matching VTP settings might result in issues in negotiating VLAN trunks, port-channels or Virtual Port Channels.

Translater gateways

Computers require very precise, rigidly defined rules or protocol for successful communication. Even slight variations can render communication impossible. In order for two computers using different protocols to communicate, some kind of translation must take place. The device that performs this translation is called a gateway.

What are the gateways?

The link between two computers to connect to internet or another network is called gateway. The gateway works like a portal among two programs by means of communications between protocol and permit them to share data on same computers or among different computers. Gateways are also known as protocol converter that can perform at any OSI model layer. The task of a gateway is very complex as compared to router and switch.

Gateway benefits and limitations

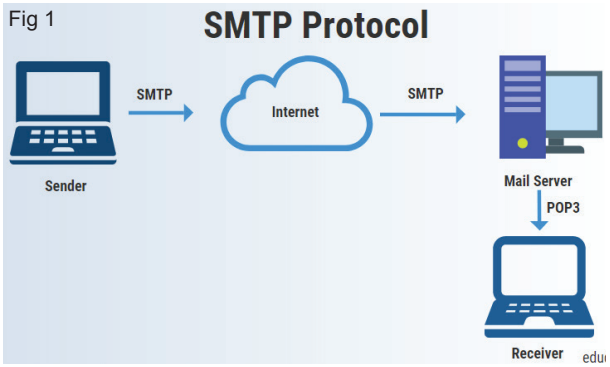
Gateway Benefits	Gateway Limitations
Provides connectivity that may otherwise be impossible	• Limited capacity and expandability. • Limited ability to translate dissimilar concepts.
May expand options for competitive bidding	• Configuration and programming of devices through the gateway is generally not possible.
Provides a point of isolation between two largely independent systems	• Failure results in communication loss between all devices on opposite sides of the gateway.
Permits interconnection of legacy systems with newer products	• Possible time delay or the return of cached data that is old. • More difficult to troubleshoot problems.

Network Protocols

Objectives: At the end of this lesson you shall be able to
- **define network protocols (SMTP, FTP, HTTP, POP, SNMP, LDAP & DHCP)**
- **define network security.**

SMTP (Fig 1)

Fig 1

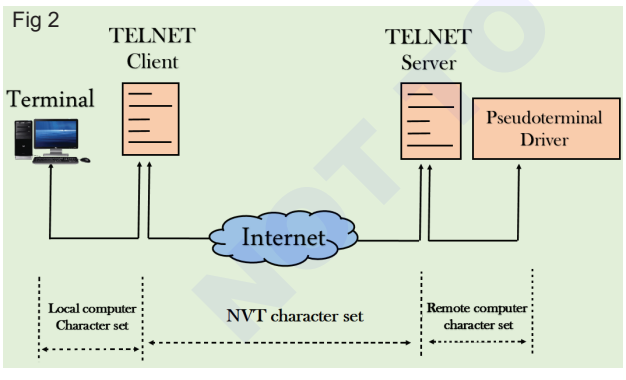


SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving email. SMTP is used most commonly by email clients, including Gmail, Outlook, Apple Mail and Yahoo Mail.

SMTP can send and receive email, but email clients typically use a program with SMTP for sending email. Because SMTP is limited in its ability to queue messages at the receiving end, it's usually used with either Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP), which lets the user save messages in a server mailbox and download them periodically from a server. SMTP is typically limited to and relied on to send messages from a sender to a recipient.

TELNET (Fig 2)

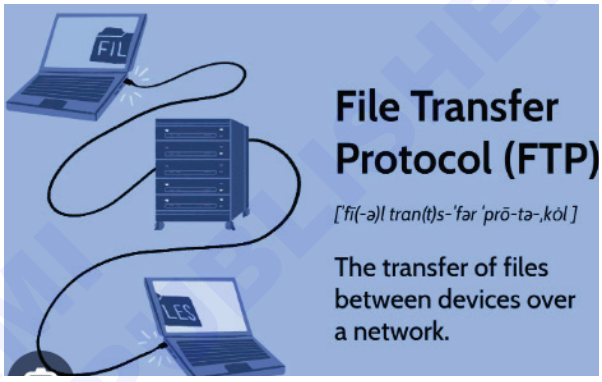
Fig 2



Telnet is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the internet). Using telnet client software on your computer, you can make a connection to a telnet server (that is, the remote host). Once your telnet client establishes a connection to the remote host, your client becomes a virtual terminal, allowing you to communicate with the remote host from your computer. In most cases, you'll need to log into the remote host, which requires that you have an account on that system. Occasionally, you can log in as guest or public without having an account.

FTP (Fig 3)

Fig 3

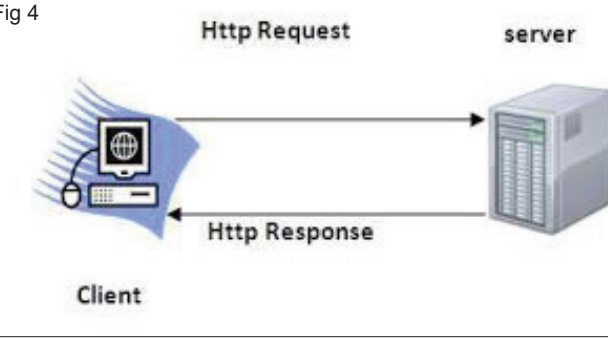


FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files from one host to another over a TCP-based network, such as the Internet. FTP works by opening two connections that link the computers trying to communicate with each other.

There are a few cases in which you'll want to rely on FTP: Transferring large files. FTP is often used to transfer files that are too large to send via email or other means. Transferring files between servers.

HTTP (Fig 4)

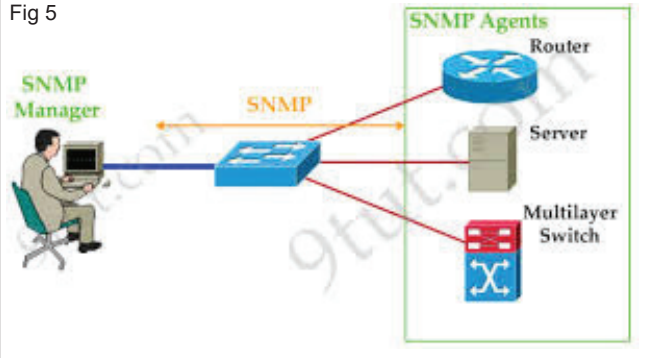
Fig 4



The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.

SNMP (Fig 5)

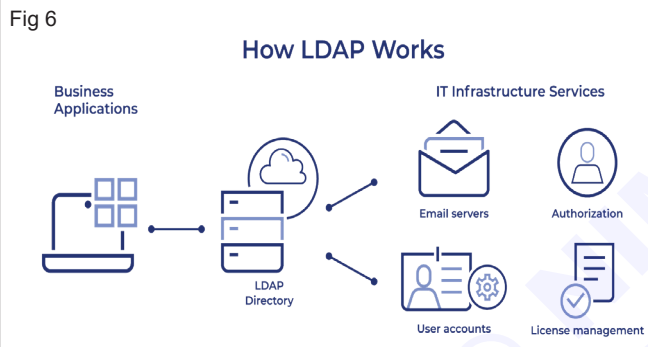
Fig 5



Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP. SNMP is used for communication between routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices.

LDAP (Fig 6)

Fig 6



Lightweight directory access protocol (LDAP) is a protocol that helps users find data about organizations, persons, and more. LDAP has two main goals: to store data in the LDAP directory and authenticate users to access the directory.

DHCP (Fig 7)

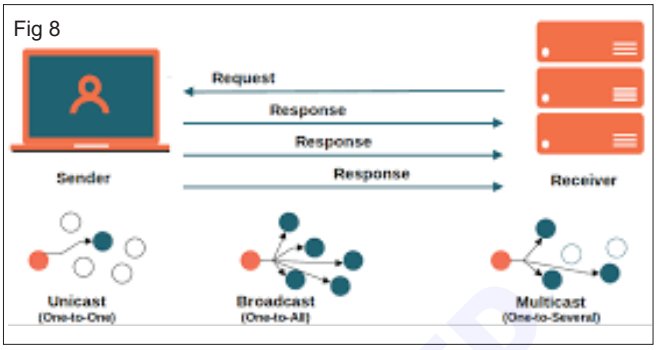
Fig 7

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP.

UDP (Fig 8)

Fig 8

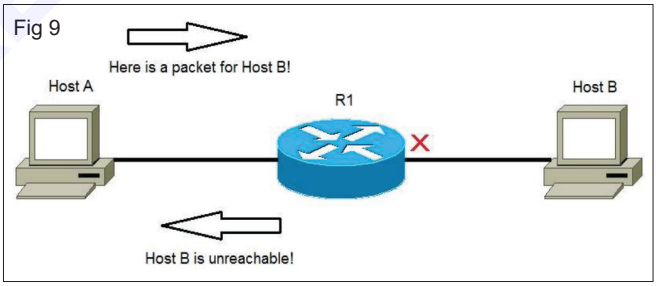


User Datagram Protocol (UDP) is a communications protocol for time-sensitive applications like gaming, playing videos, or Domain Name System (DNS) lookups. UDP results in speedier communication because it does not spend time forming a firm connection with the destination before transferring the data.

The main difference between TCP (transmission control protocol) and UDP (user datagram protocol) is that TCP is a connection-based protocol and UDP is connectionless. While TCP is more reliable, it transfers data more slowly. UDP is less reliable but works more quickly.

Internet Control Message Protocol (ICMP) (Fig 9)

Fig 9

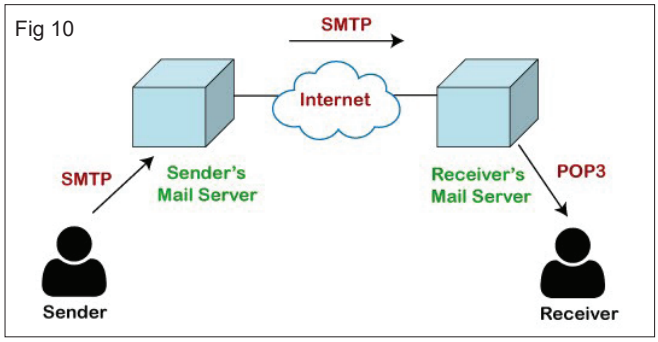


The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. It is assigned protocol number 1.

ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and trace route).

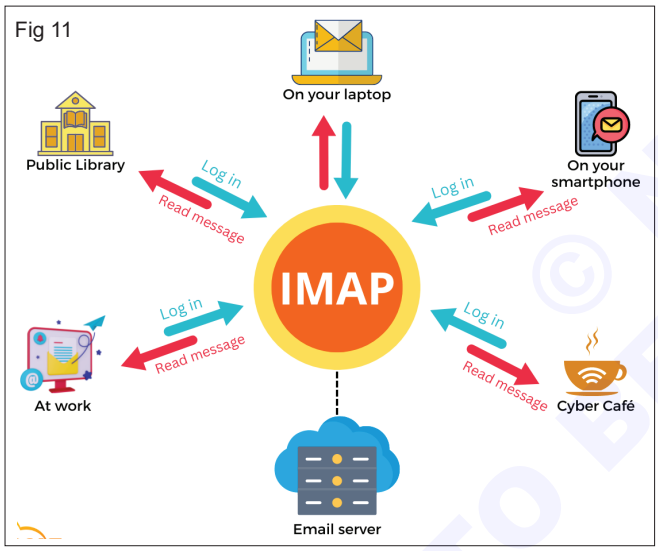
ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6.

Post Office Protocol (POP) (Fig 10)



Post Office Protocol (POP) is an application-layer Internet standard protocol used by locale-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP and IMAP (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both. The POP protocol has been developed through several versions, with version 3 (POP3) being the current standard. Most Webmail service providers such as Hotmail, Gmail and Yahoo! Mail also provide IMAP and POP3 service.

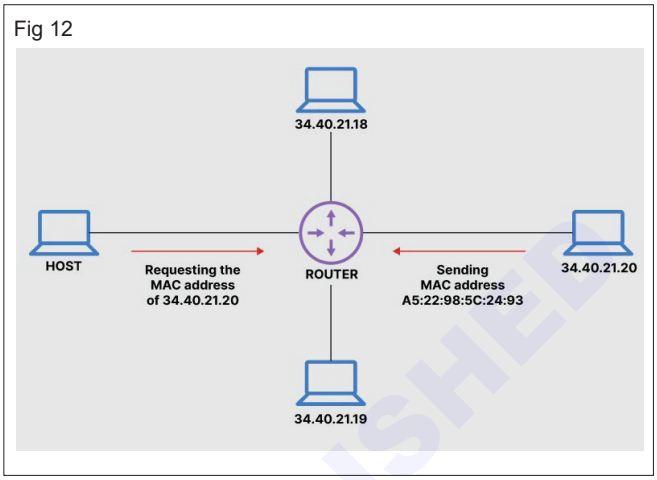
Internet Message Access Protocol (IMAP) (Fig 11)



Internet message access protocol (IMAP) is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the Post Office Protocol (POP). Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server.

The Internet Message Access Protocol (commonly known as IMAP) is an Application Layer Internet protocol that allows a client to access e-mail on a remote mail server. The current version, IMAP version 4 revision 1 (IMAP4rev1), is defined by RFC 3501. An IMAP server typically listens on well-known port 143. IMAP over SSL (IMAPS) is assigned well-known port number 993.

ARP - Address Resolution Protocol (Fig 12)



It refers to the protocol itself and the command line utility used to view and manipulate the ARP cache. It is the means by which IP addresses are mapped to MAC addresses. ARP builds and maintains a table called the ARP cache which retains these mappings.

RARP - Reverse ARP

It is used by a computer to obtain its own IP address.

ARP is also a command line utility provided with both UNIX/Linux and Windows implementations of TCP/IP

Network Security

Network security is a set of technologies that protects the usability and integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats.

Three basic security concepts important to information on the internet are confidentiality, integrity, and availability.

Internet security refers to security designed to protect systems and the activities of employees and other users while connected to the internet, web browsers, web apps, websites, and networks. Internet security solutions protect users and corporate assets from cybersecurity attacks and threats.

Concept of Internet and Social Networking

Objectives: At the end of this lesson you shall be able to
- **concept of internet, DNS server, social networking, video calling, video conferencing, UTM and firewall**
- **architecture of internet and internet access techniques.**

Internet

The Internet is the world wide system of interconnected computer networks that use the Internet protocol suite TCP/IP to link crores and crores of devices worldwide by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a wide range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

The main difference between the Internet and a corporate or group network, is that all the small networks that make up the Internet are linked, but corporate networks are kept private. To access the Internet, the network that is connected to the Internet has to be accessed. These networks are run by Internet service providers (ISPs), In order to get connected to the Internet, the following should be done:

1 Connect the computer to the ISP's network by using a communication device, such as a modem or router.

2 The ISP connects its network to its provider's network by using a router and a communication link, such as a leased Telecom line.

3 Finally, a connection is made to a part of the Internet backbone, which allows connections to every network that is connected to the Internet.

Internet Protocols

A protocol is a set of standards or conventions that are followed when formatting data to be used for electronic communications.

Internet Access methods

1 Dial-up

2 Cable

3 DSL

4 ISDN

5 T1/T3

6 Fiber

7 Satellite

8 Wireless

9 Line-of-sight wireless Internet service

10 Cellular (mobile hotspot)

11 WiMax

Dial-up Connection

Dial-up connection provides connection to Internet through a dial-up terminal connection. The computer, which provides Internet access is known as 'Host' and the computer that receives the access, is 'Client' or 'Terminal'. The client computer uses modem to access a "host" and acts as if it is a terminal directly connected to that host. In dial-up connection to Internet, Host carries all the command that are typed on a client machine and forward them to Internet. It also receives the data or information from the Internet on behalf of the 'Client' and passes it to them.

To access dial-up accounts the following is needed;

1 Computer

2 Modem

3 Telephone Connection

4 Account from the ISP

5 Internet browser

Cable Modem Connection

A cable modem is a type of Network Bridge and modem that provides bi-directional data communication via radio frequency channels. Cable connections implement a cable modem in the home or office that takes a digital network signal from the network card and translates (modulates) it into an analog broadband signal. This signal is then passed on to the cable network. When using cable, the data transmission is in a shared medium with other users until the connection reaches the cable company's office.

Leased Connection

Leased connection is also known as direct Internet access or Level Three connection. It is the secure, dedicated and most expensive, level of Internet connection. With leased connection, your computer is dedicatedly and directly connected to the Internet using high-speed transmission lines. It is on-line twenty-four hours a day, seven days a week.

DSL Connection

Digital Subscriber Line (DSL) provides digital data transmission over the wires of a local telephone network. The most common form of Digital Subscriber Line (DSL) is Asynchronous Digital Subscriber Line (ADSL). ADSL service is delivered simultaneously with wired telephone service on the same telephone line.

This is possible because DSL uses higher frequency bands for data separated by filtering. On the customer premises, a DSL filter on each outlet removes the high frequency interference, to enable simultaneous use of the telephone and data.

ADSL always has slower upload speeds because the connection is broken into upstream and downstream channels. The data bit rate of consumer ADSL services typically ranges from 256 kbit/s to 40 Mbit/s in the direction to the customer (downstream), depending on DSL technology, line conditions, and service-level implementation. In ADSL, the data throughput in the upstream direction, (the direction to the service provider) is lower, that is why it is known as Asymmetric service. Better speeds are possible with ADSL2+, a newer generation of ADSL connection available to those living within two kilometers of an exchange. In Symmetric Digital Subscriber Line (SDSL) services, the downstream and upstream data rates are equal.

VDSL Very-high-bitrate Digital Subscriber Line service is closer to cable Internet in speed and behavior than ADSL. It is up to five times faster for downloads and ten times faster for uploads. Maximum upload speeds is around 60 Mbps and the signal is equally strong upstream as it is downstream.

ISDN

It is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the circuits of public switched telephone network. Integrated Services Digital Network (ISDN) service comes in two basic forms: basic rate and primary rate.

Basic-rate ISDN: Uses three channels: two 64 Kbps lines for data (128 Kbps) and one 16 Kbps line as a control channel, which is used for establishing and maintaining connections. The data channels are referred to as B channels, and the control channel is referred to as a D channel.

Primary-rate ISDN: Uses twenty-three 64 Kbps B data channels (1.44 Mbps) and one 64 Kbps D channel for control information.

T1/T3

T1 and T3 are two common types of leased lines used in telecommunications. T1 connections offer transmission speeds of 1.544 Mbps over 24 pairs of wires. Each pair of wires can carry a 64 Kbps signal, called a channel. T1 connections can be implemented over copper wire.

T3 connections, on the other hand, require a better medium than copper, such as microwave or fiber optic. They are capable of speeds ranging from 6 Mbps to 45 Mbps.

Fiber

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. Internet access over fiber connections is defined in the Optical Carrier (OC) standards. There are different levels of OC, with OC3 being a common type of Internet connection for large networks as it can carry voice, video, and other data at a transfer rate of 155.52 Mbps. Fiber-to-the-home connections can have transfer rates of 150 Mbps.

Satellite

Satellite Internet services are done in two methods, one-way with terrestrial return and two-way. Because satellites providing service in most residential areas were designed to send data, the first Internet access over satellites involved downloading from the satellite, but data had to be uploaded via dialup modem. This transmission tied up phone lines, and upload speeds were rather slow. Two-way systems added technology to return a signal to the satellite. Speeds for uploads ran in the neighborhood of only 1 Mbps, but they did free up phone lines. Download speeds over satellite systems rival those of broadband services (such as ADSL and cable). Just like satellite television, satellite Internet is susceptible to the weather and elements.

Wireless

Wireless access to the Internet is provided through standard 802.11 (Wi-Fi) wireless networks, which are set up to provide coverage in prescribed areas. In some locations, wireless access is provided for free to customers of certain businesses, or by a municipal government like Fredericton, New Brunswick (www.fred-ezone.ca).Sometimes, a company may set up access points in a wide range of locations, offering access through them as part of a subscription service. These wireless access points allow connectivity but only to the company's Web site to set up an account. After you set up and pay for an account, you can use any of the company's access points to access the Internet.

Line-of-sight wireless Internet service

A line-of-sight wireless connection is typically used by a company that wants to connect two locations that are spread over a distance to a network. To connect these two locations, the company will typically place large wireless antennas on top of the buildings to allow the antennas to have a clear line-of-sight between one another with nothing in between to obstruct the wireless signal.

Cellular / Mobile Hotspot

Sometimes called wireless, 3G, or 4G, this system makes use of a cellular providers wireless network. To connect to a cellular network, a cellular modem is needed by the computer or a cellular router for the network. The cellular modem may be built into the computer, or added as a PCMCIA card or a USB adapter; some phones may even be used as a cellular modem. The benefit of this technology is that Internet can be accessed from anywhere the wireless provider has coverage.

WAN cellular

Speeds will vary with each wireless carrier, but you will see rated speeds anywhere from 384 Kbps up to 4.9 Mbps. Speeds are dependent upon the provider providing service on EDGE (Enhanced Data for GSM Evolution), High Data Rate (HDR), EV-DO (Evolution-Data Optimized, or Evolution-Data Only) or 3G (Third Generation) networks. 4G networks have began driving data speeds to new levels.

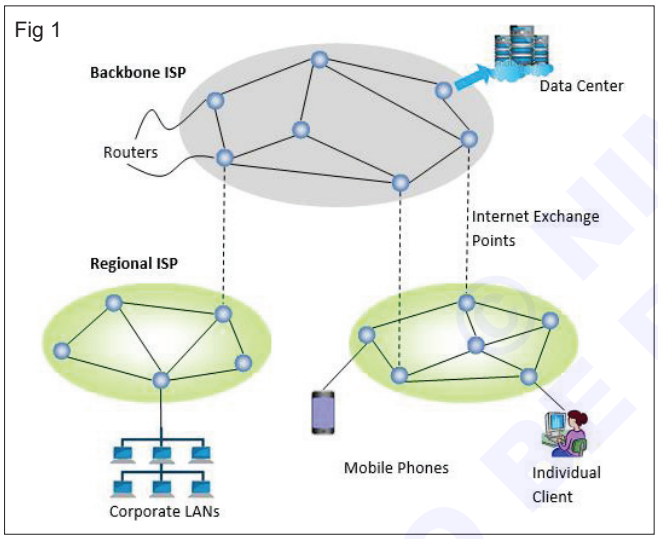
WiMax

WiMax is a wireless standard that stands for Worldwide Interoperability for Microwave Access. WiMax is a technology that is designed to cover wide areas like a cellular network, but provide the transfer rate of a wireless network.

Architecture of Internet

The architecture of the Internet is ever-changing due to continuous changes in the technologies as well as the nature of the service provided. The heterogeneity and vastness of the Internet make it difficult to describe every aspect of its architecture. (Fig 1)

Fig 1



The overall architecture can be described in three levels

1 Backbone ISP (Internet Service Provider)

2 Regional ISPs

3 Clients

The following diagram shows the three levels −

Backbone ISP (Internet Service Provider) − Backbone ISPs are large international backbone networks. They are equipped with thousands of routers and store enormous amounts of information in data centers, connected through high bandwidth fiber optic links. Everyone needs to connect with a backbone ISP to access the entire Internet.

There are different ways through which a client can connect to the ISP. A commonly used way is DSL (Digital Subscriber Line) which reuses the telephone connection of the user for transmission of digital data. The user uses a dial-up connection instead of the telephone call. Connectivity is also done by sending signals over cable TV system that reuses unused cable TV channels for data transmission. For high-speed Internet access, the connectivity can be done through FTTH (Fiber to the Home), that uses optical fibers for transmitting data. Nowadays, most Internet access is done through the wireless connection to mobile phones from fixed subscribers, who transmit data within their coverage area.

DNS Server

The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP address for those sites.

DNS, or the Domain Name System, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44). Introduction to DNS Introduction to DNS Introduction to DNS.

For example, when a Web address (URL) is typed into a browser, a DNS query is made to learn an IP address of a Web server associated with that name. Using the www.example.com URL, example.com is the domain name, and www is the hostname. DNS resolution maps www.example.com into an IP address (such as 192.0. 2.1).

Internet Access Techniques

Internet access can be provided using different broadband technologies including satellite, cable, telephone wires, wireless or mobile connections. Find out how to get internet access both in the home and outside it.

ISPs

An internet service provider (ISP) is a company that provides access to the internet. ISPs can provide this access through multiple means, including dial-up, DSL, cable, wireless and fiber-optic connections. A variety of companies serve as ISPs, including cable providers, mobile carriers, and telephone companies.

In some cases, a single company may offer multiple types of service (e.g., cable and wireless), while in other cases, a company may focus on just one type of service (e.g., fiber-optic). Without an ISP, individuals and businesses could not reach the internet and the opportunities it provides.

Typical services offered by ISPs

Internet access is the primary service offered by ISPs, but there are a variety of other services they may provide. These can include:

- **Equipment rental**: Many ISPs will rent equipment like modems and routers to their customers. This can be a convenient option for those who do not want to purchase their own equipment or do not need the latest and greatest technology.

- **Tech support**: Many ISPs offer tech support to their customers. This can be a valuable service for those unfamiliar with setting up or troubleshooting internet connections.
- **Email access**: Some ISPs offer email services to their customers. This can be a convenient way to have an email address linked to your ISP account.
- **Tiered connection plans**: ISPs typically offer different tiers of service, with different speeds and data allowances. This is a good option for those who want to pay for a higher-speed connection or who need more data than what is included in the basic package.

As a leading provider of internet service, Verizon offers a variety of services to consumers, including:

- **Fios Internet**: Fios Internet is a 100% fiber-optic network that delivers some of the fastest internet speeds to millions of homes in the mid-Atlantic and New England.
- **5G Home Internet:** 5G Home Internet is a wireless home internet service utilizing 5G Ultra Wideband technology that provides the network performance and speed you want to stream, game or work flexibly.
- **LTE Home Internet**: Verizon LTE Home is a wireless internet service that offers download speeds of 25-50 Mbps, with typical upload speeds of 4 Mbps.

It's important to note that there is a difference between Mbps and Kbps. Mbps stands for megabits per second, while Kbps stands for kilobits per second — one megabit is the equivalent of 1,000 kilobits.

A dialup service connects to the Internet through a phone line with a maximum speed of 56kbps. Broadband refers to a connection that has capacity to transmit large amount of data at high speed. Presently a connection having download speeds of 256kbps or more is classified as broadband.

Wi-Fi is a wireless connection between multiple devices and your router, and just one of the ways you can access the internet. Broadband is the actual internet connection afforded by your internet service provider (ISP), which you can access directly via a LAN or Ethernet connection between your modem and device.

Dial-up speeds don't reach over 56 kbps, which means they don't qualify as broadband or high-speed internet. This also means that dial-up internet is too slow for streaming video or audio, playing modern online games, and using video chat.

Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a connection to an Internet service provider (ISP) by dialing a telephone number on a conventional telephone line.

Social networking services are World Wide Web applications that highlight user-generated content (Web 2.0) which acts as a platform to build social networks or social relations among people who share similar personal and career interests, activities, backgrounds or real-life connections. User-generated content plays the main role in the functioning of social networking services. Some of the popular services used world wide are Facebook, Google+, LinkedIn, Instagram, Pinterest, Vine, Tumblr, and Twitter. Web 2.0 is about connecting people and making technology more efficient for people.

Social Networking

Social network services can be classified into three types:

1 Socializing social network services: mainly used for socializing with existing friends e.g., Facebook

2 Networking social network services: for non-social interpersonal communication e.g., LinkedIn

3 Social navigation social network services: primarily for helping users to find specific information or resources e.g., Goodreads for books.

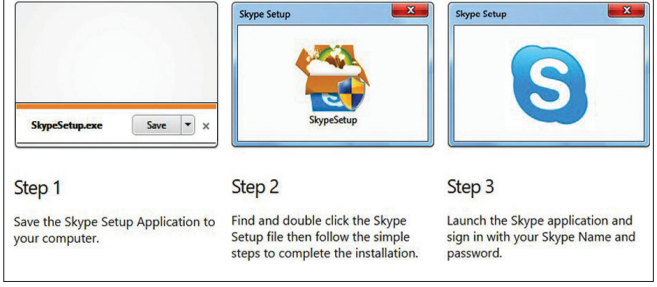
Voice over Internet Protocol (VoIP) is a form of communication that allows to make phone calls over a broadband internet connection instead of typical analog telephone lines. It uses a group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. VoIP requires a connection to the Internet through an ISP, a VoIP service to extend the reach to traditional landlines, and VoIP software to actually place calls. Examples of the VoIP protocols are:-

- Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP), Gateway Control Protocol (Megaco, H.248), Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), Secure Real-time Transport Protocol (SRTP), Session Description Protocol (SDP), Inter-Asterisk exchange (IAX), Jingle XMPP VoIP extensions, Skype protocol, TeamSpeak.

Skype is an application that provides video chat and voice call services. The name for the software is derived from "Sky peer-to-peer", which was then abbreviated to "Skype". Skype is an application that provides video chat and voice call services. The users of skype can exchange digital documents such as images, text, video and any others, and also can transmit both text and video messages. Skype allows the creation of video conference calls.

Skype can be downloaded from www.skype.com. The installation steps are given in Fig 2.

Fig 2



Registered users of Skype are identified by a unique Skype Name and are listed in the Skype directory. Skype allows these registered users to communicate through both instant messaging and voice chat. Voice chat allows telephone calls between pairs of users and conference calling. Skype's text chat client allows group chats, emoticons, storing chat history, and editing of previous messages. Skype supports conference calls, video chats, and screen sharing between 25 people at a time for free. Skype has introduced Mojis, Mojis are short clips/gifs featuring characters from films and TV shows to be entered into conversations with the same ease as emoticons.

Skype uses a proprietary Internet telephony (VoIP) network called the Skype protocol.

Google Hangouts is a communication platform developed by Google which includes instant messaging, video chat, SMS and VoIP features. Google Hangouts is used to have one-to-one or group conversations using text chat, voice or video calls. The service can be accessed online through the Gmail or Google+ websites, or through mobile apps available for Android and iOS. Users can also perform a group video chat with up to 25 concurrent users in HD video for Work/ Education.

Hangouts are used to

- Start a chat conversation or video call.
- Make phone calls using Wi-Fi or data.
- Send text messages.

To use hangouts a Google Account, a computer or phone with a camera and microphone and an internet or data connection is needed. It is recommended to use Hangouts in the Google Chrome browser. If browsers other than Google Chrome browser is used then it is necessary to install the Hangouts plugin.

Application sharing uses the internet to remotely view and control a particular software application on someone else's computer. The greatest benefit of application sharing is that a remote user can run software that isn't installed on his computer, even software that isn't compatible with his operating system or that requires much more processing power than his computer can usually handle.

Video Conferencing: Video conference is an online meeting (or a meeting over distance) that takes place between two people, where each participant can see an image of the other, and where both the people are able to speak and listen to the other participants in real time. The essential components for videoconferencing are:

- A microphone, a webcam and speakers
- A display
- A software program that captures the voice stream from the microphone, encodes it, transmits to the other participant, and simultaneously decodes the digital voice stream being received from the remote participant in the video conference (most commonly referred to as a Codec).
- A software program that bridges both parties together across a digital connection, managing the exchange of voice and video between participants. At either end of the connection, the video and voice traffic is combined and delivered to each participant in the form of a real-time video image and audio stream.
- An optional management tool for the scheduling of video conferencing sessions

Video conferencing also allows to share contents from a device during a video call.

Point-to-Point Video Conferencing: It is where one person or group is connected to another. Microphone and camera that enable the meeting to take place are usually integrated in to desktop computing solutions like a laptop or tablet, or can be combined into a separate room fitted with accessories, Desktop solutions are used by individuals. In room-based solutions utilize dedicated video conferencing technology where groups of people can participate in the meeting. (Fig 3)

Fig 3

Multi-point video conferencing: In multi-point video calls, three or more locations are connected together, where all participants can see and hear each other, as well as see any content being shared during the meeting. Here, digital information, streams of voice, video and content are processed by a central, independent software program. Combining the individual participant's video and voice traffic, the program re-sends a collective data stream back to meeting participants in the form of real-time audio and video imagery. Individuals can participate in a meeting in an "audio only" mode, or combine audio with video images of the meeting on screen. Depending upon the technical capability of the video conferencing system being used, images seen by participants are either classified as "active speaker" or "continuous presence."

In "active speaker" mode, the screen only provides an image of the person that is speaking at any point in time. In more advanced solutions with "continuous presence" mode, the bridge divides the image on the screen into a number of different areas. (Fig 4)

Fig 4

The person speaking at any point in time is presented in a large central area, and other meeting participants are shown displayed around the central image.

The "continuous presence" mode thus allows meeting participants to view and interact with all meeting participants in a 'virtual meeting room.'

The software program which creates the "virtual meeting room" and the digital processing hardware on which it resides, is often called a video bridge, or "bridge", for short. Another term for a bridge which is often used is a video conferencing "multi-point control unit" or "MCU." An MCU must be able to create, control and facilitate multiple simultaneous live video conferencing meetings. To link these users into a common, virtual meeting, the MCU must therefore be able to understand and translate between several different protocols (i.e. H.264 for communication over IP, and H.263 for ISDN). The MCU will also allow those joining the video bridge to do so at the highest speed and the best possible quality that their individual system can support. Although there are two separate processes taking place here, this is often jointly referred to as "transcoding."

H.263 is a video compression standard originally designed as a low-bit-rate compressed format for videoconferencing.

H.264 or MPEG-4 Part 10, Advanced Video Coding (MPEG-4 AVC) is one of the most commonly used formats for the recording, compression, and distribution of video content. It is widely used for streaming internet videos from YouTube, and web software such as the Adobe Flash Player and Microsoft Silverlight, and also for HDTV broadcasts over cable and satellite.

Microsoft NetMeeting is a VoIP and multi-point videoconferencing client which was included in many versions of Microsoft Windows. It uses the H.323 protocol for videoconferencing and supports 30 frames per second. Microsoft Netmeeting helps to hold face-to-face conversations with friends and family, and collaborate with co-workers around the world. Features include: Video and Audio conferencing Whiteboard, which lets the user to collaborate in real time with others via graphic information, Text chat, File transfer, Program sharing, Remote desktop sharing, which lets the user to operate a computer from a remote location Advanced calling features Microsoft Internet Directory, which is a Web site provided and maintained by Microsoft to locate people to call on the Internet. NetMeeting has been discontinued and is no longer included with Microsoft Windows.

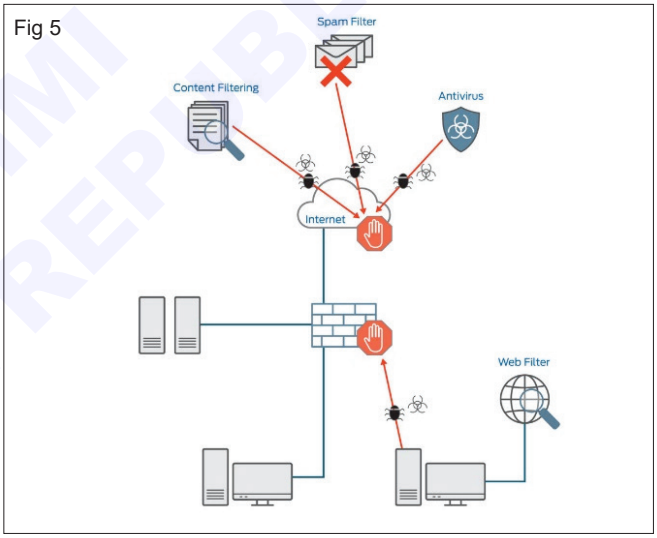
Video Calling

Video call made via a mobile phone with a camera and a screen, allowing the participants to see each other as they talk. Video calling an act or instance of communicating with one or more people using a smartphone, mobile device, webcam, etc., to transmit and receive both audio and video. Video calling allows you to directly call one other person and talk exclusively to them via their direct number or another identifier. Video conferencing allows multiple participants to call in to the same virtual meeting, using a designated number or access code created specifically for that meeting.

Video calling gives team members the ability to see colleagues' or customers' faces during a call, providing many advantages over traditional audio-only calls. It can provide a more personal venue for communication between remote team members or clients who don't have the ability to meet in-person.

UTM and Firewall (Fig 5)

Fig 5



UTM enables an organization to consolidate their IT security services into one device, potentially simplifying the protection of the network. As a result, your business can monitor all threats and security-related activity through a single pane of glass.

Originally called unified threat management (UTM), these capabilities better known as a Next-Generation Firewall (NGFW) today, provide multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way. NGFW includes functions such as anti-virus, anti-spam, content filtering, and web filtering.

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Wired & Wireless Networks

Objectives: At the end of this lesson you shall be able to
- **collaborating using wired and wireless networks**
- **protecting a network and network performance.**

Wired and Wireless Networks

The two types of connections for networks are wired or wireless. A wired connection uses cables such as electrically conducting copper cables, to connect devices together. A wireless network connect together devices through different frequencies of electromagnetic radiation instead.

Network

As we all know, “wired” refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.

There are three major types of wired connection: Twisted Pair. Coaxial Cable. Fiber Optic Cable.

Wireless Network

“Wireless” means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite disc receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

Wireless Local Area Networks (WLAN) are the most widely-used form of the wireless network. WLANs are frequently found in homes, offices, coffee shops and airports to provide wireless Internet access for devices such as laptops, smartphones and tablets. WLANs utilize wireless routers to connect devices to the internet.

Network security is defined as the process of creating a strategic defensive approach that secures a company’s data and its resources across its network. It protects the organization against any form of a potential threat or unauthorized access.

Network protection

While it is common for organizations to recognize the need to secure their networks, many still struggle with knowing what steps to take or where to start.

1 Implement a firewall

A firewall acts as a barrier between your network and the outside world, as it monitors incoming and outgoing network traffic. Deploying a firewall will enable your organization to filter and block unauthorized access attempts.

By defining strict rules for the firewall, you can control the types of traffic allowed into your network, reducing the risk of malicious intrusions.

Implementing a firewall also involves regular firewall audits to ensure it remains effective. This can be achieved using firewall audit software, which can automatically review, analyze, and signal potential weaknesses in firewalls.

2 Use strong passwords

One of the simplest ways to enhance network security is by using strong passwords. Weak passwords are vulnerable to brute-force attacks and can be easily cracked by malicious actors.

Implement a password policy across your organization that enforces complex passwords containing a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, encourage regular password updates to prevent unauthorized access.

A password management service can help enforce better password hygiene across the organization.

3 Enable two-factor authentication (2FA)

In addition to enforcing a strong password policy, organizations should implement 2FA wherever possible. Also known as multifactor authentication (MFA), 2FA provides an extra layer of security by requiring users to provide two forms of identification to access the network.

By enabling 2FA or MFA, even if passwords are compromised, unauthorized access can be significantly mitigated.

4 Regularly update software and firmware

Software and firmware updates often contain patches and security fixes that address vulnerabilities in the system. Regularly update all network devices, including routers, switches, firewalls, and servers, with the latest security patches.

Additionally, ensure that all software and applications used on networked devices are up to date, as attackers can exploit outdated software.

5 Use virtual private networks (VPNs)

When accessing your network remotely or connecting to public Wi-Fi, using a VPN is crucial to secure your data transmission. VPNs encrypt your network traffic, making it difficult for hackers to intercept and decipher sensitive information.

Keep in mind that VPNs can come in all shapes, sizes, and security levels. Look at the best VPN service providers and make sure that your preferred service can meet your unique network security needs.

6 Employ intrusion detection and prevention systems (IDPS)

IDPS solutions monitor network traffic for malicious activities and can detect and prevent unauthorized access attempts or attacks. These systems can provide real-time alerts and take automated actions to mitigate potential security threats.

Deploying an IDPS adds an extra layer of defense against network intrusions and helps maintain network integrity.

Main components of a secure network?

A secure network comprises various components that work together to protect data and systems from unauthorized access and cyber threats. Some of the key components include routers and switches, firewalls, IDPSs, and VPNs.

Secure routers and switches

Routers and switches are critical components that enable network connectivity. Secure routers and switches incorporate features like access control lists (ACLs) and encryption to protect the network traffic and prevent unauthorized access to sensitive information.

Firewalls

Firewalls act as a barrier between the internal network and the outside world. They monitor and control incoming and outgoing network traffic according to predefined rules, blocking unauthorized access attempts and potentially malicious activities.

IDPSs

IDPSs detect and respond to network-based attacks by monitoring network traffic, analyzing patterns, and identifying suspicious or malicious activity. They can take proactive measures to prevent attacks or provide real-time alerts for immediate response.

Network segmentation

Network segmentation is a network management practice that allows you to divide your networks into smaller subnetworks or segments based on different criteria, such as departments, functions, or security levels.

By segmenting the network, organizations can limit the impact of a potential breach and control access to sensitive resources more effectively.

VPNs

VPNs provide secure remote access to private networks over the internet. They encrypt network traffic, ensuring the confidentiality and integrity of data transmitted between remote users and the network. VPNs are commonly used to connect remote workers or branch offices securely.

Secure wireless access points (WAPs)

Wireless access points are used to provide wireless network connectivity. Secure WAPs implement robust encryption protocols, such as WPA2 or WPA3, and strong authentication mechanisms to prevent unauthorized access to the wireless network.

Performance of a Network:

The performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. Finding the performance of a network depends on both quality of the network and the quantity of the network.

Parameters for Measuring Network Performance

- Bandwidth
- Latency (Delay)
- Bandwidth – Delay Product
- Throughput
- Jitter

Bandwidth

One of the most essential conditions of a website's performance is the amount of bandwidth allocated to the network. Bandwidth determines how rapidly the webserver is able to upload the requested information. While there are different factors to consider with respect to a site's performance, bandwidth is every now and again the restricting element.

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices, the bandwidth is measured in bits per second(bps) or bytes per second. In the case of analog devices, the bandwidth is measured in cycles per second, or Hertz (Hz).

Bandwidth is only one component of what an individual sees as the speed of a network. People frequently mistake bandwidth with internet speed in light of the fact that Internet Service Providers (ISPs) tend to claim that they have a fast "40Mbps connection" in their advertising campaigns. True internet speed is actually the amount of data you receive every second and that has a lot to do with latency too. "Bandwidth" means "Capacity" and "Speed" means "Transfer rate".

More bandwidth does not mean more speed. Let us take a case where we have double the width of the tap pipe, but the water rate is still the same as it was when the tap pipe was half the width. Hence, there will be no improvement in speed. When we consider WAN links, we mostly mean bandwidth but when we consider LAN, we mostly mean speed. This is on the grounds that we are generally constrained by expensive cable bandwidth over WAN rather than hardware and interface data transfer rates (or speed) over LAN.

- **Bandwidth in Hertz**: It is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, let us consider the bandwidth of a subscriber telephone line as 4 kHz.
- **Bandwidth in Bits per Seconds**: It refers to the number of bits per second that a channel, a link, or rather a network can transmit. For example, we can say the bandwidth of a Fast Ethernet network is a maximum of 100 Mbps, which means that the network can send 100 Mbps of data.

Note: There exists an explicit relationship between the bandwidth in hertz and the bandwidth in bits per second. An increase in bandwidth in hertz means an increase in bandwidth in bits per second. The relationship depends upon whether we have baseband transmission or transmission with modulation.

Latency

In a network, during the process of data communication, latency (also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination. The network connections where small delays occur are called “Low-Latency-Networks” and the network connections which suffer from long delays are known as “High-Latency-Networks”.

High latency leads to the creation of bottlenecks in any network communication. It stops the data from taking full advantage of the network pipe and conclusively decreases the bandwidth of the communicating network. The effect of the latency on a network’s bandwidth can be temporary or never-ending depending on the source of the delays. Latency is also known as a ping rate and is measured in milliseconds(ms).

- In simpler terms latency may be defined as the time required to successfully send a packet across a network.
- It is measured in many ways like a round trip, one-way, etc.
- It might be affected by any component in the chain utilized to vehiculate data, like workstations, WAN links, routers, LAN, and servers, and eventually may be limited for large networks, by the speed of light.

Latency = Propagation Time + Transmission Time + Queuing Time + Processing Delay

Propagation Time

It is the time required for a bit to travel from the source to the destination. Propagation time can be calculated as the ratio between the link length (distance) and the propagation speed over the communicating medium. For example, for an electric signal, propagation time is the time taken for the signal to travel through a wire.

Propagation time = Distance / Propagation speed

Example:

Input: What will be the propagation time when the distance between two points is 12, 000 km?

Assuming the propagation speed to be 2.4 * 10^8 m/s in cable.

Output: We can calculate the propagation time as-

Propagation time = (12000 * 10000) / (2.4 * 10^8) = 50 ms

Transmission Time

Transmission Time is a time based on how long it takes to send the signal down the transmission line. It consists of time costs for an EM signal to propagate from one side to the other, or costs like the training signals that are usually put on the front of a packet by the sender, which helps the receiver synchronize clocks. The transmission time of a message relies upon the size of the message and the bandwidth of the channel.

Transmission time = Message size / Bandwidth

Example:

Input: What will be the propagation time and the transmission time for a 2.5-kbyte

message when the bandwidth of the network is 1 Gbps? Assuming the distance between

sender and receiver is 12, 000 km and speed of light is 2.4 * 10^8 m/s.

Output: We can calculate the propagation and transmission time as-

Propagation time = (12000 * 10000) / (2.4 * 10^8) = 50 ms

Transmission time = (2560 * 8) / 10^9 = 0.020 ms

Note: Since the message is short and the bandwidth is high, the dominant factor is the propagation time and not the transmission time (which can be ignored).

Queuing Time

Queuing time is a time based on how long the packet has to sit around in the router. Quite frequently the wire is busy, so we are not able to transmit a packet immediately. The queuing time is usually not a fixed factor, hence it changes with the load thrust in the network. In cases like these, the packet sits waiting, ready to go, in a queue. These delays are predominantly characterized by the measure of traffic on the system. The more the traffic, the more likely a packet is stuck in the queue, just sitting in the memory, waiting.

Processing Delay

Processing delay is the delay based on how long it takes the router to figure out where to send the packet. As soon as the router finds it out, it will queue the packet for transmission. These costs are predominantly based on the complexity of the protocol. The router must decipher enough of the packet to make sense of which queue to put the packet in. Typically the lower-level layers of the stack have simpler protocols. If a router does not know which physical port to send the packet to, it will send it to all the ports, queuing the packet in many queues immediately. Differently, at a higher level, like in IP protocols, the processing may include making an ARP request to find out the physical address of the destination before queuing the packet for transmission. This situation may also be considered as a processing delay.

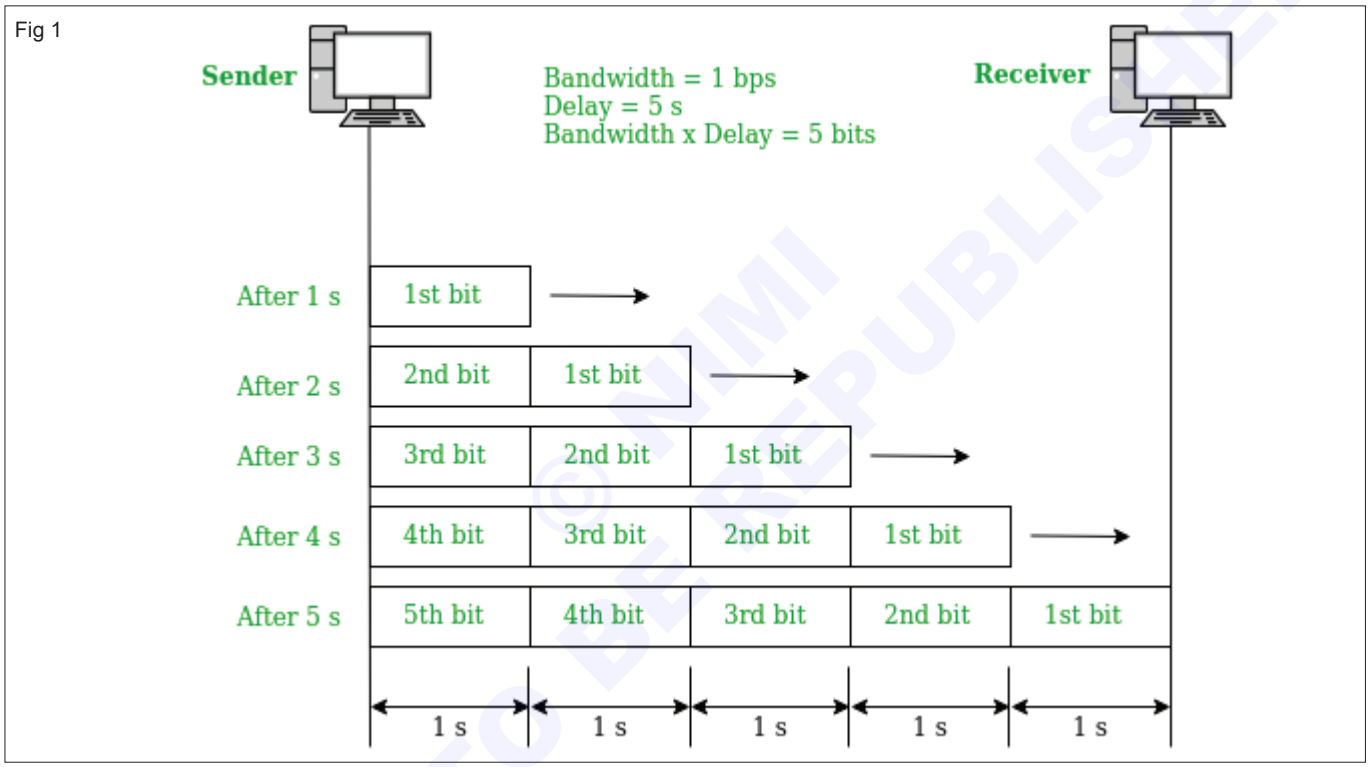
Bandwidth – Delay Product

Bandwidth and Delay are two performance measurements of a link. However, what is significant in data communications is the product of the two, the bandwidth-delay product. Let us take two hypothetical cases as examples. (Fig 1)

Case 1: Assume a link is of bandwidth 1bps and the delay of the link is 5s. Let us find the bandwidth-delay product in this case. From the image, we can say that this product 1 x 5 is the maximum number of bits that can fill the link. There can be close to 5 bits at any time on the link.

Bandwidth Delay Product (Fig 1)

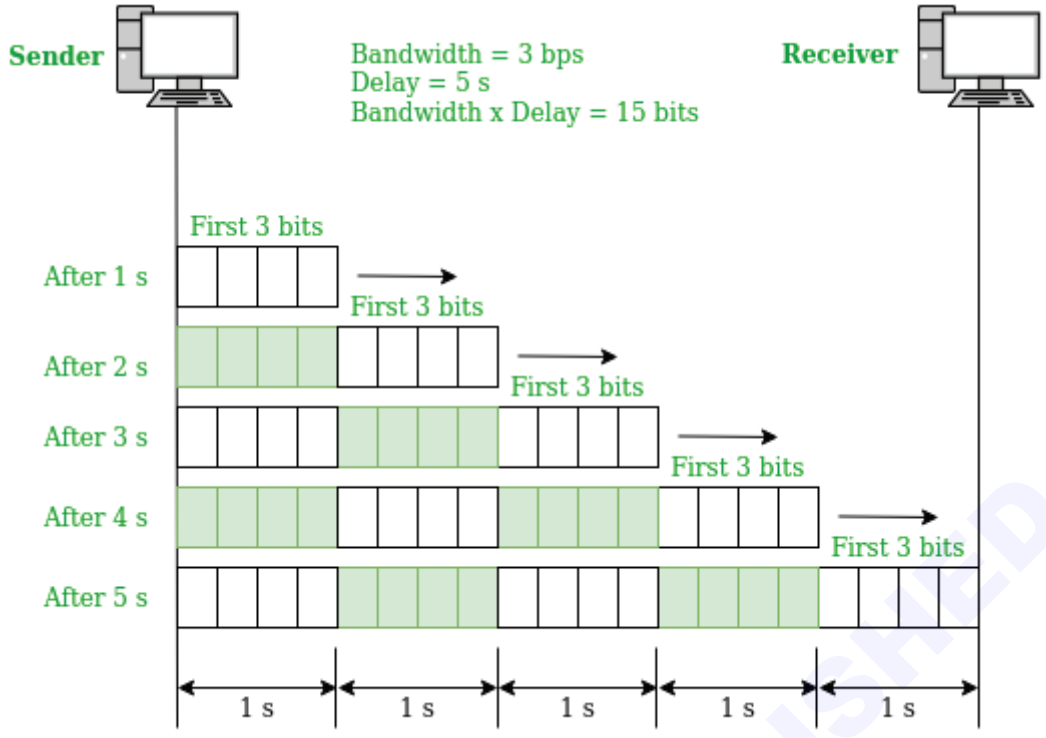
Fig 1



Case 2: Assume a link is of bandwidth 3bps. From the image, we can say that there can be a maximum of 3 x 5 = 15 bits on the line. The reason is that, at each second, there are 3 bits on the line and the duration of each bit is 0.33s.

For both examples, the product of bandwidth and delay is the number of bits that can fill the link. This estimation is significant in the event that we have to send data in bursts and wait for the acknowledgment of each burst before sending the following one. To utilize the maximum ability of the link, we have to make the size of our burst twice the product of bandwidth and delay. Also, we need to fill up the full-duplex channel. The sender ought to send a burst of data of (2*bandwidth*delay) bits. The sender at that point waits for the receiver's acknowledgement for part of the burst before sending another burst. The amount: 2*bandwidth*delay is the number of bits that can be in transition at any time. (Fig 2)

Fig 2



Throughput

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio, and hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption. The terms 'throughput' and 'bandwidth' are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.

Throughput is measured by tabulating the amount of data transferred between multiple locations during a specific period of time, usually resulting in the unit of bits per second(bps), which has evolved to bytes per second(Bps), kilobytes per second (KBps), megabytes per second (MBps) and gigabytes per second (Gbps). Throughput may be affected by numerous factors, such as the hindrance of the underlying analog physical medium, the available processing power of the system components, and end-user behavior. When numerous protocol expenses are taken into account, the use rate of the transferred data can be significantly lower than the maximum achievable throughput.

Let us consider: A highway that has a capacity of moving, say, 200 vehicles at a time. But at a random time, someone notices only, say, 150 vehicles moving through it due to some congestion on the road. As a result, the capacity is likely to be 200 vehicles per unit time and the throughput is 150 vehicles at a time.

Example

Input: A network with bandwidth of 10 Mbps can pass only an average of 12, 000 frames

per minute where each frame carries an average of 10, 000 bits. What will be the

through put for this network?

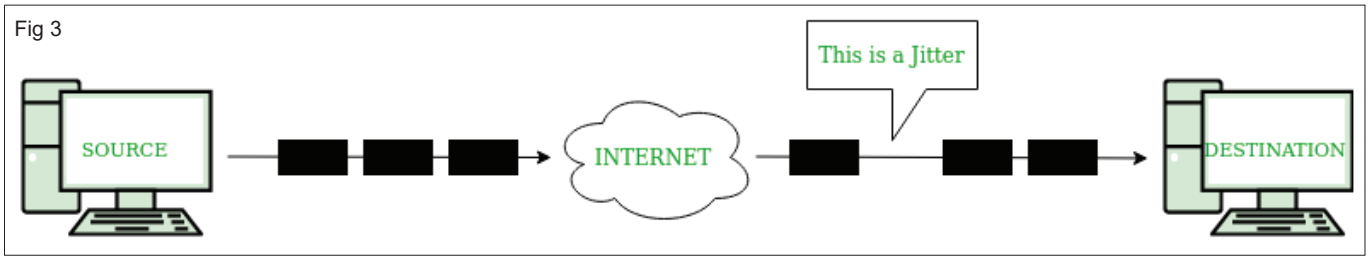
Output: We can calculate the throughput as-

Throughput = (12, 000 x 10, 000) / 60 = 2 Mbps

The throughput is nearly equal to one-fifth of the bandwidth in this case.

Jitter (Fig 3)

Fig 3



Jitter is another performance issue related to the delay. In technical terms, jitter is a "packet delay variance". It can simply mean that jitter is considered a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds(ms). It is defined as an interference in the normal order of sending data packets. For example: if the delay for the first packet is 10 ms, for the second is 35 ms, and for the third is 50 ms, then the real-time destination application that uses the packets experiences jitter.

Simply, a jitter is any deviation in or displacement of, the signal pulses in a high-frequency digital signal. The deviation can be in connection with the amplitude, the width of the signal pulse, or the phase timing. The major causes of jitter are electromagnetic interference(EMI) and crosstalk between signals. Jitter can lead to the flickering of a display screen, affects the capability of a processor in a desktop or server to proceed as expected, introduce clicks or other undesired impacts in audio signals, and loss of transmitted data between network devices.

Jitter is harmful and causes network congestion and packet loss.

- Congestion is like a traffic jam on the highway. Cars cannot move forward at a reasonable speed in a traffic jam. Like a traffic jam, in congestion, all the packets come to a junction at the same time. Nothing can get loaded.
- The second negative effect is packet loss. When packets arrive at unexpected intervals, the receiving system is not able to process the information, which leads to missing information also called "packet loss". This has negative effects on video viewing. If a video becomes pixelated and is skipping, the network is experiencing a jitter. The result of the jitter is packet loss. When you are playing a game online, the effect of packet loss can be that a player begins moving around on the screen randomly. Even worse, the game goes from one scene to the next, skipping over part of the game-play.

In the above image, it can be noticed that the time it takes for packets to be sent is not the same as the time in which they will arrive at the receiver side. One of the packets faces an unexpected delay on its way and is received after the expected time. This is jitter.

A jitter buffer can reduce the effects of jitter, either in a network, on a router or switch, or on a computer. The system at the destination receiving the network packets usually receives them from the buffer and not from the source system directly. Each packet is fed out of the buffer at a regular rate. Another approach to diminish jitter in case of multiple paths for traffic is to selectively route traffic along the most stable paths or to always pick the path that can come closest to the targeted packet delivery rate.

Factors Affecting Network Performance

Below mentioned are the factors that affect the network performance.

- Network Infrastructure
- Applications used in the Network
- Network Issues
- Network Security

Network Infrastructure

Network Infrastructure is one of the factors that affect network performance. Network Infrastructure consists of routers, switches services of a network like IP Addressing, wireless protocols, etc., and these factors directly affect the performance of the network.

Applications Used in the Network

Applications that are used in the Network can also have an impact on the performance of the network as some applications that have poor performance can take large bandwidth, for more complicated applications, its maintenance is also important and therefore it impacts the performance of the network.

Network Issues

Network Issue is a factor in Network Performance as the flaws or loopholes in these issues can lead to many systemic issues. Hardware issues can also impact the performance of the network.

Network Security

Network Security provides privacy, data integrity, etc. Performance can be influenced by taking network bandwidth which has the work of managing the scanning of devices, encryption of data, etc. But these cases negatively influence the network.

Surveillance using Network Devices

Objectives: At the end of this lesson you shall be able to
- **surveillance using network devices**
- **remote management of devices.**

Network Surveillance

Computer and network surveillance is the monitoring of computer activity and data stored locally on a computer or data being transferred over computer networks such as the Internet.

It is usually done covertly by organizations, governments or individuals to monitor illegal activities. Surveillance takes many forms, including physical observation, electronic monitoring, video recording, data collection, and analysis.

Internet surveillance is the act of monitoring and logging your online data and traffic by a third party, such as the government, Internet service providers, Big Tech companies, or criminals.

Unfortunately, while you may think that you're not interesting enough for someone to spy on you or monitor your online activities – you are and you're being a victim of Internet surveillance every second you spend online.

Network Monitoring

Network monitoring, also frequently called network management, is the practice of consistently overseeing a computer network for any failures or deficiencies to ensure continued network performance. Technically, network monitoring can be viewed as a subset of network management, but the two are considered equivalent in practice.

Network monitoring collects and reports on a variety of data from a computer network, including routers, switches, firewalls, load balancers and even endpoints, like servers and workstations. The collected data is filtered and analyzed to identify a variety of network problems. These network problems can include the following:

- Device failures
- Link outages
- Interface errors
- Packet loss
- Application response time
- Configuration changes

The functions of a network monitoring and management system can be broken down into several categories, each of which performs a specific function.

Below is a reference network management architecture, developed by Net Craftsmen, that identifies the different data collection categories, how they share data and the protocols that are used.

Event collection and processing

Event collection relies on Simple Network Management Protocol (SNMP) traps and syslog to collect network event data. Events enable the network to advise administrators of important events without having to poll network devices. Event processing is used to identify critical events, reducing the volume of alerts that network administrators must handle.

Network change and configuration management

Network change and configuration management (NCCM) archives network device configurations and can be used to automate configuration updates. Configurations may be retrieved and updated using any of several mechanisms, including the command-line interface (CLI), SNMP, RESTCONF and NETCONF.

Configuration analysis identifies day-to-day changes (drift) and audit compliance exceptions where configurations don't match network design policies. Both drift and audit are critical functions for ensuring that network configurations match the intended design and operation.

Performance Monitoring

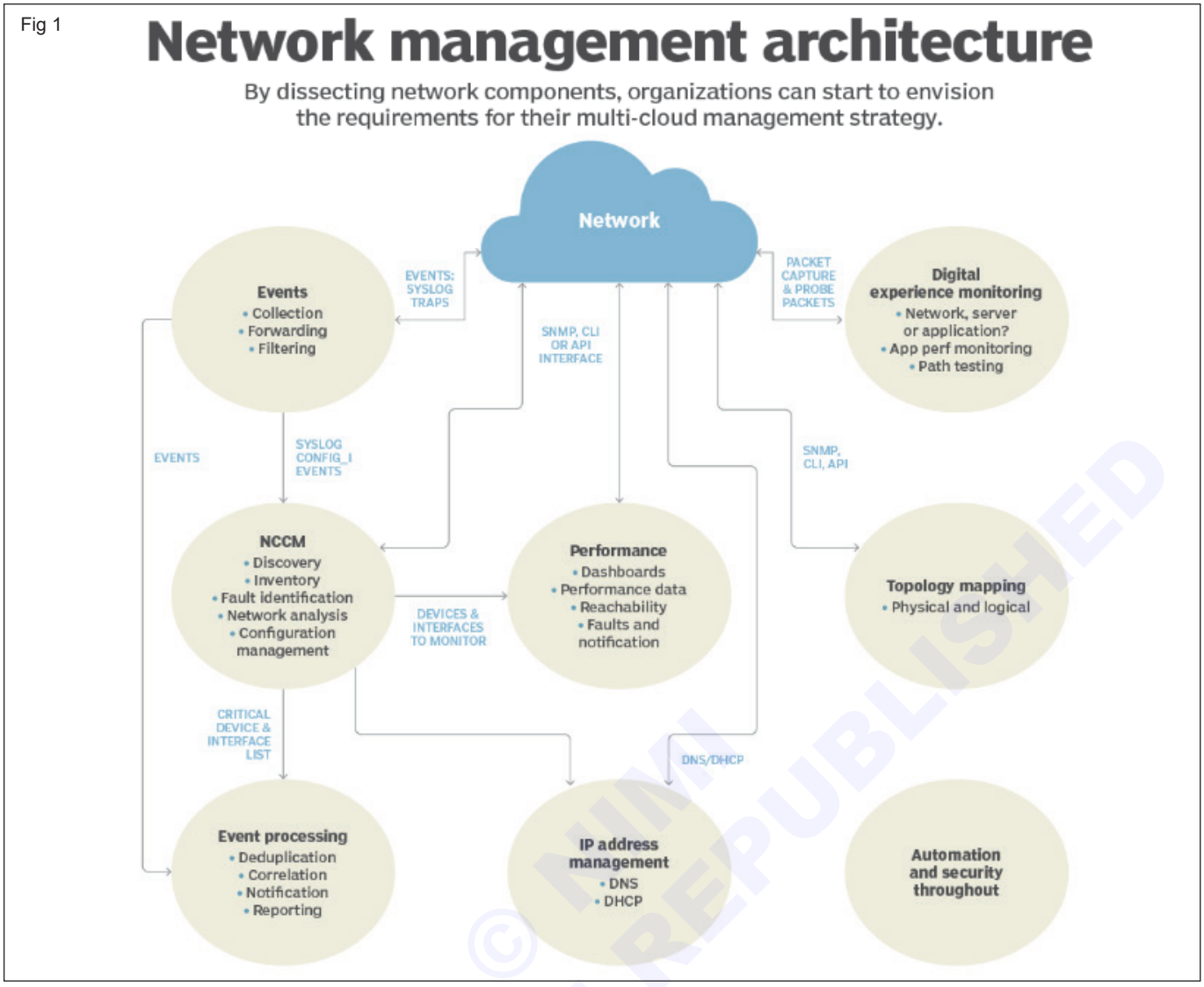
Performance monitoring collects device performance data, like central processing unit (CPU) and memory utilization, temperature, power supply voltages and fan operation. Interface performance data is used to identify failures, packet loss, congestion and other network problems.

Data is collected using SNMP, Windows Management Instrumentation (WMI), the CLI or telemetry. Network devices and Linux-based endpoints typically rely on SNMP or telemetry for data collection, while Windows-based devices rely on the WMI remote protocol. WMI is a client-server framework that enables system management using the Common Information Model, which represents the components of the OS. (Fig 1)

Telemetry

Newer devices and monitoring systems may employ network telemetry to push network performance data to a network monitoring system. Telemetry may use Extensible Markup Language or JavaScript Object Notation-encoded data. Some network monitoring systems and related network devices use representational state transfer interfaces to collect data using these same data formats.

Fig 1



IP address management

IP address management tracks IP address use and controls the allocation of addresses to network devices. This function typically uses the CLI or an application programming interface (API) to other network management systems.

Topology mapping

The topology and mapping function collects device connection data to create physical and logical topology maps that form the foundation of basic troubleshooting. SNMP polling or the CLI are used to collect data on routing neighbors (Layer 3), switching neighbors (Layer 2), address translation tables (Layer 2 to Layer 3 mapping) and neighbor discovery protocols, like Link Layer Discovery Protocol.

Digital experience monitoring

Digital experience monitoring employs active testing tools, such as ping, traceroute and synthetic monitoring, to test that the network is working as intended. It may also employ software agents that run on endpoints, like servers and workstations, to collect data about application performance and network performance. Combining application performance monitoring with network monitoring enables IT organizations to diagnose whether an application problem is due to the network or some other factor, including external networks.

Security and automation

The architecture should include security and automation throughout. Security continues to be an important element of a smoothly running network, and automation is used to guarantee consistent implementation of network policies. The security design should include intrusion detection and intrusion prevention devices and the software to monitor and manage them. Automation may be provided by separate tools or integrated within an NCCM system.

Combining data from multiple sources enables a network monitoring system to identify failures quickly and to report on performance problems before they negatively affect applications that use the network.

How does network monitoring work?

Network monitoring collects massive amounts of data and analyzes the data to identify real or potential network problems that should be investigated. One way to reduce the data volume is to establish ranking of analysis rule exceptions using top N reports, e.g.,

top 10. Examples include the following from each of the architectural elements:

- **Events:** The devices reporting the most events or the most frequently occurring events.
- **NCCM:** The most important devices with configuration changes or the devices with the most configuration changes.
- **Performance:** Highest utilization interfaces, interfaces with the most errors by count or by percentage packets or devices with the greatest CPU or memory utilization.
- **Address management:** Subnets that are almost out of available addresses.
- **Topology:** Devices with the most neighbor changes.
- **Digital experience monitoring:** The systems reporting the slowest applications or the paths that are exhibiting the most problems.

Organizations frequently require a different tool for each architectural element. Consolidating the reports into one place provides a concise view of the network's operation. The reports must support links to the collected data to enable network administrators to perform detailed troubleshooting.

Benefits of network monitoring

The advantages of network monitoring include the following:

- Immediate notification of the failure of a network device or server;
- Rapid identification of security threats;
- Alerting network administrators to errors and performance problems within the network or within the applications, enabling them to address network issues more quickly;
- Tracking changes to network configurations and connectivity that could cause a network problem;
- Automated configuration of network devices;
- Identifying whether an application performance problem is due to the network or some other cause; and
- Visualizing the performance of the IT infrastructure.

A well-running network monitoring system enables the network administrators to address performance degradations proactively and react quickly to network failures. The expansion of networks to cloud implementations and software as a service (SaaS) has greatly expanded monitoring's scope and complexity.

Network monitoring software

Network monitoring software is available from a variety of sources, including open source and commercial. Open source tools often have a paid support version, frequently including premium features beyond those available in the free version. If a network uses devices from multiple vendors, then the network monitoring system needs to support those products. Vendor-supplied software rarely supports devices from other vendors.

Monitoring tools have adapted to the expansion of networks to cloud and SaaS. Network equipment vendors are frequently implementing controller-based architectures that incorporate many of the required monitoring and control functions. These controllers typically include APIs for integration with automation systems and other network monitoring and management tools.

Finding a single pane of glass manager is difficult. The variety of functionality that is needed for network management makes it challenging for a single product to do everything. The most successful approach matches a network monitoring tool with its corresponding functional category. For example, an event processing system has different requirements than a network performance monitoring system. Collecting useful summaries, like the top N reports, into a single dashboard often has the best results.

Organizations should also remember to include staffing requirements. Monitoring tools should be supported by at least two staff members who can keep it updated and be the experts on its operation.

When it comes to network monitoring and management costs, one rule of thumb is to keep it at 10% of the annual amortized cost of the network. These software packages require a lot of development effort, and organizations typically purchase one copy. Organizations shouldn't expect to monitor and manage a $1 million network using a $20,000 system. Alternatively, network administrators can calculate the cost of network downtime and factor that into the cost of the network monitoring systems.

Network monitoring examples

A good example system depends on the requirements, such as the event volume and the number of device interfaces to be monitored. Large networks have different requirements than a small organization's needs. Complex multi-cloud, SaaS, collocated data centers and on-premises data centers require more complex monitoring systems.

A network is a large, complex system in which many things need to work correctly for optimum network health and application performance. It should be monitored as an entire system, not a collection of devices. A word of caution: Organizations shouldn't skimp on thorough coverage. Monitoring a subset of active data center interfaces and key interfaces is a recipe for an undetected failure.

Remote Management

Remote management is the ability of an MDM (Mobile Device Management) to allow users to remotely control its connected mobile devices, such as smartphones and tablets. In situations where businesses need control over their company devices but cannot access

them physically, the ability to remotely manage them is a must.

Remote MDM is a feature of MDM programs and allows administrators to access their full device catalog from anywhere in the world, whether the device is Android or iOS. Administrators need this tool in order to maintain company data and confidentiality and ensure that proper updates are adhered to.

The features of MDM remote management also allow companies to ensure employee compliance, disallow non-work related activities on the devices, and install work applications onto the device for customization purposes. MDM remote management is a great tool for businesses to have in their pockets as they expand and make updates to company practices and policies, as devices can easily have new programs added in bulk.

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network.

Types of security cameras

There is a wide variety of security cameras, and each one serves a different purpose. Some of the most common security cameras are:

Basic or Fixed Security Camera: It is a general purpose camera that does not move, change direction, or zoom. (Fig 2)

Fig 2

Pan and Tilt or Pan-Tilt-Zoom Camera: Pan and tilt cameras can be adjusted quickly, change direction, or zoom, and can even lock in on and follow a moving object that shouldn't be in an area. Pan and tilt cameras have the ability to spin and angle up and down due to a motorized interior mount. It also enables the user to remotely control where the camera looks from the users smartphone or other web-enabled device.

Wireless Camera: Wireless surveillance cameras connect to the security system through an internet connection and are very easy to set up. Usually, it can be customized and can be controlled from a smart phone or computer.

Night Vision Camera

Night vision cameras use infrared technology to illuminate poorly lit areas and record footage at night.

Exterior or Outdoor Camera: They have night vision elements and are weather-proof.

Motion Detection Camera: These cameras can start recording or start taking pictures when it senses movement, so hours of useless footage recording can be avoided. Some motion detection cameras, like pan and tilt cameras, can lock in on a moving object and follow it.

Hidden / Covert Camera: The cameras can be concealed in secret places like bookshelf, coke cans etc. and are used to spy on or catch behavior that might be hard to detect otherwise.

Dome Camera: These cameras are dome-shaped and are often used indoors. Some dome cameras have infrared lighting and can be designed to be tamper-proof. Dome cameras are commonly pan-tilt-zoom capable and, because of the tinted dome that shields the camera, it is difficult to find where the camera is currently facing.

IP Camera

IP (internet Protocol) camera can be defined as a digital video camera that can send and receive data via a computer network or broadband connection. A network camera is a video camera that can be accessed and controlled over any IP network such as a LAN, Intranet, or Internet. By simply using a standard web browser over a high speed Internet connection, users are able to conveniently view a camera's live video and sometimes audio, from any local or remote location. It can be used for surveillance. Cameras are available in Ethernet and Wi-Fi compatible models, network cameras come in a wide variety of categories such as Pan/Tilt/Zoom which enables users to move and change the cameras view, audio enabled units capable of recording sound, to infrared cameras for night use.

IP cameras are equipped with a built-in web server and on board processing, combines the capabilities of a video camera with the power of a computer. IP cameras do not require additional software or a direct PC connection to operate, making it easily placed anywhere along a network. With its own IP address, network cameras connect directly to wired or wireless networks and can be accessed remotely over the internet 24 hours a day. The cameras are easily integrated into existing networks through Universal Plug and Play compatibility

The benefits of using IP camera are

1 Flexible video access options, from restricted to authorized to public.

2 Supports both local or remote access.

3 Cameras install easily and affordably to the existing IP network.

4 Eliminates the need for expensive coaxial cabling to cameras.

5 Viewing footage requires only a computer and a web browser or dedicated software.

6 Shares a unified communications network with data, voice, and wireless traffic, reducing operations and maintenance costs.

Requirements of IP surveillance system

Storage Requirements

Video requires a lot of storage. A small surveillance system of five basic IP cameras recording continuously for a week consumes over one Terabyte (TB) of storage.

Larger installation of 30 high-resolution cameras using even the latest compression techniques still consume 2TB per week.

Wireless: A network camera with wireless support is useful when running a cable between a LAN and a network camera is impractical, difficult, or expensive.

Wireless network cameras are suitable for use outdoors, in buildings where the installation of cables would damage the interior, or in cases where there is a need to move cameras to new locations on a regular basis, such as in a supermarket. Ensure that the wireless network camera supports security protocols such as IEEE 802.1X and WPA/WPA2 (Wi-Fi Protected Access), which will help secure wireless communication.

Security

A video surveillance network camera should provide different levels of password-protected access.

For instance, some authorized users may only have access to view images from specific cameras; others have operator-level access, and a few have access to administer all settings in a network camera.

Beyond multi-level password protection, a network camera may offer AES encryption to secure video streams; IP address filtering, which gives or denies access rights to defined IP addresses; IEEE 802.1X to control network access; and user access logs.

Video recorders

A network video recorder (NVR) is a software program that records video in a digital format to a hard disk drive, USB flash drive, SD memory card or other mass storage device. An NVR contains no dedicated video capture hardware. The software is typically run on a dedicated device, usually with an embedded operating system. An NVR is used in an IP video surveillance system.

Network video recorders are different from digital video recorders (DVR) as their input is from a network rather than a direct connection to a video capture card or tuner. Video on a DVR is encoded and processed at the DVR, while video on an NVR is encoded and processed at the camera, then streamed to the NVR for storage or remote viewing. Additional processing is done at the NVR, such as further compression.

Network Security Devices & Cryptography

Objectives: At the end of this lesson you shall be able to
- **modern network security threats and the basics of securing a network**
- **security considerations of LAN & Wi-Fi**
- **concept of network security devices and cryptography.**

Network security threats are of several types some of the common types of attacks are

1 Social engineering attacks

2 Network based attacks

3 Software based attacks

Social engineering attack: Social engineering attack is obtaining confidential information by means of human interaction. Some of the popular social engineering attacks are

Hacker initiates IT administrator: The hacker calls or e-mails an employee and acts to be the network administrator. The hacker tricks the employee into divulging a password or even resetting the password.

Hacker imitates user: The hacker calls or e-mails the network administrator and pretends to be a user who forgot her password, asking the administrator to reset her password for her.

Hacker e-mails program: The hacker typically e-mails all the users on a network, telling them about a security bug in the OS and that they need to run the update.exe file attached to the e-mail.

Phishing: It is a type of social engineering that involves the hacker sending you an e-mail that is impersonating a site such as a bank or an online site. The e-mail message typically tells you that a pressing matter exists, such as a security compromise with your account, and that you need to log on to your account to verify your transactions. The e-mail message gives you a link to use to navigate to the site, but instead of navigating to the real site, the hacker is leading you to a fake site that he has created which looks like the real site, but when you type in your username and password, the hacker captures that information and then uses it to access your account on the real site!

Whaling & Vishing

Whaling attacks are similar to phishing attacks in the method of sending email but sends the e-mail to a specific person who may have a lot to lose from the attack. The whaling victim is usually an executive for a company where the hacker obtains their name from the company site and personalizes the e-mail using the name of the executive. Vishing tries to trick people and steal money from them. The difference is with vishing the contact is made with a phone call instead of an e-mail message.

Shoulder surfing: In this attack the attacker looks from behind the user and watches what the user types. Sensitive information such as passwords and IDs can be stolen by this method.

Network based attacks: Network technologies or network based protocols are used for this kind of attacks. Some of the types are

Password and Brute Force attack: In this type of attack the attacker uses words of the dictionary to force open in to the account. hackers use a program that mostly uses two text files. One text file contains the most popular user accounts found on networks, The second text file contains a list of all the words in the English dictionary such as administrator, admin, and root. The program then tries every user account in the user account file with every word in the dictionary file, attempting to determine the password for the user account. In a brute force attack, instead of trying to use words from a dictionary, the hacker uses a program that tries to find out the password by trying different combinations of characters.

Denial of service: DOS attack causes a system to be so busy that it cannot service a real request from a client, basically overloading the system and shutting it down. For example a hacker may attack the e-mail server by flooding the server with e-mail messages, causing it to be so busy that it cannot send anymore e-mails.

Ping of death: The hacker continuously pings the system, and the system is so busy sending replies that it cannot do its normal function. By this the service has been denied for which the system has been created for.

Teardrop: The teardrop program creates IP fragments, which are divided pieces of an original IP packet, as it travels through the Internet. The problem is that the fragmented fields of these packets overlap thereby making the destination computer unable to re-assemble these packets and may crash, hang or reboot. For example the field of two fragments created by teardrop will be Fragment1: 100-300 and Fragement2: 200-400.

Ping Flood (ICMP flood): It is caused by an attacker sending a large number of ping packets (ICMP echo request packets) to the Winsock or dialer software. This prevents it from responding to server ping activity requests, which causes the server to eventually timeout the connection. A symptom of a ping flood is a huge amount of modem activity, as indicated by the modem lights. This is also referred to as a ping storm.

Distributed DOS (DDOS) attacks use intermediary computers called agents on which programs called zombies have previously been surreptitiously installed. The hacker activates these zombie programs remotely, causing the intermediary computers (which can number in the hundreds or even thousands) to simultaneously launch the actual attack. Because the attack comes from the computers running the zombie programs, which may be on networks anywhere in the world, the hacker is able to conceal the true origin of the attack.

DNS DOS attack: The Domain Name System (DNS) DOS attack exploits the difference in size between a DNS query and a DNS response, in which all of the network's bandwidth is tied up by bogus DNS queries. The attacker uses the DNS servers as "amplifiers" to multiply the DNS traffic. The attacker begins by sending small DNS queries to each DNS server, which contain the spoofed IP address of the intended victim. The responses returned to the small queries are much larger in size, so that if there are a large number of responses returned at the same time, the link will become congested and denial of service will take place.

SYN attack/LAND attack: Synchronization request (SYN) attacks exploit the Transmission Control Protocol (TCP) three-way handshake, the process by which a communications session is established between two computers. The "handshake" includes the following steps:

1 The client machine sends a SYN segment.

2 The server sends an acknowledgement (ACK) message and a SYN, which acknowledges the client machine's request that was sent in step 1 and sends the client a synchronization request of its own. The client and server machines must synchronize each other's sequence numbers.

3 The client sends an ACK back to the server, acknowledging the server's request for synchronization. When both machines have acknowledged each other's requests, the handshake has been successfully completed and a connection is established between the two computers.

A SYN attack uses this process to flood the system targeted with multiple SYN packets that have bad source IP addresses, which causes the system to respond with SYN/ACK messages. The problem comes when the system, waiting for the ACK message, puts the waiting SYN/ACK messages into a queue. The queue is limited in the number of messages it can handle, and when it is full, all subsequent incoming SYN packets will be ignored. In order for a SYN/ACK to be removed from the queue, an ACK must be returned from the client, or the interval timer must run out and terminate the three-way handshake process. Because the source IP addresses for the SYN packets sent by the attacker are no good, the ACKs that the server is waiting for never come. The queue stays full, and there is no room for valid SYN requests to be processed. Thus service is denied to legitimate clients attempting to establish communications with the server.

The LAND attack is a variation on the SYN attack. In the LAND attack, instead of sending SYN packets with IP addresses that do not exist, the flood of SYN packets all have the same spoof IP address that of the targeted computer.

UDP bomb or UDP flood: An attacker can use the User Datagram Protocol (UDP) and one of several services that echo packets upon receipt to create service-denying

network congestion by generating a flood of UDP

packets between two target systems.

Spoofing: Spoofing is a type of attack in which a hacker modifies the source address of a network packet, which is a piece of information that is sent out on the network. This packet includes the data being sent but also has a header section that contains the source address (where the data is coming from) and the destination address (where the data is headed). If the hacker wants to change who the packet looks like it is coming from, the hacker modifies the source address of the packet. There are three major types of spoofing MAC spoofing, IP spoofing, and e-mail spoofing.

MAC spoofing: MAC spoofing is when the hacker alters the source MAC address of the packet.

IP Spoofing: IP spoofing is when the hacker alters the source IP address in a packet changing the packet

headers of a message to indicate that it came from an IP address other than the true source.

Scanning: In network security scanning refers to a software program that is used by hackers to remotely determine what TCP/UDP ports are open on a given system, and thus vulnerable to attack. TCP and UDP services and applications use a number of well-known ports, which are widely published. TCP and UDP services and applications use a number of well-known ports, which are widely published. For example, Telnet normally uses port 23. If the hacker finds that port open and listening, he knows that Telnet is probably enabled on the machine. He can then try to infiltrate the system, for example by guessing the appropriate password in a brute force attack. If a port is open, it will respond when another computer attempts to contact it over the network.

Some of the commonly used ports are:

TCP/UDP port 20: FTP (data)

TCP/UDP port 21: FTP (control)

TCP/UDP port23: Telnet

TCP/UDP port 25: SMTP

TCP/UDP port 53: DNS

TCP/UDP port 67: BOOTP server

TCP/UDP port 68: BOOTP client

TCP/UDP port 69: TFTP

TCP/UDP port 80: HTTP

TCP/UDP port 88: Kerberos

TCP/UDP port 110: POP3

TCP/UDP port 119: NNTP

TCP/UDP port 137: NetBIOS name service

TCP/UDP port 138: NetBIOS datagram service

TCP/UDP port 139: NetBIOS session service

TCP/UDP port 194: IRC

TCP/UDP port 220: IMAPv3

TCP/UDP port 389: LDAP

SMURF attack

It is a combination of a denial of service and spoofing and same method as the ping flood, but directs the flood of ICMP echo request packets at the network's router. The hacker pings a large number of systems but modifies the source address of the packet so that the ping request looks like it is coming from a different system. All systems that were pinged reply to the modified source address an unsuspecting victim. The victims system (most likely a server) receives so many replies to the ping request that it is overwhelmed with traffic, causing it to be unable to answer any other request from the network.

Eavesdropping attack: An eavesdropping attack occurs when a hacker uses some sort of packet sniffer program to see all the traffic on the network. Hackers use packet sniffers to find out login passwords or to monitor activities

A man-in-the-middle attack involves the hacker monitoring network traffic but also intercepting the data, potentially modifying the data, and then sending out the modified result. The person the packet is destined for never knows that the data was intercepted and altered in transit.

Session hijacking: A session hijack is similar to a man-in-the-middle attack, but instead of the hacker intercepting the data, altering it, and sending it to whomever it was destined for, the hacker simply hijacks the conversation a session and then impersonates one of the parties. The other party has no idea that he is communicating with someone other than the original partner.

Wireless attacks

War driving: Using wireless equipment to detect wireless management packets. Hackers can crack the wireless encryption if a weak encryption protocol such as WEP is used. Hackers can also spoof the MAC address of their system and try to bypass the MAC address filters. Also, there are wireless scanners such as Kismet that can be used to discover wireless networks even though SSID broadcasting is disabled.

Software-based attacks: a software attack comes through software that a user runs. SQL injection: An SQL injection attack occurs when the hacker sends Transact SQL statements (statements that manipulate a database) into an application so that the application will send those statements to the database to be executed. If the application developer does not validate data inputted in the application, the hacker can modify the data or even delete it. The hacker can potentially manipulate the OS through the application that sends the input to the database.

Buffer overflow: It involves the hacker sending more data to a piece of software than it is expecting. The information sent to an application is typically stored in an area of memory (a buffer). When more data than expected is sent to the application, the information is stored in memory beyond the allocated buffer. If the hacker can go beyond the allocated buffer, he can run the code.

Malware: Malicious software, also known as malware, is any software that does harm to the system, such as a virus or spyware.

Virus: A virus is a program that causes harm to your system. Usually, viruses are spread through e-mails and are included in attachments, such as word processing documents and spreadsheets. The virus can do any of a number of things: delete files from your system, modify the system configuration, or e-mail all your contacts in your e-mail software.

Trojan horse: A Trojan horse is software that a user is typically tricked into running on the system; and when the software runs, it does something totally different than what the user expected it to do. For example, Net Bus (an older attack) is an example of a Trojan horse program sent as a file called patch.exe. The user receiving the file, typically through an e-mail, believes that the file will fix a security issue. The problem is that patch.exe is a Trojan horse, and when that horse starts running, it opens the computer up to allow a hacker to connect to the system.

Rootkit: A rootkit is malicious software installed on your system by the hacker that gives the hacker unauthorized access to the system at a later time.

Worm: A worm is a virus that does not need to be activated by someone opening the file. The worm is self-replicating, meaning that it spreads itself from system to system, infecting each computer. To protect against a worm, you should install a firewall. A firewall is a piece of software or hardware that prevents someone from entering your system.

Logic bomb: A logic bomb is malicious software that could run every day, but the software was designed to wreak havoc on your system on a certain date and time. The scary thing about logic bombs is that they seem like useful software until the day the programmer decides it will become malicious!

Spyware and adware: Spyware is a type of malicious software that when installed on your system, monitors your activity, including Internet activity. Adware is

software that after being installed on your system, will pop up with ads promoting different products and websites. Be sure to install spyware protection and adware protection on your system to prevent such software from running on your computer.

Use of social network and P2P

A large number of viruses are being written in applications used in social networking sites such as Twitter, My Space, and Facebook. Peer-to-peer software is used to share music, videos, and software applications on the Internet for the rest of the world to download. Examples of such software is Bit Torrent, this is a popular way for hackers to distribute viruses across the network.

Securing a Network

Physical Security: The Server room should be secured from unauthorised physical access. Getting physical

access to a server can help the hacker to boot the server from a bootable CD which could bypass the OS entirely. BIOS setting can be done to help control the security of the system. some of the BIOS settings used to help physical security.

Drive lock: Drive lock is a hard disk specification used to prevent access and booting from the drive. To protect access to the drive, there are two drive lock passwords: a user password and a master password. The user password is used by the user wanting to access the system; the master password is used to reset the user password if the user forgets the password. If the user password and master password are forgotten or lost, the drive is useless.

Power on password: A power-on password can be set in CMOS to limit who can use the system.

Intrusion detection: Most systems have intrusion detection features that can be enabled through the BIOS that will notify you if the cover is taken off the system. This is designed to alert you if someone opens the cover and takes internal components.

TPM: The Trusted Platform Module (TPM) is a chip on computer hardware used to store cryptography keys that are typically used to encrypt data. A TPM chip can also be used to authenticate a device because it contains a unique key that identifies the chip, or hardware device.

Disable the ability to boot from a floppy disk or CD-ROM in the CMOS setup on the systems.

Disable network ports. To prevent a hacker from plugging into the network, and performing a number of network attacks, ensure that network ports, or jacks, in lobbies and front entrances are disabled unless an administrator enables them.

Security in Authentication: Authentication is the process of verifying the identity of a person or a source of information. Authentication may involve typing a username and password on a system before granting access. If a intruder knows the username and password he can easily create or make changes to the system.

Authentication Process: When a user types an username and password to log on to a system, that username and password are verified against a database known as the user account database, which has a list of the usernames and passwords allowed to access the system. If the username and password typed are in the user account database, then the user is allowed to access the system. Otherwise, an error message is displayed and access is not allowed. In a Microsoft network, the account database is the Active Directory Database and resides on a server known as a domain controller. When the user logs on to a Microsoft network environment, the username and password typed are placed in a logon request message that is sent to the domain controller to be verified against the Active Directory Database. If the username and password typed by the user are correct, an access token is generated. An access token is a piece of information that identifies the user and is associated with everything the user does on the computer and network. The access token contains the user account information and any groups of which the user is a member. When a user tries to access a resource on the network, the user account and group membership in the access token are compared against the permission list of a resource. If the user account in the access token or one of the groups contained in the access token are also contained in the permission list, then the user is granted access to the resource. If not, an access-denied message is displayed. To enhance the security in addition to the username and password other authentication techniques such as biometrics, smart card, key fobs, RFID badges etc. can be used along with the user name and password. Biometrics is using ones unique physical characteristics, such as a fingerprint or the blood vessels in ones retina, to prove ones identity. A smart card is a small, ATM cardlike device that contains the account information of the user. The user has to insert the smart card into a smart card reader that is connected to a computer, and then enter the PIN associated with the smart card.

A strong password should be used in securing the user account. A strong password is a password that is very difficult for hackers to guess or crack. It should contain a mix of uppercase and lowercase characters, contains a mix of numbers and letters, and is a minimum of six characters long.

Security in Authorization: Authorization is the process of giving a user permission to access a resource or the right to perform an OS task. An user must be first authenticated to the network then, after authentication, the user can access the resources authorized for. To access a file, folder, or printer on the network, the user must be authorized to access the resource. To authorize access to a resource, permissions must be set on the resource. Permission is the level of access of an user to a resource and rights are the privilege of an user to perform an OS task. By allotting the correct rights and privileges to an user security threats can be avoided.

Security in Transmission of Data: In most network communications information sent along the network wire in cleartext, which means that anyone connected to the same network can read the information. When information in cleartext is traveling across the Internet, anyone can view that information. Internet protocols, such as HTTP, sends information in cleartext. To secure the information sent it has to be encrypted before it is released to the internet. Encrypting the information means that the information is run through a mathematical calculation that generates an altered version of the information. For example, the words **NIMI Chennai** could be encrypted to look like **9y3y 7sf99xy.** If anyone intercepts such encrypted information and views it while it is traveling across the wire, the information would mean nothing. Some of the popular methods of securing transmitted information are.

Secure Sockets Layer (SSL): This protocol is used to encrypt different types of Internet traffic. SSL is used to encrypt HTTP traffic by applying a digital certificate to the Web site. The digital certificate contains the key that is used to encrypt and decrypt the traffic.

Internet Protocol Security (IPSec): This protocol can encrypt all TCP/IP traffic between systems. A network administrator, configures IPSec on the server and the clients with the same key or digital certificates, which are used to encrypt and decrypt network traffic.

Virtual Private Network (VPN): A VPN allows a user to connect across the Internet to a remote network, typically an office network, and send information between the user system and the office network securely. The information is secured because the VPN technology used creates an encrypted tunnel between the user and the office network, any data that travels through the tunnel is encrypted.

Security Data in Hard Drive: Data stored in Hard Drives can be secured using the following means

EFS: The Encrypting File System (EFS) is a feature of NTFS and can be enabled through the file properties. After the file is encrypted, it can be read only by authorized persons.

Bit Locker: Windows can encrypt the entire partition or volume, which protects all data on the partition, including the Windows OS, the Registry, and the data. With Bit Locker, data is encrypted by using keys stored in a TPM chip or a USB drive, depending upon how Bit Locker has been configured.

Third-party software: Third-party software to encrypt data. For example, the free program TrueCrypt (www.truecrypt.org) can be used to encrypt all the data into a TrueCrypt file and then the file can be copied to a USB flash drive.

Wireless network security

Wireless network is not a secure network. Some of the improvements that can be done for wireless security are

1 Change Default Usernames and Passwords

Each router has a default username and password, and it should be changed. If the router's password is either unchanged common or weak, a hacker might be able to reconfigure the router and wipe out all the other security measures, making them useless. Always use a good mix of numbers, symbols, upper case and lower case characters to create a strong password. Avoid using common words, which are known to friends and neighbors. Change passwords frequently.

2 Change the default SSID

The SSID is the name of the user's network. It often reveals the name of a house or office from where Wi-Fi signal is coming, allowing hackers to zero in on the location. Change the SSID to a random name.

3 Disable SSID broadcasts

Disabling the SSID broadcast makes the WiFi router invisible to laptops and cell phones in the area, which automatically scan for Wi-Fi hotspots and try to join them.

4 Disable DHCP or use reservations

DHCP (Dynamic Host Configuration Protocol) enables remote computers connected to the router to obtain an IP address and connect to the network without needing to know the IP and router address information. Disabling the DHCP services is a simple add effective way of keeping intruders away. Set up the computers on the network with static IP addresses. If DHCP is still needed, restrict the number of DHCP IP users to the number of computers on the network. For example, if only five laptops will be

connected to the network, limit the DHCP IP addresses to 5 from the default 50.

5 Use MAC filtering

Each device comes with a unique Media Access Control address (MAC address) that identifies it on a network. MAC address filtering, also known as link-layer filtering or GUI filtering is a feature for IPv4 addresses that includes or excludes computers and devices based on their MAC address. With MAC filtering it can be set which specific computer is allowed to access the WIFI. With MAC address filtering a router will first compare a device's MAC address against an approved list of MAC addresses and only allow a device onto the Wi-Fi network if its MAC address has been specifically approved.

To know the computer's MAC address, go to the DOS prompt and then type "ipconfig /all". Various network setting infos like the user's IP address and NDS settings. The MAC address is the vale of the "Physical Address". Another way to find the MAC address (windows 10) is to navigate to Control Panel > Network and Internet > Network Connections, Right-click on the network connection and select "Status." Click the "Details" button. Locate the Physical Address. The value for the physical address in the Network Connection Details window is the MAC address.

6 Use IP filtering

IP packet filtering consists of creating a series of definitions called filters, which define for the router what types of traffic are allowed or disallowed on each interface. Filters can be set for incoming and outgoing traffic.

Input filters define what inbound traffic on that interface the router is allowed to route or process.

Output filters define what traffic the router is allowed to send from that interface.

Packet filters should be implemented carefully to prevent the filters from being too restrictive, which would impair the functionality of other protocols that might be operating on the computer.

7 Use the strongest security available on the wireless access point.

8 Change the static security keys every now and then.

9 Limit the user accounts that can use wireless connectivity.

10 Turn down the signal strength to the minimum needed to support connectivity.

The method of hiding or disguising messages is called a cryptosystem. A cryptosystem is a collection of algorithms. Messages are disguised using these algorithms. Each algorithm has a key used to decrypt the message encrypted using that algorithm. Cryptography is the art of creating and using cryptosystems. The word cryptography comes from Greek meaning secret writing. In other words Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptographic systems have four basic parts:

1 **Plaintext:** This is the original message before anything is done to it. It is still in either the human readable form or in the format the sender of the message created it in.

2 **Ciphertext:** This is the form the plaintext takes after it has been encrypted using a cryptographic algorithm. It is an intelligible form.

3 **Cryptographic algorithm:** This is the mathematical operation that converts plaintext into ciphertext.

4 **Key:** This is the tool used to turn ciphertext into plaintext.

Cryptography offers three core services: encryption, hashing, and authentication.

Encryption

There are two types of Encryption:

1 Symmetric and

2 Asymmetric.

Symmetric Encryption: In symmetric cryptosystems, only one key, the secret key, is used to both encrypt and decrypt a message. For symmetric encryption to work, the two parties must find a sharable and trusted scheme to share their secret key. The strength of algorithms rests with the key distribution technique, a way to deliver the key to both parties. To encrypt information using symmetric encryption, a symmetric encryption algorithm is used. Some of the commonly used algorithms are

1 Data Encryption Standard (DES)

2 Blowfish

3 Two fish

4 Triple DES (3DES) 3DES is an improvement on DES.

5 Rivest Cipher (RC4/RC5)

6 Advanced Encryption Standard (AES)

7 AES256

Asymmetric Encryption: In asymmetric cryptosystems two keys are used. To encrypt a message, a public key is used and to decrypt the message a private key is used. The public key is made available to the public and the private key is kept private. The sender encrypts the message using the recipients public key. The recipient decrypts the ciphertext using his or her private key. Some commonly used Asymmetric algorithms are

1 Rivest Shamir Adleman (RSA)

2 Diffie-Hellman

3 Elliptic curve

Encryption is used to encrypt data in storage, and to encrypt communication between systems or people.

Data Encryption: Data Encryption prevents unauthorised persons from viewing the data. Encryption can be performed by software on the system or by hardware using computer chips installed on the system. Trusted Platform Module (TPM) is a computer chip on a system that is used to store the cryptographic keys used to encrypt data. Some of the applications of Encryption are

Full disk Todays operating systems support full-disk encryption. Windows 7 and 8 have BitLocker, which encrypts the contents of the entire drive, including the operating system, or encrypt specific partitions. In order to fully boot the system, an individual would need to know the key so that the encrypted contents can be decrypted.

Database When storing information such as credit card numbers, or passwords in a database, it is important to encrypt these sensitive information.

Individual files can be encrypted using the Encrypting File System (EFS) in Windows to encrypt individual files and folders.

Removable media Encryption

Mobile devices Most mobile devices allows encrypting the contents of the mobile device so that if the device is lost or stolen, no one is able to retrieve the data on the device.

Encrypting communication

Some of the common protocols used for encrypting communication in network traffic are

HTTP secure (HTTPS) HTTPS uses SSL to encrypt the communication between the client and the web server. HTTPS is also known as Secure HTTP (SHTTP).

Secure socket Layer (SSL)/Transport Layer Security (TLS) TLS is a more secure protocol that is designed to replace SSL.

Secure MIME (S/MIME) S/MIME is the protocol used to encrypt e-mail messages on the network.

Internet Protocol Security (IPSec) IPSec security protocol is designed to encrypt all IP traffic, no matter what the application is. IPSec has two modes: transport mode and tunnel mode. With transport mode, only the payload of the packet (data portion) is encrypted. With tunnel mode, the header of the packet and the data are encrypted. IPSec uses different protocols for different cryptography services: Authentication Header (AH), which is responsible for authenticating the sender with IPSec, and Encapsulating Security Payload (ESP), which is responsible for encrypting the data in the packet to provide confidentiality.

Secure Shell (SSH) SSH is designed to be a secure replacement to Telnet, and provides authentication and encryption services. SSH can be used to create an encrypted channel so that communication through the channel is encrypted.

Secure FTP (SFTP) SFTP, also known as FTP Secure (FTPS), is an extension on SSH that allows secure transfer and management of files through an SSH channel.

Secure Copy Protocol (SCP) Like SFTP, SCP runs on top of an SSH channel in order to encrypt the communication used to transfer a file.

Wireless Encryption: Wireless networks can be encrypted through WEP, WPA, and WPA2 technologies

WEP: Wired Equivalency Protocol (WEP) encrypts data to provide data security. It uses a static key; the client needs to know the right key to gain communication through a WEP-enabled device. The keys are commonly 10, 26, or 58 hexadecimal characters long. Because of security weaknesses and the availability of newer protocols, WEP is not used widely.

WPA: WiFi Protected Access (WPA) is an improvement on WEP. It uses the Temporal Key Integrity

Protocol (TKIP). WEP used a static 40- or 128-bit key, whereas TKIP uses a 128-bit dynamic per-packet key. It generates a new key for each packet sent. WPA also introduced message integrity checking.

WPA2

WiFi Protected Access 2 (WPA2) is a huge improvement it uses Counter Mode CBC-MAC Protocol (CCMP), which is a protocol based on the Advanced Encryption Standard (AES) security algorithm. over WEP and WPA.

Hashing

Hashing ensures that the information has not been tampered with since it was created or sent to a recipient, in short it ensures the integrity of data or a message. To use hashing, the sender first runs the data through a hashing algorithm, which calculates a hash value based on the data. The idea is that no two pieces of data create the same hash value. Once the hash value is calculated, it is stored or sent with the message. When the message is received, the recipient runs it through the same hashing algorithm to calculate the hash value on the message. The calculated hash value is then compared against the hash value sent with the message, and if they are the same, this means that the information has not been altered.

Some common hashing algorithms are

1 Message Digest (MD)

2 Secure Hash Algorithm (SHA)

3 SHA-256 and SHA-512

4 LANMAN

5 NT LAN Manager (NTLM)

6 RACE Integrity Primitive Evaluation Message Digest (RIPEMD)

7 Hash-based Message Authentication Code (HMAC)

MD5 and SHA-1 are currently the most popular hashing algorithms used to ensure message and data integrity.

Authentication: Authentication is implemented in three ways.

Basic authentication involves a server which maintains a user file of either passwords and usernames or some other useful piece of authenticating information. This information is always examined before authorization is granted.

In challenge- response authentication, the server or any other authenticating system generates a challenge to the host requesting authentication and expecting a response.

Centralized authentication is when a central server authenticates, authorizes, and audits all network users. If the authentication process is successful, the client seeking authentication is then authorized to use the requested system resources, otherwise the authentication process fails and authorization is denied.

The most commonly used authentication methods are password authentication, public-key authentication, remote authentication, and anonymous authentication.

Password Authentication: It is the oldest, most durable, and most widely used authentication methods.

Some of the types are reusable passwords, one- time passwords, challenge- response passwords, and combined approach authentication.

Public Key Authentication: It requires each user of the scheme to first generate a pair of keys and store each in a file. Each key is usually between 1,024 and 2,048 bits in length. Public- private key pairs are typically created using a key generation utility. The pair will consist of a users public and private key pair. The server knows the users public key because it is published widely. However, only the user has the private key. The centralized authentication server commonly known as the access control server (ACS), is in charge of authentication using public key systems. When a user tries to access an ACS, it looks up the users public key and uses it to send a challenge to the user. The server expects a response to the challenge where the user must use his or her private key. If the user then signs the response using his or her private key, he or she is authenticated as legitimate. To enhance public key security, the private key never leaves the user vers machine, and therefore, cannot be stolen or guessed like a password. In addition, the private key has a passphrase associated with it, so even if the private key is stolen, the attacker must still guess the passphrase in order to gain access. Most commonly used authentication systems are secure sockets layer, kerberos, and MD5 authentication.

In Secure Sockets Layer (SSL) authentication, authentication, encryption, and data integrity are provided using public key infrastructure (PKI). SSL authentication, being cryptographic based, uses a public/private key pair that must be generated before the process can begin. Communicating elements acquire verification certificates from a certificate authority (CA), a trusted third party between any two communicating elements like network servers, that certify that the other two or more entities involved in the intercommunication, including individual users, databases, administrators, clients, and servers are who they say they are. These certificates are signed by calculating a checksum over the certificate, encrypting the checksum and other information using the private key of a signing certificate. User certificates can be created and signed by a signing certificate which can be used in the SSL protocol for authentication purposes.

Kerberos authentication is a network authentication protocol that provides strong authentication for client/ server applications by using PKI technology. Kerberos is typically used when a user on a net work. is attempting to make use of a network service and the service wants assurance that the user is who he says he is. To that end, the kerberos user gets a ticket that is issued by the kerberos authentication server (AS). The service then examines the ticket to verify the identity of the user. If all checks out, then the user is issued an access ticket.

MD5 authentication is one of the standard encryption algorithms in use today for authentication. The authentication process using MD5 is very simple. Each user has a file containing a set of keys that are used as input into an MD5 hash. The information being supplied to the authenticating server, like passwords, has its MD5 checksum calculated using these keys, and is then transferred to the authenticating server, along with the MD5 hash result. The authenticating server then gets user identity information like a password, obtains the user set of keys from a key file, and then calculates the MD5 hash value. If the two are in agreement, authentication is successful.

Remote Authentication

Not all users are directly connected to the networks whose services they want to use. In fact, many workers use company resources remotely while they are on the road. So remote authentication is essential for many system administrators.

Remote authentication is used to authenticate those users who dial in to the ACS from a remote host. This can be done several ways including using secure remote procedure call, dial- up, and remote authentication dialing user services authentication. Secure Remote Procedure Call (RPC) authentication is used by clients who do not need to identify themselves to the server, and the server does not require any identification from the client. Services falling in this category, like the Network File System (NFS), require stronger security than the other services and RPC authentication provides that degree of security. Since the RPC authentication subsystem package is open ended, different forms and multiple types of authentication can be used by RPC including: NULL authentication, UNIX authentication, data encryption standard (DES) authentication, DES Authentication Protocol, and Diffie- Hellman Encryption.

Dial-up authentication authenticates a remote user, who is usually on a serial line or ISDN. The most common dial- up connection is the Point- to-Point Protocol (PPP). Dial- up authentication services authenticate the peer device, not the user of the device. There are several dial-up authentication mechanisms. For example, PPP authenti-cation has the following mechanisms: Password Authentication Protocol(PAP), the Challenge Handshake Protocol (CHAP), and the Extensible Authentication Protocol (EAP).

Remote Authentication Dial- in User Services (RADIUS) is a common user protocol that provides user dial- in to the ACS which does the user authentication. Because all information from the remote host travels in the clear, RADIUS is considered to be vulnerable to attacks and, therefore, not secure.

Anonymous Authentication

There are many times a system administrator may want outside users to access public areas of the network without accessing the entire system. Clients who need this type of access typically use anonymous authentication. In order to give them access to some system resources, for example to a company Web site, these users, usually customers, are given access

to the resources via a special anonymous account. System services that are used by many users who are not indigenous, like the World Wide Web service or the FTP service, must include an anonymous account to process anonymous requests.

Digital signature - Based authentication

It is an authentication technique that does not require passwords and usernames. A digital signature is a cryptographic scheme used by the message recipient and any third party to verify the sender identity and/or message for authenticity. It consists of an electronic signature that uses public key infrastructure (PKI) to verify the identity of the sender of a message or the signer of a document. The scheme may include a number of algorithms and functions including the digital signature algorithm (DSA), Elliptic curve digital signature and algorithm (ECDSA), account authority digital signature, authentication function, and signing function.

Wireless authentication

Because of the growing use of wireless technology, mobile computing has skyrocketed in the last several years. However, wireless technology has had a persistent low security problem that this rapid growth makes worse. There is a growing need for wireless network authentication for mobile devices since they connect to fixed networks as well as mobile networks.

Antivirus: It is a security program installed in a computer or mobile device to protect it from getting infected by malware. Malware is the term used for any malicious software such as worms, trojans, viruses and spyware. Antivirus software identifies malware in two ways signature detection and behaviour detection. Signature detection method scans the computer for any characteristics or signatures of programs known to be malicious. If a pattern in the computer matches with a set of definitions the program attempts to neutralize it. This method requires updates to protect from new cases of malware. By this method Antivirus can only protect against what it recognizes as harmful. Even if the antivirus is updated to the latest virus definitions there are chances that a new malware can bypass the antivirus software.

In behaviour detection the antivirus does not try to detect the malware, instead it monitors the behaviour of the malware installed in the system. When program acts suspiciously by accessing protected files or trying to modify another program it alerts the user of the activity. This method provides protection from newly created malware but the problem is that it can generate false alarms. The computer user should be well aware of a real alarm and false alarm to wade of the threat. Regardless of how an Antivirus works it can never provide full protection from all types of malware.

UTM

Unified Threat Management (UTM) is a term used to describe a category of security appliances which integrates a range of security features into a single appliance. UTM appliances combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single platform. UTM is designed protect users from blended threats while reducing complexity.

Unified threat management (UTM) is an emerging trend in the network security. Functions that previously had been handled by multiple systems such as Spam blocking, Gateway antivirus, Spyware prevention, Intrusion prevention, URL filtering can be handled by a single threat management system.

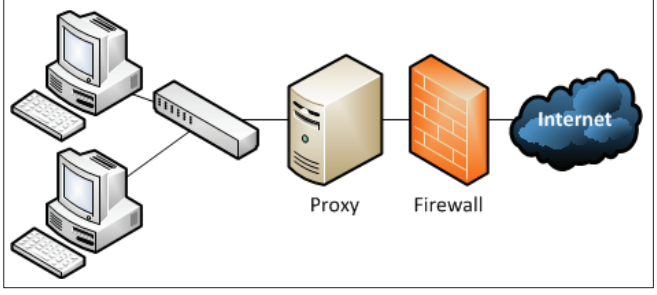
UTM is managed from a single interface as a collective system. This saves network administrators and engineers from installing, configuring, and maintaining multiple security devices, and from trying to make dissimilar platforms all work in unison to protect their network infrastructure. Because all protective functionality resides within one device and management interface, all of its protective methods are integrated and better able to provide “unified” coverage. Also, a single UTM device saves room in the server rack, utilizes less power, and generates less heat because it can be deployed with a single device that occupies fewer slots. Functions of the UTM are antivirus for we, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering and leak prevention. UTMs also function as remote routing, network address translation (NAT), and virtual private network (VPN) support.

Firewall

A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to the computer. A firewall is considered as a first line of defense in protecting private information.

A firewall can help prevent hackers or malicious software from gaining access to the computer through a network or the Internet. A firewall can also help stop the computer from sending malicious software to other computers. see Fig 1.

Fig 1



Firewalls are basically placed on the start of the network to block out unwanted internet traffic and are also enable in servers and client computers to protect them from threats such as virus or worms.

Firewalls can be implemented in both hardware and software, or a combination of both.

Hardware Firewall

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers. Most hardware firewalls will have a minimum of four network ports to connect other computers.

Software Firewall

Software firewalls are installed in the computer and can be customized and allowing some control over its function and protection features. A software firewall will protect the computer from outside attempts to control or gain access to the computer.

Firewall working principle: Information is sent in the form of network packets (pieces of data) that are broken down into three parts:

Header: Contains address information, such as source and destination addresses.

Body: Contains the packet data, known as the payload.

Trailer: Contains checksum information, which is a value calculated off the data in the packet and helps ensure that the data has not been tampered with or damaged in transit. If the receiving system calculates a different value based on the data it receives, and that calculated value is different than the checksum value, the receiving system knows that the data has been altered in transit. A firewall is designed to look at the contents of the packet specifically, the header information to decide whether the data should be allowed into the system or discarded. The firewall uses the source and destination IP addresses from the header, as well as the port number, to help make this decision. A port number represents an application that runs on the system. Each TCP/IP application that is running on the system uses a different port number, which is how data is sent to one application and not the other. Firewall also uses the port number to decide whether the data should be allowed into your system.

Firewall Techniques

There are several types of firewall techniques that will prevent potentially harmful information from getting through:

Packet Filtering

Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application Gateway

Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level Gateway

Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy Server

Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. For greater security, data can be encrypted.

Firewall in Windows 10

The Windows 10 firewall allows for both packet filtering and application-based firewall. It also gives the firewall software both inbound and outbound control.

Windows firewall prevents unauthorized entities from accessing the personal computer and the information stored on it. It blocks malicious hackers and unwanted malware from accessing the files and from modifying the settings.

The firewall monitors and establishes a set of rules concerning how apps on your computer are allowed to communicate via the local network connection with the Internet. Windows firewall also blocks incoming connections but allows software on the computer such as web browsers to work normally, based on a pre-established set of rules.

Windows Firewall Profiles: Windows supports three different profiles.

- Domain Profile
- Private profile
- Public Profile

It is a best practice to select the best suitable profile and enable only one profile at a time

Domain Profile: Domain profile is set, if the computer is connected to the same network where it has a computer account. When domain profile is set only the firewall rules set to the domain profile through group policy gets applied.

Private Profile: The private profile is a user-assigned profile and is used to designate private or home networks. These settings are more restrictive than domain profile

Public Profile: It is used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations. This is the most restrictive set of rules for the firewall.

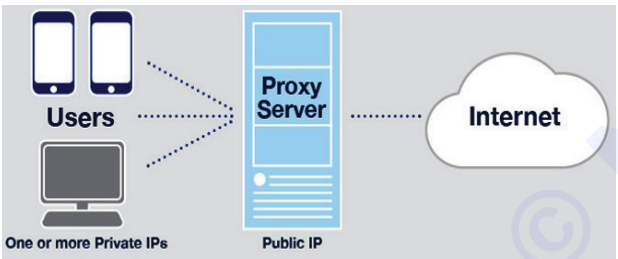
Server Concepts

Objectives: At the end of this lesson you shall be able to
- **concept of server and their hardware identifying**
- **concept of active directory and their namespace, logical & physical elements of active directory**
- **overview of ADDS.**

Proxy server

A proxy server is a computer that functions as an intermediate between a web browser and the Internet. Proxy servers are used to improve security by filtering out some web content and malicious software. Proxy servers are also used to improve web performance by storing a copy of frequently used webpages. When a browser requests a webpage stored in the proxy server's collection (cache), it is provided by the proxy server, which is faster than going to the web. It also offers a computer network service to allow clients to make indirect network connections to other network services. Various uses of Proxy server are: (Fig 1)

Fig 1



To share Internet connection on a LAN.

To speed up Internet surfing.

To hide the IP address of the client computer, so as to act as an intermediary between the user's computer and the Internet to prevent from attack and unexpected access.

To implement Internet access control like authentication for Internet connection, bandwidth control, online time control, Internet web filter and content filter etc.

To bypass security restrictions and filters.

To scan outbound content.

To circumvent regional restrictions. For example, a server using IP-based geolocation to restrict its service to a certain country can be accessed using a proxy located in that country to access the service.

Web proxies

A common proxy application is a caching Web proxy. This provides a nearby cache of Web pages and files available on remote Web servers, allowing local network clients to access them more quickly or reliably.

When it receives a request for a Web resource (specified by a URL), a caching proxy looks for the resulting URL in its local cache. If found, it returns the document immediately. Otherwise it fetches it from the remote server, returns it to the requester and saves a copy in the cache. The cache usually uses an expiry algorithm to remove documents from the cache, according to their age, size, and access history. Two simple cache algorithms are Least Recently Used (LRU) and Least Frequently Used (LFU). LRU removes the least-recently used documents, and LFU removes the least-frequently used documents.

Web proxies can also filter the content of Web pages served. Some censorware applications - which attempt to block offensive Web content - are implemented as Web proxies. Other web proxies reformat web pages for a specific purpose or audience; for example, Skweezer reformats web pages for cell phones and PDAs. Network operators can also deploy proxies to intercept computer viruses and other hostile content served from remote Web pages.

A special case of web proxies are "CGI proxies." These are web sites which allow a user to access a site through them. They generally use PHP or CGI to implement the proxying functionality. CGI proxies are frequently used to gain access to web sites blocked by corporate or school proxies. Since they also hide the user's own IP address from the web sites they access through the proxy, they are sometimes also used to gain a degree of anonymity.

You may see references to four different types of proxy servers:

Transparent Proxy: This type of proxy server identifies itself as a proxy server and also makes the original IP address available through the http headers. These are generally used to cache websites and do not effectively provide any anonymity to those who use them. However, the use of a transparent proxy will get you around simple IP bans. They are transparent in the terms that the IP address is exposed.

Anonymous Proxy: This type of proxy server does not make the original IP address available. It is detectable, but provides reasonable secrecy for most users.

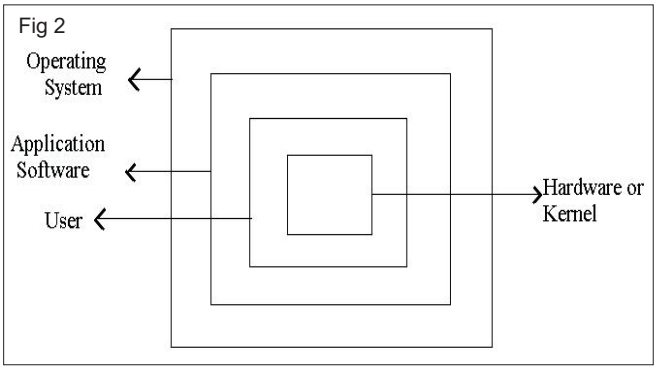
Distorting Proxy: It identifies itself as a proxy server, but makes an incorrect original IP address available through the http headers.

High Anonymity Proxy: It does not identify itself as a proxy server and does not make available the original IP address.

Operating system

Operating System is software that works as an interface between a user and the computer hardware. The primary objective of an operating system is to make computer system convenient to use and to utilize computer hardware in an efficient manner. The operating system performs the basic tasks such as receiving input from the keyboard, processing instructions and sending output to the screen. (Fig 2)

Fig 2



The Software is the Non-Touchable Parts of the Computer, and Software's are those which are used for Performing an Operation So that Software's are just used for Making an Application but hardware's are those which are used for Performing an Operation.

Client

- A Computer joined in the Domain with Client Operating system. (Fig 3)

Fig 3

- Client Operating systems like Windows 7, Windows 8, Windows XP/2000.

Member servers

- A Computer joined in the Domain with Server Operating System (Member Server is also a CLIENT in the Network.
- Server Operating systems like Windows Server 2003, Windows Server 2008, Windows Server 2012.

Server

A server is an instance of a computer program that accepts and responds to requests made by client. Less formally, any device that runs server software could be considered a server as well. Servers are used to manage network resources.

For example, a user may setup a server to control access to a network, send/receive e-mail, manage print jobs, or host a website.

Some servers are committed to a specific task, often referred to as dedicated. As a result, there are a number of dedicated server categories, like PRINT SERVERS, FILE SERVERS, NETWORK SERVERS AND DATABASE SERVERS. However, many servers today are shared servers which can take on the responsibility of e-mail, DNS, FTP, and even multiple websites in the case of a web server.

Because they are commonly used to deliver services that are required constantly, most servers are never turned off. Consequently, when servers fail, they cause the network users or company many problems. To solve these issues, servers are commonly high-end computers setup to be fault tolerant.

Windows Server is a brand name for a group of server operating systems released by Microsoft. It includes all Windows operating systems branded "Windows Server", but not any other Microsoft product. The first Windows server edition to be released under that brand was Windows Server 2003. However, the first server edition of Windows was Windows NT 3.1 Advanced Server, followed by Windows NT 3.5 Server, Windows NT 4.0 Server, and Windows 2000 Server; the latter was the first server edition to include Active Directory, DNS Server, DHCP Server, Group Policy, as well as many other popular features used today.

This brand includes the following operating systems:

- Windows Server 2003 (April 2003)
- Windows Server 2003 R2 (December 2005)
- Windows Server 2008 (February 2008)
- Windows Server 2008 R2 (July 2009)
- Windows Server 2012 (August 2012)
- Windows Server 2012 R2 (October 2013)
- Windows Server 2016 (September 2016)

Table 1

Hardware requirements for the server

Requirement	Details
Processor	1.4 GHz or higher 64 Bit Processor
Memory	For Windows Server® 2008, 512 MB minimum, 2 GB recommended For Windows Server 2008 R2, 512 MB minimum, 2 GB recommended For Windows Server 2012, 1 GB minimum, 2 GB recommended For Windows Server 2012 R2, 1 GB minimum, 2 GB recommended
Hard Disk Space	32 GB or Higher.
Operating System	Windows Server 2008 (32 bit or 64 bit) Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2

Server roles and Role Services

Roles

A server role is a set of software programs that, when they are installed and properly configured, lets a computer perform a specific function for multiple users or other computers within a network. Generally, roles share the following characteristics.

- They describe the primary function, purpose, or use of a computer. A specific computer can be dedicated to perform a single role that is heavily used in the enterprise, or may perform multiple roles if each role is only lightly used in the enterprise.
- They provide users throughout an organization access to resources managed by other computers, such as Web sites, printers, or files that are stored on different computers.
- They typically include their own databases that can queue user or computer requests, or record information about network users and computers that relates to the role. For example, Active Directory Domain Services includes a database for storing the names and hierarchical relationships of all computers in a network.
- As soon as they are properly installed and configured, roles function automatically. This allows the computers on which they are installed to perform prescribed tasks with limited user commands or supervision.

Role services

Role services are software programs that provide the functionality of a role. When you install a role, you can choose which role services the role provides for other users and computers in your enterprise. Some roles, such as DNS Server, have only a single function, and therefore do not have available role services. Other roles, such as Remote Desktop Services, have several role services that can be installed, depending on the remote computing needs of your enterprise.

Server Form Factors

Servers come in a number of physical form factors or packaging, including:

- **Tower:** The simplest servers, such as high-end PCs, are provided in tower cases and share similar restrictions in their extensibility.
- **Rack-mount:** Larger servers often take rack-mount form. This is a standard, 19-inch wide enclosure that is some multiple of 1.75 inches tall and designed to be mounted into a larger enclosure termed a rack, which allows a site to create an appropriate mix of server configurations. A rack generally integrates some number of services such as power, storage and network connections.
- **Blade:** As the technologies used to fabricate components in building server computers has evolved, those components have become more integrated and substantially smaller. This allowed a server to be built on a single board so a rack-mount-sized enclosure could hold many such boards, each with its own processing, memory, network and (minimal) storage. This led to a new form factor for servers: blades. The developing trend is that blades will encroach and take over rack-mount form factors.

Here is a brief summary of these physical form factors and where to use them:

- The tower form factor is used for low-capacity servers where scalability beyond two towers is not needed.
- The rack-mount form factor is used to provide servers of substantial capability and multiple nodes, with each node itself being highly capable and configurable.
- The blade form factor is best suited for servers containing large numbers of nodes of limited capability, each of which typically builds on PC technology with its low cost and small size.

Computer power supply

Computer power supply is the electric source of all components of a computer. Though it is one of the neglected one compare to the other parts, power supply is a must for a system. Often this part of a computer gets failure and most of the time it is not serviceable.

It will be more easier and cheaper to replace than try to service it.

You should give due attention like you do for other components when you choose or replace the power supply unit.

Function of computer power supply

The function of power unit is to convert the electrical power (AC) comes from wall socket to a suitable type and voltage (DC) so that each component of a computer works properly.

Lack of proper supply of power will damage a computer system. The power supply receives 120 or 230V and converts into 3.3V, 5.5V and 12V. Why different converted power? That is because all components of a computer system don't need the same power.

For example, motherboard and cards use 3.3V. The most power demand parts such as Fan and drives need 12V to operate.

Choosing Computer power supply

Usually, power units come with a case, however, it is a requirement to know the factors behind this unit before picking a new one. Power supplies available on the market have different size and shape that will fit into a particular type of computer case. This is called Form factor, layout and dimensions of a unit.

When you are going to replace a malfunction power unit, you should choose the exact form factor that will go with the existing case of your computer.

There are 3 types of power supply in common use:

- AT Power Supply - used in very old PCs.
- ATX Power Supply - still used in some PCs.
- ATX-2 Power Supply - commonly in use today.

The voltages produced by AT/ATX/ATX-2 power supplies are:

- +3.3 Volts DC (ATX/ATX-2)
- +5 Volts DC (AT/ATX/ATX-2)
- -5 Volts DC (AT/ATX/ATX-2)
- +5 Volts DC Standby (ATX/ATX-2)
- +12 Volts DC (AT/ATX/ATX-2)
- -12 Volts DC (AT/ATX/ATX-2)

A power supply can be easily changed and are generally not expensive, so if one fails (which is far from uncommon) then replacement is usually the most economical solution.

Table 2

Power Supply Power Connector

	24 pin Power Connector	Connects to the mother board ATX Power Connector. See mother board labeled "K" for reference on where to connect your ATX Power Connectors to your motherboard.
	ATX 12V Power Connector	Connects to the mother board ATX Power Connector. See mother board Labeled "N" for reference on where to connect your ATX Power Connectors to your motherboard.
	SATA Power Connector	Connects to your serial ATA drive power socket such as SATA hard drive and SATA optical drives.
	Floppy Drive power connector	Connects to your Floppy drive power socket.

	Parallel ATA power connector	Connects to your Hard drive, Optical Drives, Fans and other peripheral devices that may requires 12V power supply.
	6+2 PCI-E	Connect to a high end video adapter card
	4+4 Pin ATX/EPS	Connects to the motherboard 8 Pin EATX 12v Power Connector, see image. It can also be use on a ATX 12V power connector using half of it, see motherboard Labeled “N”. 4+4 pin ATX/ EPS are mostly used for high end motherboard and servers.

Processor

The Central Processing Unit (CPU) in your server, also referred to simply as the processor, is what interprets and executes instructions, processing data and performing tasks like serving web pages, running database queries and executing other program and computing commands. The more processors in a server, the faster and more efficiently the server is capable of working, and the more instructions can be executed in a shorter space of time.

How fast a processor works depends partly on the clock speed, which is the speed at which the processor executes instructions. The faster the clock, the more instructions the CPU can execute per second. It is the processor speed, measured in hertz (GHz).

But as processors progress, improvements in chip architecture mean that irrespective of the clock speed, a processor can execute more instructions simultaneously, Most modern hosted servers offer multi-core, multithreaded processors, which means that one very good processor may perform more tasks, more efficiently and faster than two or more lesser or older processors, have a faster clock speed.

Multi-core means that a server actually has more than one processor core working to complete the tasks demanded by its users. Although a 4-core processor won’t necessarily be 4x faster than a single-core processor, it will still be able to execute instructions even if one or more of the cores is being fully utilized, rather than stalling. Multithreading further improves performance by allowing multiple threads of code, or multiple parts of a process to be executed simultaneously.

Another important specification of a processor is the cache memory, memory that reduces the time needed to access data from the main memory of the server. The cache memory allows the processor to store and access frequently required data much more quickly. The higher the cache memory, the wider the variety of data that can be held in cache, speeding up the performance of the processor.

Beyond these workload multipliers, each generation of processor chipsets brings with it improvements in chip architecture designed to increase the speed and capacity of performance, by reducing latency and increasing throughput at various stages of the computing process.

Installation

The basic steps to install Ubuntu Server Edition are same as those for installing any other operating system. Unlike the Desktop Edition, the Server Edition does not include a graphical installation program. The Server Edition uses a console menu based process instead.

- Download and burn the appropriate ISO file from the Ubuntu web site.
- Boot the system from the CD-ROM drive.
- At the boot prompt it will be asked to select a language.
- From the main boot menu there are some additional options to install Ubuntu Server Edition. Install the basic Ubuntu Server, check the CD-ROM for defects, check the system’s RAM, boot from first hard disk, or rescue a broken system.
- The installer asks which language it should use. Afterwards, it is asked to select the location.
- Next, the installation process begins by asking for the keyboard layout. Ask the installer to attempt auto-detecting it, or select it manually from a list.
- The installer then discovers the hardware configuration, and configures the network settings using DHCP. If do not wish to use DHCP at the next screen choose “Go Back”, and have the option to “Configure the network manually”.
- Next, the installer asks for the system’s hostname.
- A new user is set up; this user will have root access through the sudo utility.
- After the user settings have been completed, encrypt the home directory option will come.

- Next, the installer asks for the system's time Zone.
- Choose the options to configure the hard drive layout. Afterwards it is asked which disk to install it. Then may get confirmation prompts before rewriting the partition table or setting up LVM depending on the disk layout. If it is choosing LVM, Installer will be asked for the size of the root logical volume.
- The Ubuntu base system is then installed.
- The next step in the installation process is to decide how to update the system. There are three options:
  - **No automatic updates:** This requires an administrator to log into the machine and manually install updates.
  - **Install security updates automatically:** This will install the unattended-upgrades package, which will install security updates without the intervention of an administrator.
  - **Manage the system with Landscape:** Landscape is a paid service provided by Canonical to help manage the Ubuntu machines.
- Now the option to install, or not install several package tasks. Also, there is an option to launch aptitude to choose specific packages to install.
- Finally, the last step before rebooting is to set the clock to UTC.

History and Development of Active Directory

Microsoft offered a preview of Active Directory in 1999 and released it a year later with Windows 2000 Server. Microsoft continued to develop new features with each successive Windows Server release.

Windows Server 2003 included a notable update to add forests and the ability to edit and change the position of domains within forests. Domains on Windows Server 2000 could not support newer AD updates running in Server 2003.

Windows Server 2008 introduced AD FS. Additionally, Microsoft rebranded the directory for domain management as AD DS, and AD became an umbrella term for the directory-based services it supported.

Concept of Active Directory

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.

Active Directory categorizes directory objects by name and attributes. For example, the name of a user might include the name string, along with information associated with the user, such as passwords and Secure Shell keys.

Overview of ADDS

Active Directory Domain Services (AD DS) is the foundation of every Windows domain network. It stores information about domain members, including devices and users, verifies their credentials, and defines their access rights. The server running this service is called a domain controller. A domain controller is contacted when a user logs into a device, accesses another device across the network, or runs a line-of-business Metro-style app sideloaded into a machine.

Other Active Directory services (excluding LDS, as described below) and most Microsoft server technologies rely on or use Domain Services; examples include Group Policy, Encrypting File System, BitLocker, Domain Name Services, Remote Desktop Services, Exchange Server, and SharePoint Server.

The self-managed Active Directory DS must be distinct from managed Azure AD DS, a cloud product.

Lightweight Directory Services [edit]

Active Directory Lightweight Directory Services (AD LDS), previously called Active Directory Application Mode (ADAM),[18] implements the LDAP protocol for AD DS.[19] It runs as a service on Windows Server and offers the same functionality as AD DS, including an equal API. However, AD LDS does not require the creation of domains or domain controllers. It provides a Data Store for storing directory data and a Directory Service with an LDAP Directory Service Interface. Unlike AD DS, multiple AD LDS instances can operate on the same server.

Windows Server 2016 updated AD DS to improve AD security and migrate AD environments to cloud or hybrid cloud environments. Security updates included the addition of PAM.

PAM monitored access to an object, the type of access granted and what actions the user took. PAM added bastion AD forests to provide an additional secure and isolated forest environment. Windows Server 2016 ended support for devices on Windows Server 2003.

In December 2016, Microsoft released Azure AD Connect to join an on-premises Active Directory system with Azure Active Directory (Azure AD) to enable SSO for Microsoft's cloud services, such as Office 365. Azure AD Connect works with systems running Windows Server 2008, Windows Server 2012, Windows Server 2016 and Windows Server 2019.

Active directory Namespace

A namespace is a hierarchical collection of service and object names, typically stored within DNS and Active Directory. There are some similarities between the Active Directory namespace and the DNS namespace, both of which are required by Windows Server 2003.

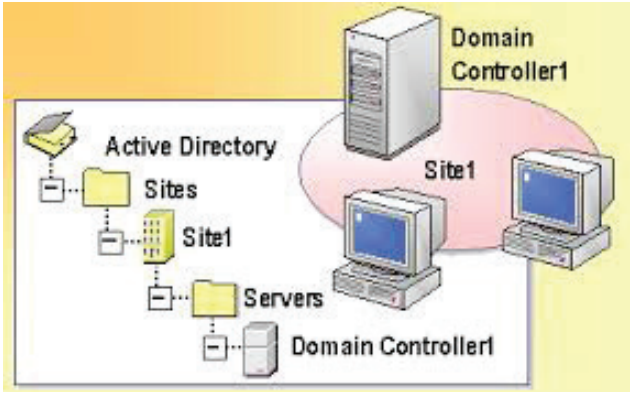
Logical and Physical elements of Active Directory:

In Active Directory, the logical structure is separate from the physical structure. You use the logical structure

to organize your network resources, and you use the physical structure to configure and manage your network traffic.

Physical Structure (Fig 4)

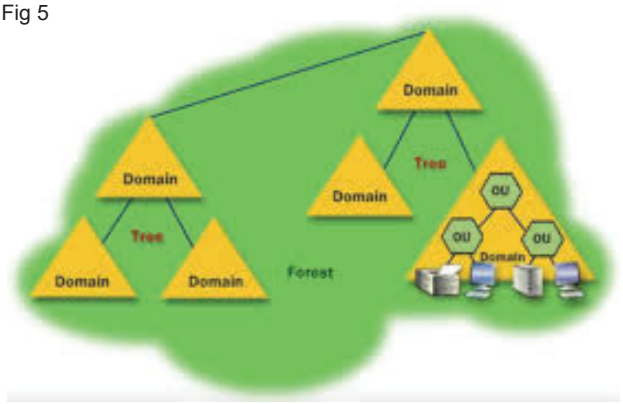
Fig 4



The physical structure of Active Directory is composed of sites and domain controllers. The physical structure of Active Directory defines where and when replication and logon traffic occur. Understanding the physical components of Active Directory is critical to optimizing network traffic and the logon process. In addition, this information can help in troubleshooting replication and logon problems.

Logical Structure (Fig 5)

Fig 5



The logical structure of Active Directory is flexible and provides a method for designing a directory hierarchy that makes sense to both its users and those who manage it. The logical components of Active Directory structure include:

- Domains
- Organizational units
- Trees
- Forests

Understanding the purpose and function of the logical components of the Active Directory structure is important for a variety of tasks, including planning, installing, configuring, and troubleshooting Active Directory.

DNS & DHCP

Objectives: At the end of this lesson you shall be able to
- **understand the concept of DNS**
- **understand the concept of name resolution**
- **understand the concept of DHCP.**

DNS, Domain Name System

It is a hierarchical distributed naming system for computers, servers and every resource connected via network and internet. It has been in wide use since the 1980's and it fundamental role is to translate domain names to IP addresses in order to be easily memorized by users.

Domain Name Service (DNS) is the service used to convert human readable names of hosts to IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or the hyphen. Avoid the underscore. A fully qualified domain name (FQDN) consists of the host name plus domain name as in the following example: computername.domain.com

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: network component and host component.
- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

IP address is 32-bit number while on the other hand domain names are easy to remember names. For example, when we enter an email address we always enter a symbolic string such as webmaster@ tutorialspoint.com.

Uniform Resource Locator (URL) refers to a web address which uniquely identifies a document over the internet.

This document can be a web page, image, audio, video or anything else present on the web.

For example, www.itimallepally.com/internet_technology/ index.html is an URL to the index.html which is stored on itimallepally web server under internet_technology directory.

URL Types

There are two forms of URL as listed below:

1 Absolute URL

2 Relative URL

Absolute URL

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

For example http:// www.itimallepally.com / internet_ technology /index.htm. where:

- http is the protocol.
- itimallepally.com is the server name.
- index.htm is the file name.

The protocol part tells the web browser how to handle the file. Similarly, we have some other protocols also that can be used to create URL are:

- FTP
- https
- Gopher
- mailto
- news

Relative URL

Relative URL is a partial address of a webpage. Unlike absolute URL, the protocol and server part are omitted from relative URL.

Relative URLs are used for internal links i.e. to create links to file that are part of same website as the WebPages on which you are placing the link.

For example to link an image on itimallepally.com/ internet_technology/internet_reference_models, we can use the relative URL which can take the form like / internet_technologies/internet-osi-model.jpg

Difference between Absolute and Relative URL

Absolute URL	Relative URL
Used to link webpages on different websites.	Used to link webpages within the same websites.
Difficult to manage.	Easy to manage.
Changes when the server name or directory name changes.	Remains same even of we change the server name or directory name.
Take time to access.	Comparatively faster to access.

Tree level domain in Domain Naming System

Domains are named using the Domain Name System (DNS). If company is called DETTELANAGANA Corporation, DNS name would be (for example) dettelangana.com. This is the top-level domain name for your company. The security domain in Active Directory maps directly to the DNS domain name.

For larger organizations you can subdivide Active Directory into child domains (based on geography for example). If DETTELANGANA Corporation has three divisions named ITIMALLEPALLY, ITISHANTHINAGAR, and ITIVNCOLONY, the sub-domains can have the DNS names

itimallepally.dettelangana.com,

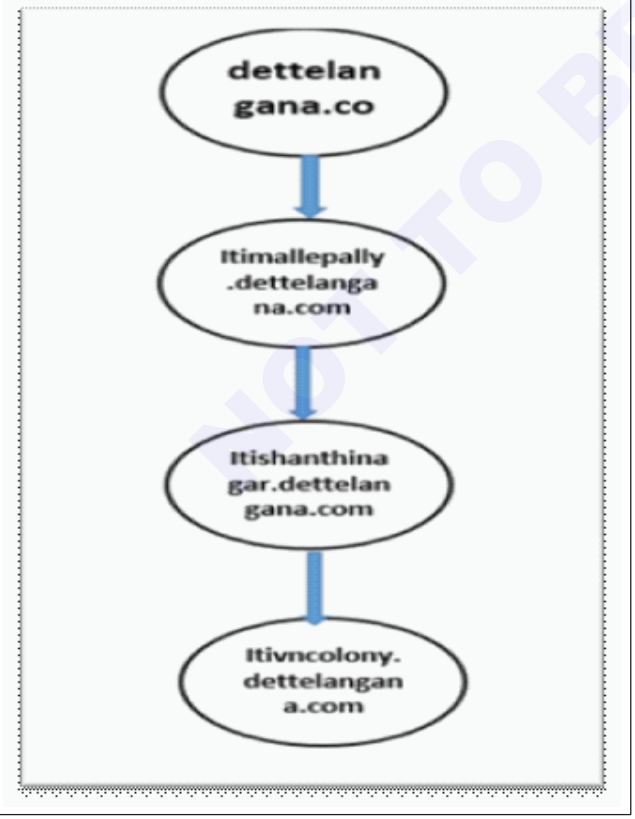
itishanthinagar.dettelangana.com

itivncolony.dettelangana.com.

Each domain requires a server computer. In the above scenario need at least four servers to host Active Directory as follows can be called as TREE.

TREE Level Domain (Fig 1)

Fig 1



Active Directory Domain Services (AD DS) is a server role in Active Directory that allows admins to manage and store information about resources from a network, as well as application data, in a distributed database. AD DS can also help admins manage a network's elements (computers and end users) and reorder them into a custom hierarchy.

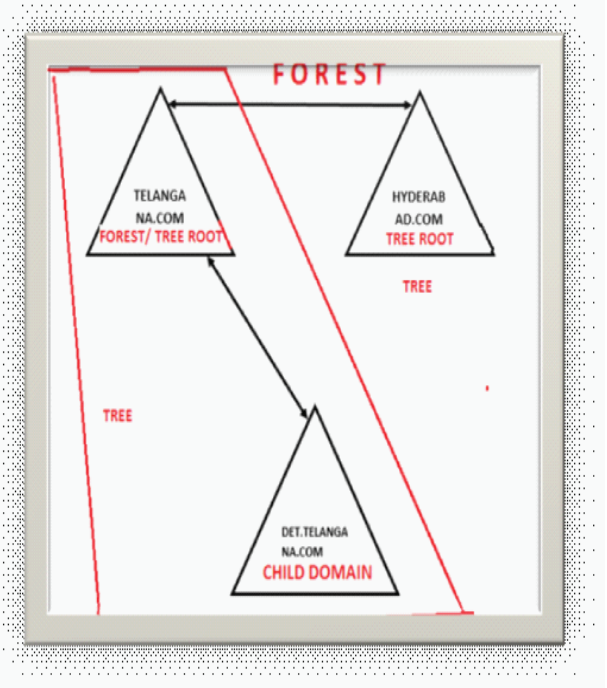
The structure of the hierarchy includes an AD forest, the forest's domains and organizational units in those domains. AD DS integrates security by authenticating logons and controlling who has access to directory resources.

The makeup of AD DS includes:

- AD Users and Computers
- AD Administrative Center
- AD Domains and Trusts
- AD Sites and Services
- A server for Network Information Service tools

Forest Level Domain (Fig 2)

Fig 2



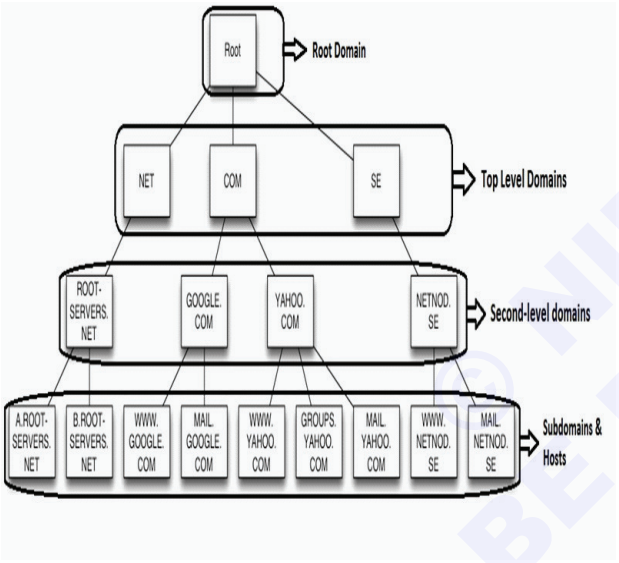
- Multiple domain trees within a single forest do not form a contiguous namespace.
- Although trees in a forest do not share a namespace, a forest will have a single root domain, called the forest root domain.
- The forest root domain is the first domain created in the forest.
- These two forest-wide predefined groups reside in forest root domain.

- Enterprise admins
- Schema admins

Domain Name Space

Domain name space refers a hierarchy in internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy: (Fig 3)

Fig 3



Ex: 1 roxy.cs.colorado.edu

2 paulallen.com

3 ee.colorado.edu

In the above diagram each sub tree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on. (Fig 4)

Name Server

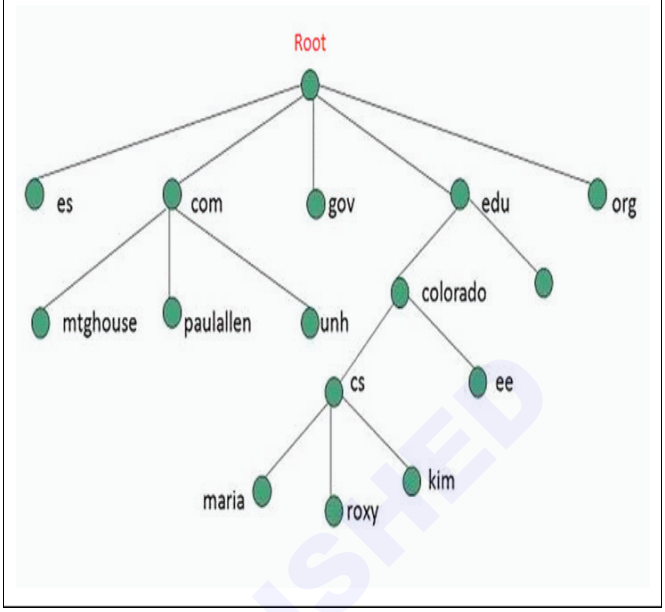
Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names.
- The entire name space is divided into the zones

The DNS Server service provides for three types of zones:

- Primary zone
- Secondary zone
- Stub zone

Fig 4



Primary zone

When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named zone_name.dns and it is located in the %windir%\System32\Dns folder on the server.

Secondary zone

When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.

Stub zone

When a zone that this DNS server hosts is a stub zone, this DNS server is a source only for information about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.

You can use stub zones to:

- Keep delegated zone information current. By updating a stub zone for one of its child zones regularly, the DNS server that hosts both the parent zone and the stub zone will maintain a current list of authoritative DNS servers for the child zone.

- Improve name resolution. Stub zones enable a DNS server to perform recursion using the stub zone's list of name servers, without having to query the Internet or an internal root server for the DNS namespace.
- Simplify DNS administration. By using stub zones throughout your DNS infrastructure, you can distribute a list of the authoritative DNS servers for a zone without using secondary zones. However, stub zones do not serve the same purpose as secondary zones, and they are not an alternative for enhancing redundancy and load sharing.

There are two lists of DNS servers involved in the loading and maintenance of a stub zone:

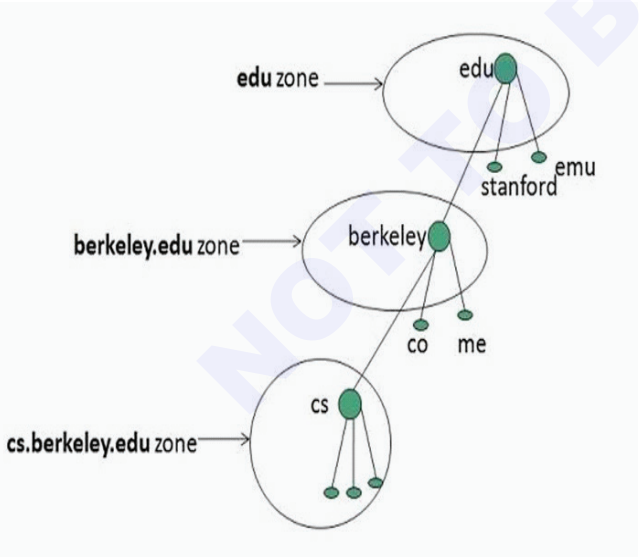
- The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.
- The list of the authoritative DNS servers for a zone. This list is contained in the stub zone using name server (NS) resource records.

When a DNS server loads a stub zone, such as widgets. tailspintoys.com, it queries the master servers, which can be in different locations, for the necessary resource records of the authoritative servers for the zone widgets. tailspintoys.com. The list of master servers may contain a single server or multiple servers, and it can be changed anytime.

DNS Zones and Records (Fig 5)

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.

Fig 5



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels, the original server keeps reference to these lower levels of servers.

The DNS data is kept in a database that can be stored in a text file or in the active directory database when the DNS service is configured on a domain controller.

The DNS data is organized into zones; each zone is a specific portion of DNS namespace that is stored in a separate file or as a unit of replication when stored in active directory. DNS servers can host one or more zones of a particular domain. When creating an active directory domain, a corresponding DNS zone with the same name as the new domain must exist or be created during the process to ensure proper functionality of the directory services.

DNS zones contain different resource records. Resource records specify a resource type, and the IP address to locate the resource. DNS zones can resolve names to IP addresses or IP addresses to names for devices running the TCP/IP protocol like workstations, servers, routers, switches, etc.

The two types of common DNS zones configured on most DNS implementations are forward lookup and reverse lookup zones.

Forward Lookup Zones

Forward DNS lookup is using an Internet domain name to find an IP address. Reverse DNS lookup is using an Internet IP address to find a domain name. When you enter the address for a Web site at your browser (the address is formally called the Uniform Resource Locator, or URL), the address is transmitted to a nearby router which does a forward DNS lookup in a routing table to locate the IP address.

Forward DNS (which stands for domain name system) lookup is the more common lookup since most users think in terms of domain names rather than IP addresses. However, occasionally you may see a Web page with a URL in which the domain name part is expressed as an IP address (sometimes called a dot address) and want to be able to see its domain name.

An Internet facility that lets to do either forward or reverse DNS lookup yourself is called nslookup. It comes with some operating systems or you can download the program and install.

Reverse Lookup Zones

Reverse DNS (DNS) is a method of resolving an IP address into a domain name, just as the domain name system (DNS) resolves domain names into associated IP addresses. One of the applications of reverse DNS is as a spam filter.

Typically, a spammer uses an invalid IP address, one that doesn't match the domain name. A reverse DNS lookup program inputs IP addresses of incoming messages to a DNS database. If no valid name is found to match the IP address, the server blocks that message.

Although reverse DNS is fairly effective for filtering spam, it also sometimes blocks valid e-mail, at least in the current technological environment. A number of problems, including network delays and improperly configured networks or servers, can prevent legitimate messages from getting through the filter.

In January 2003, AT&T WorldNet started using reverse DNS in conjunction with other anti-spam software. The company was forced to remove the filter just 24 hours after it was deployed, after subscribers reported that messages going undelivered.

nslookup

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, “akram.com”) and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address specified.

For example, if you entered “akram.com” (which is one of the instructors site), would receive as a response our IP address, which happens to be :

64.212.43.37

Or if entered “64.212.43.37”, it would return “site.akram.com”.

nslookup sends a domain name query packet to a designated (or defaulted) domain name system (DNS) server. Depending on the system using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root server system for the entire domain name system hierarchy.

Using the Linux and possibly other versions of nslookup, you can locate other information associated with the host name or IP address, such as associated mail services. nslookup is included with some UNIX-based operating systems and in later Windows systems. In Windows XP, the command can be entered on the “Command prompt” screen. A more limited alternative to nslookup for looking up an IP address is the ping command.

Types of name servers

Following are the three categories of Name Servers that manages the entire Domain Name System:

1 Root Server

2 Primary Server

3 Secondary Server

Root server

Root Server is the top level server consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

Primary servers

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

Secondary server

Secondary Server transfers complete information about a zone from another server may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

DNS Working

DNS translates the domain name into IP address automatically. Following steps will take through the steps included in domain resolution process:

- When an website address typed in to the web browser www.akram.com , it asks the local DNS Server for its IP address.

Here the local DNS is at ISP end.

- When an local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that I do not know the IP address of www.akram.com but know the IP address of DNS Server.
- The local DNS server then asks the com DNS Server the same question.
- The com DNS Server replies the same that it does not know the IP address of www.akram.com but knows the address of akram.com.
- Then local DNS asks the akram.com DNS server the same question.
- Then akram.com DNS server replies with IP address of www.akram.com.
- Now, the local DNS sends the IP address of www.akram.com to the computer that sends the request.

Root Hints and Iterative Queries

When installing DNS on Windows Server 2012 R2 a list of Internet root server addresses (root hints) is preloaded by default. These root hints point to the top level DNS servers on the internet. These servers hold intelligence about the top level domains like .com, .org, .net, .edu, etc. When installing the DNS service, this information is copied from the cache.dns file which is by default located on the %windir%\system32\dns directory.

The root hint servers are not configured to respond to recursive queries, and DNS servers only send iterative queries to the root hints.

When recursion is enabled on a DNS server, it means that the server may send DNS queries to its configured root hints or to other DNS servers when acting as a forwarder. Recursive queries are name resolution requests made to a DNS server in which the requester asks the DNS server to provide a complete yes or no answer. The DNS server cannot respond with a referral for the requestor to contact another DNS server.

NETBIOS names

One of the important steps in trying to resolve IP problems is determining if name resolution is working. It seems simple enough: If connect to a computer by IP address and not by NetBIOS name, the problem is with name resolution. That is great, but what happens if NetBIOS name resolution is not functioning, To help overcome this obstacle, will explore the components of NetBIOS resolution and help isolate the cause of name resolution problems.

The first issue is determining the kind of name. In the Windows client world, there are two basic types of names. The first kind is a name for IP addresses. Host name resolution uses a host's file and DNS for resolution. The second kind of name is the NetBIOS name, which is used for Windows (SMB) type sharing and messaging. These are the names that are used when you are mapping a drive or connecting to a printer. These names are resolved either by using an LMHosts file on the local machine or WINS server, or by broadcasting a request.

How NetBIOS names work

NetBIOS names are located through a series of steps that begins with checking the local cache. You then check an LMHosts file and, lastly, progress into a broadcast message that looks for the name.

Dnscmd.exe: DNS Server Troubleshooting Tool

This command-line tool assists administrators in Domain Name System (DNS) management.

DNSCmd displays and changes the properties of DNS servers, zones, and resource records. It manually modifies these properties, creates and deletes zones and resource records, and forces replication events between DNS server physical memory and DNS databases and data files. Some operations of this tool work at the DNS server level while others work at the zone level.

Note

- DNSCmd enhances the functionality of and replaces Dnsstat.exe, a tool included in some versions of the Windows NT Resource Kit.

Corresponding UI

To manually view and manage DNS by using the DNS Server snap-in in Windows

- Click Start, point to Programs, and then point to Administrative Tools.
- Click DNS.
- For information about how to use DNS, right-click DNS, and then click Help.

DNS Client

Name	Description
DNS Client Deregistration	A computer that is configured to use Dynamic Host Configuration Protocol (DHCP) to obtain IP addresses can automatically register its IP address and Domain Name System (DNS) name with the DNS server that is authoritative for the zone that hosts their domains. This eliminates the need for an administrator to manage host (A or AAAA) resource records for client computers. When DHCP assigns a new address to a computer, the DHCP client can request that its previous address be removed from the DNS server. This process is called deregistration. Problems with automatic deregistration do not prevent a computer from accessing the network, but they can cause names to be resolved to incorrect addresses.
DNS Client Registration	A computer that is configured to use Dynamic Host Configuration Protocol (DHCP) to obtain IP addresses can automatically register its IP address and Domain Name System (DNS) name with the DNS server that is authoritative for the zone that hosts its domain. This eliminates the need for an administrator to manage host (A or AAAA) resource records for client computers. Problems with automatic registration do not prevent a computer from accessing the network, but they can prevent other network computers from being able to locate the computer.
DNS Client Service Status	Domain Name System (DNS) is a protocol that makes it possible for a computer to obtain the numeric IP address of another computer by submitting the target computer's name to a DNS server computer. The DNS Client service sends requests for name resolution services to DNS servers. Problems with the DNS Client service can prevent a network computer from locating other network computers.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.

The Microsoft Windows Server 2003 operating system includes a DHCP Server service, which is an optional networking component. All Windows-based clients include the DHCP client as part of TCP/IP, including Windows Server 2012, 2008, 2003, Microsoft Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition (Windows Me), and Windows 98.

Benefits of DHCP

In Windows Server, the DHCP Server service provides the following benefits:

- Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- Reduced network administration. DHCP includes the following features to reduce network administration:
- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Use of DHCP

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.

DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP -enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.
- Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients.

The following table lists common terms associated with DHCP.

Term	Definition
DHCP server	A computer running the DHCP Server service that holds information about available IP addresses and related configuration information as defined by the DHCP administrator and responds to requests from DHCP clients.
DHCP client	A computer that gets its IP configuration information by using DHCP.
Scope	A range of IP addresses that are available to be leased to DHCP clients by the DHCP Server service.
Subnetting	The process of partitioning a single TCP/IP network into a number of separate network segments called subnets.
DHCP option	Configuration parameters that a DHCP server assigns to clients. Most DHCP options are predefined, based on optional parameters defined in Request for Comments (RFC) 2132, although extended options can be added by vendors or users.

Term	Definition
Option class	An additional set of options that can be provided to a DHCP client based on its computer class membership. The administrator can use option classes to sub manage option values provided to DHCP clients. There are two types of options classes supported by a DHCP server running Windows Server, vendor classes and user classes.
Lease	The length of time for which a DHCP client can use a DHCP-assigned IP address configuration.
Reservation	A specific IP address within a scope permanently set aside for leased use by a specific DHCP client. Client reservations are made in the DHCP database using the DHCP snap-in and are based on a unique client device identifier for each reserved entry.
Exclusion/exclusion range	One or more IP addresses within a DHCP scope that are not allocated by the DHCP Server service. Exclusions ensure that the specified IP addresses will not be offered to clients by the DHCP server as part of the general address pool.
DHCP relay agent	Either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet. Also referred to as a BOOTP relay agent.
Super scope	A configuration that allows a DHCP server to provide leases from more than one.

Working of DHCP

- When a client boots up for the first time (or try to join a new network), it needs to obtain an IP address to communicate. So it first transmits a DHCPDISCOVER message on its local subnet. Because the client has no way of knowing the subnet to which it belongs, the DHCPDISCOVER is an all-subnets broadcast (destination IP address of 255.255.255.255, which is a layer 3 broadcast address) and a destination MAC address of FF-FF-FF-FF-FF-FF (which is a layer 2 broadcast address). The client does not have a configured IP address, so the source IP address of 0.0.0.0 is used. The purpose of DHCPDISCOVER message is to try to find out a DHCP Server (a server that can assign IP addresses).
- After receiving the discover message, the DHCP Server will dynamically pick up an unassigned IP address from its IP pool and broadcast a DHCPOFFER message to the Client. DHCPOFFER message could contain other information such as subnet mask, default gateway, IP address lease time, and domain name server (DNS).
- When the DHCP Server receives the DHCPREQUEST message from the client, the DHCP Server accepts the request by sending the client a unicast DHCPACKNOWLEDGEMENT message (DHCPACK).

In conclusion, there are four messages sent between the DHCP Client and DHCP Server: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACKNOWLEDGEMENT. This process is often abbreviated as DORA (for Discover, Offer, Request, Acknowledgement).

After receiving DHCPACKNOWLEDGEMENT, the IP address is leased to the DHCP Client. A client will usually keep the same address by periodically contacting the DHCP server to renew the lease before the lease expires.

When a DHCP address conflict occurs

During the IP assignment process, the DHCP Server uses ping to test the availability of an IP before issuing it to the client. If no one replies, then the DHCP Server believes that IP has not been allocated and it can safely assign that IP to a client. If someone answers the ping, the DHCP Server records a conflict, the address is then removed from the DHCP pool and it will not be assigned to a client until the administrator resolves the conflict manually.

Concept of Lease

With all the necessary information on how DHCP works, one should also know that the IP address assigned by DHCP server to DHCP client is on a lease. After the lease expires the DHCP server is free to assign the same IP address to any other host or device requesting for the same. For example, keeping lease time 8-10 hours is helpful in case of PC's that are shut down at the end of the day. So, lease has to be renewed from time to time. The DHCP client tries to renew the lease after half of the lease time has expired. This is done by the exchange of DHCPREQUEST and DHCPACK messages. While doing all this, the client enters the renewing stage.

Concept of VPN, RRAS & TCP/IP routing

Objectives: At the end of this lesson you shall be able to
- **understand the concept of remote access**
- **understand the concept of virtual private network (VPN)**
- **understand the remote access authentication protocol**
- **understand the concept of IAS,TCP/IP routing.**

Routing

A router is a device that manages the flow of data between network segments, or subnets. A router directs incoming and outgoing packets based on the information it holds about the state of its own network interfaces and a list of possible sources and destinations for network traffic. Depending upon the needs based on the number and types of hardware devices and applications used in our environment, we can decide whether to use a dedicated hardware router, a software-based router, or a combination of both. Dedicated hardware routers handle heavier routing demands best, and less expensive software-based routers are sufficient to handle lighter routing loads.

A software-based routing solution, such as the Routing and Remote Access service in Windows Server 2012, can be ideal on a small, segmented network with relatively light traffic between subnets.

Remote access

By configuring Routing and Remote Access to act as a remote access server, we can connect remote or mobile workers to the organization's networks. Remote users can work as if their computers are physically connected to the network.

All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled by means of the remote access connection. For example, on a server running Routing and Remote Access, clients can use Windows Explorer to make drive connections and to connect to printers. Because drive letters and universal naming convention (UNC) names are fully supported by remote access, most commercial and custom applications work without modification.

A server running Routing and Remote Access provides two different types of remote access connectivity:

1 Virtual private networking (VPN)

2 Dial-up networking

Virtual Private Network

Virtual private networks (VPNs) are point-to-point connections across a private or public network, such as the Internet. A VPN client uses special TCP/IP-based protocols, called tunneling protocols, to make a virtual call to a virtual port on a VPN server. In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet. The remote access server answers the call, authenticates the caller, and transfers data between the VPN client and the organization's private network.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header. The header provides routing information that enables the data to traverse the shared or public network to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The link in which the private data is encapsulated and encrypted is known as a VPN connection.

There are two types of VPN connections:

1 Remote access VPN

2 Site-to-site VPN

Remote access VPN

Remote access VPN connections enable users working at home or on the road to access a server on a private network using the infrastructure provided by a public network, such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computer (the VPN client) and an organization's server. The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link.

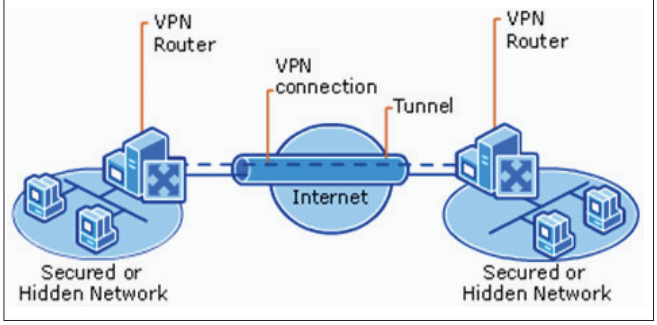
Site-to-site VPN

Site-to-site VPN connections (also known as router-to-router VPN connections) enable organizations to have routed connections between separate offices or with other organizations over a public network while helping to maintain secure communications. A routed VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link. When networks are connected over the Internet, as shown in the following figure, a router forwards packets to another router across a VPN connection. To the routers, the VPN connection operates as a data-link layer link.

A site-to-site VPN connection connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server is attached. The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for

mutual authentication, the answering router authenticates itself to the calling router. In a site-to site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers. Fig 1 shows the VPN Connecting Two Remote Sites Across the Internet.

Fig 1



Properties of VPN connections

VPN connections that use PPTP, L2TP/IPsec, and SSTP have the following properties:

1 Encapsulation

2 Authentication

3 Data encryption

Encapsulation: With VPN technology, private data is encapsulated with a header that contains routing information that allows the data to pass through the transit network.

Authentication: Authentication for VPN connections takes three different forms:

1 User-level authentication by using PPP authentication

To establish the VPN connection, the VPN server authenticates the VPN client that is attempting the connection by using a Point-to-Point Protocol (PPP) user-level authentication method and verifies that the VPN client has the suitable authorization. If mutual authentication is used, the VPN client also authenticates the VPN server, which provides protection against computers that are masked as VPN servers.

2 Computer-level authentication by using Internet Key Exchange (IKE)

To establish an Internet Protocol security (IPsec) security association, the VPN client and the VPN server use the IKE protocol to exchange either computer certificates or a preshared key

3 Data origin authentication and data integrity

To verify that the data sent on the VPN connection originated at the other end of the connection and was not modified in transit, the data contains a cryptographic checksum based on an encryption key known only to the sender and the receiver.

Data encryption

To ensure confidentiality of the data as it traverses the shared or public transit network, the data is encrypted by the sender and decrypted by the receiver. The encryption and decryption processes depend on both the sender and the receiver using a common encryption key.

Intercepted packets sent along the VPN connection in the transit network are unintelligible to anyone who does not have the common encryption key. The length of the encryption key is an important security parameter.

Installing and Enabling the Routing and Remote Access Service in Windows Server

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. The Add roles wizard can be used to install the Routing and Remote Access service. After the installation is completed, the Routing and Remote Access service is installed in a disabled state. To enable and configure the remote access server, the user must be logged on as a member of the Administrators group. To enable the Routing and Remote Access service the computer should be added to the RAS and IAS Servers security group in the domain of which the server is a member. If the server is a member of an Active Directory domain and you are not a domain administrator, instruct the domain administrator to add the computer account of this server to the RAS and IAS Servers security group in the domain. The domain administrator can add the computer account to the RAS and IAS Servers security group by using Active Directory Users and Computers or by using the netsh ras add registered server command. Open the Routing and Remote access Server Setup wizard Follow the instructions and complete the wizard.

Configure a Remote Access VPN Server

Before configuring a remote access VPN server the following things should be known.

- Determine which network interface connects to the Internet and which network interface connects to the private network.
- Determine whether remote clients will receive IP addresses from a Dynamic Host Configuration Protocol (DHCP) server on your private network or from the remote access VPN server that you are configuring.
- Determine whether you want connection requests from VPN clients to be authenticated by a Remote Authentication Dial-In User Service (RADIUS) server or by the remote access VPN server that you are configuring.
- Determine whether VPN clients can send DHCP messages to the DHCP server on your private network.
- Verify that all users have user accounts that are configured for dial-up access.

Authentication protocol

An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax. It is the most important layer of protection needed for secure communication within computer networks.

Purpose

With the increasing amount of trustworthy information being accessible over the network the need for keeping unauthorized persons from access to this data emerged. Stealing someone's identity is easy in the computing world - special verification methods had to be invented to find out whether the person/computer requesting data is correct. The task of the authentication protocol is to specify the exact series of steps needed for execution of the authentication. It must comply with the main protocol principles:

1 A Protocol has to involve two or more parties and everyone involved in the protocol must know the protocol in advance.

2 All the included parties have to follow the protocol.

3 A protocol has to be unambiguous - each step must be defined precisely.

4 A protocol must be complete - must include a specified action for every possible situation.

Remote Access Authentication Protocols

Remote access in this version of Windows supports the remote access authentication protocols listed in the following table. They are listed in order of decreasing security. We recommend that you use Extensible Authentication Protocol (EAP) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), and avoid the use of Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

Unauthenticated access

RRAS also supports unauthenticated access, which means that user credentials (a user name and password) are not required. There are some situations in which unauthenticated access is useful.

Routing and Remote Access Service

Routing and Remote Access Service (RRAS) is a Microsoft API and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router. Developers can also use RRAS to implement routing protocols. The RRAS server functionality follows and builds upon the Remote Access Service (RAS) in Windows NT 4.0. RRAS was introduced with Windows 2000 and offered as a download for Windows NT 4.0.

- Multiprotocol router - The computer running RRAS can route IP, IPX, and AppleTalk simultaneously. All routable protocols are configured from the same administrative utility. RRAS included two unicast routing protocols, Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) as well as IGMP routing and forwarding features for IP multicasting.
- Demand-dial router - IP and IPX can be routed over on-demand or persistent WAN links such as analog phone lines or ISDN, or over VPN connections.
- Remote access server - provides remote access connectivity to dial-up or VPN remote access clients that use IP, IPX, AppleTalk, or NetBEUI.

Routing services and remote access services used to work separately. Point-to-Point Protocol (PPP), the protocol suite commonly used to negotiate point-to-point connections, has allowed them to be combined.

RRAS can be used to create client applications. These applications display RAS common dialog boxes, manage remote access connections and devices, and manipulate phone-book entries.

Configuring RRAS policies to Permit or Deny Access

A traditional LAN is normally located within a single building or site. The systems within the LAN are administered by a single individual or a group of individuals and policies exist for administration and configuration. However, if users connect from outwith the LAN, the systems they connect from may not be administered by the corporate administrator or administrators. This can cause configuration problems as well as security problems.

Remote access policies help administrators apply a consistent policy to machines that are not directly administered within the corporate LAN. Administrators can use remote access policies to limit the access rights and privileges of remote users and computers by validating connections and specifying connection restrictions. Connection settings that can be validated by standard remote access policy settings include:

- Authentication methods
- Group membership
- Remote access permission
- Time of day
- Type of connection

Advanced remote access policy validation settings include the following:

- Access server identity
- Access client phone number or MAC address
- Whether user account dial-in properties are ignored
- Whether unauthenticated access is allowed

Authentication methods include the following:

- PEAP

- EAP
- MS-CHAP v1 and v2
- CHAP
- PAP
- Unauthenticated access

Internet Authentication Service (IAS)

Internet Authentication Service (IAS) is a component of Windows Server operating systems that provides centralized user authentication, authorization and accounting.

While Routing and Remote Access Service (RRAS) security is sufficient for small networks, larger companies often need a dedicated infrastructure for authentication. RADIUS is a standard for dedicated authentication servers.

Windows 2000 Server and Windows Server 2003 include the Internet Authentication Service (IAS), an implementation of RADIUS server. IAS supports authentication for Windows-based clients, as well as for third-party clients that adhere to the RADIUS standard. IAS stores its authentication information in Active Directory, and can be managed with Remote Access Policies. IAS first showed up for Windows NT 4.0 in the Windows NT 4.0 Option Pack and in Microsoft Commercial Internet System (MCIS) 2.0 and 2.5.

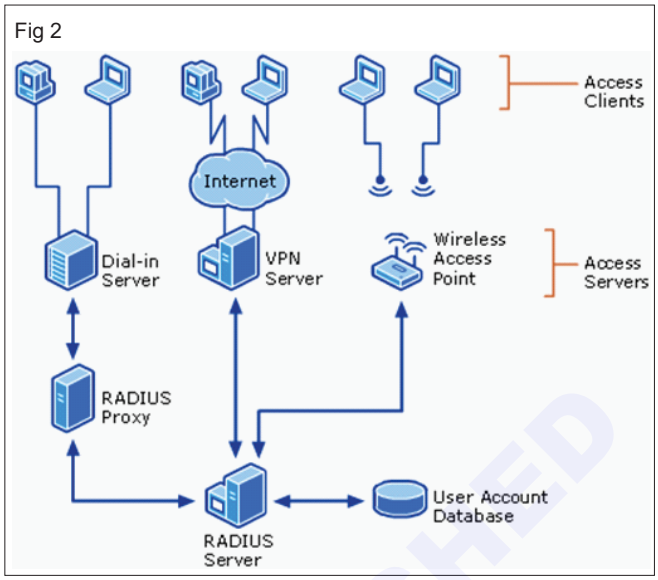
While IAS requires the use of an additional server component, it provides a number of advantages over the standard methods of RRAS authentication. These advantages include centralized authentication for users, auditing and accounting features, scalability, and seamless integration with the existing features of RRAS.

In Windows Server 2008, Network Policy Server (NPS) replaces the Internet Authentication Service (IAS). NPS performs all of the functions of IAS in Windows Server 2003 for VPN and 802.1X-based wireless and wired connections and performs health evaluation and the granting of either unlimited or limited access for Network Access Protection clients.

Components of an IAS infrastructure

There are five components to an IAS or RADIUS infrastructure: access clients, access servers (RADIUS clients), IAS servers (RADIUS servers), IAS proxies (RADIUS proxies), and user account databases. A RADIUS infrastructure is used to perform authentication, authorization and accounting of user network access attempts. Authentication is the process of verifying the credentials of the users attempting to connect to a network. The authorization process determines whether users have permission to connect to the network, and the conditions under which permission has been granted. Accounting is an option that provides record keeping of successful or failed connection attempts. (Fig 2)

Fig 2



The following figure, "Components of an IAS Infrastructure," illustrates the relationships between the five components of an IAS infrastructure.

Components of an IAS Infrastructure

Access Clients

An access client is a device that requires some level of access to a larger network. Examples of access clients are dial-up or VPN clients, wireless clients, or LAN clients connected to an authenticating switch.

Access Servers Used as RADIUS Clients

An access server is a device that provides some level of access to a larger network. An access server using a RADIUS infrastructure is also a RADIUS client, sending connection requests and accounting messages to a RADIUS server.

IAS Servers Used as RADIUS Servers

An IAS or RADIUS server is a device that receives and processes connection requests or accounting messages sent by RADIUS clients or RADIUS proxies. In the case of connection requests, the RADIUS server processes the list of RADIUS attributes in the connection request. Based on a set of rules and the information in the user account database, the RADIUS server authenticates and authorizes the connection and sends back either an Access-Accept message or an Access-Reject message. The Access-Accept message can contain connection restrictions that the access server implements the duration of the connection.

Introduction to Web Server

Objectives: At the end of this lesson you shall be able to
- **understand the functioning of web server**
- **explain the message services**
- **understand the concept of backup and recovery of server.**

Web server is a computer where the web content is stored. Web servers allows to share information over the Internet, or through intranets and extranets. Basically, web server is used to host the web sites but there exists other web servers also such as gaming, storage, FTP, email etc.

Web site is collection of web pages while web server is a software that respond to the request for web resources.

Web Server Working

Web server respond to the client request in either of the following two ways:

1 Sending the file to the client associated with the requested URL.

2 Generating response by invoking a script and communicating with database

Key Points

1 When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.

2 If the requested web page is not found, web server will send an HTTP response:Error 404 Not found.

3 If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

Architecture

Web Server Architecture follows the following two approaches:

1 Concurrent Approach

2 Single-Process-Event-Driven Approach.

Concurrent approach

Concurrent approach allows the web server to handle multiple client requests at the same time. It can be achieved by following methods:

1 Multi-process

2 Multi-threaded

3 Hybrid method.

Multi-processing

In this a single process (parent process) initiates several single-threaded child processes and distribute incoming requests to these child processes. Each of the child processes are responsible for handling single request. It is the responsibility of parent process to monitor the load and decide if processes should be killed or forked.

Multi-threaded

It creates multiple single-threaded process.

Hybrid

It is combination of above two approaches. In this approach multiple process are created and each process initiates multiple threads. Each of the threads handles one connection. Using multiple threads in single process results in less load on system resources.

Different types of web servers

There are different types of web servers available in open market. The most popular web servers are Apache, IIS, Nginx and LiteSpeed.

Apache web server (Fig 1)

Fig 1

Apache is the most popular web server in the world developed by the Apache Software Foundation. Apache is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more. About 60% of machines run on Apache Web Server.

An Apache server can be customized easily as it contains a modular structure. It is also an open source which means that you can add your own modules to the server when to require and make modifications that suit your specific needs.

It is more stable than any other web servers and is easier to solve administrative issues. It can be install on multiple platforms successfully.

Recent Apache releases provide you the feasibility of handling more requests when you compare to its earlier versions.

IIS web server (Fig 2)

Fig 2

IIS is a Microsoft product. IIS server has all the features just like Apache. But it is not an open source and more over personal modules cannot be added easily and modification becomes a little difficult job.

Microsoft developed, maintains it, thus works with all the Windows operating system platforms. Also, they had good customer support if it had any issues.

Nginx web server (Fig 3)

Fig 3

Nginx is another free open source web server, it includes IMAP/POP3 proxy server. Nginx is known for its high performance, stability, simple configuration and low resource usage.

This web server doesn't use threads to handle requests rather a much more scalable event-driven architecture which uses small and predictable amounts of memory under load. It is getting popular in the recent times and it is hosting about 7.5% of all domains worldwide.

Litespeed web server (Fig 4)

Fig 4

LiteSpeed (LSWS) is a high-performance Apache replacement. LSWS is the 4th most popular web server on the internet and it is a commercial web server.

This is compatible with most common Apache features, including mod_rewrite, .htaccess, and mod_security. LSWS can load Apache configuration files directly and works as a drop-in replacement for Apache with hosting control panels - replacing Apache in less than 15 minutes with zero downtime.

Unlike other front-end proxy solutions, LSWS replaces all Apache functions, simplifying use and making the transition from Apache smooth and easy. Most of the hosting companies were using LSWS in recent times.

Most of the web hosting companies select web server based on clients requirement, the number of clients on a single server, the applications/software clients use and the amount of traffic they generate that could handle by a web server. So, choose the web server which meets your requirements better.

Types of backup

There are quite a number of backup types and terms used when it comes to backups of your digital content. This is a compilation of the most common types of backup with a brief explanation of their meaning, common examples, advantages and disadvantages of each backup type.

Full backup

Full backup is a method of backup where all the files and folders selected for the backup will be backed up. When subsequent backups are run, the entire list of files and will be backed up again. The advantage of this backup is restores are fast and easy as the complete list of files are stored each time. The disadvantage is that each backup run is time consuming as the entire list of files is copied again. Also, full backups take up a lot more storage space when compared to incremental or differential backups.

Incremental backup

Incremental backup is a backup of all changes made since the last backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changes made since the last backup. The result is a much faster backup then a full backup for each backup run. Storage space used is much less than a full backup and less then with differential backups. Restores are slower than with a full backup and a differential backup.

Differential backup

Differential backup is a backup of all changes made since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. The result is a much faster backup then a full backup for each backup run. Storage space used is much less than a full backup but more then with Incremental backups. Restores are slower than with a full backup but usually faster then with Incremental backups.

Mirror backup

Mirror backups are as the name suggests a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident or through a virus may also cause the mirror backups to be deleted as well.

Full PC Backup or Full Computer Backup

In this backup, it is not the individual files that are backed up but entire images of the hard drives of the computer that is backed up. With the full PC backup, you can restore the computer hard drives to its exact state when the backup was done. With the Full PC backup, not only can the work documents, picture, videos and audio files be restored but the operating system, hard ware drivers, system files, registry, programs, emails etc can also be restored.

Local backup

Local backups are any kind of backup where the storage medium is kept close at hand or in the same building as the source. It could be a backup done on a second internal hard drive, an attached external hard drive, CD/ DVD -ROM or Network Attached Storage (NAS). Local backups protect digital content from hard drive failures and virus attacks. They also provide protection from accidental mistakes or deletes. Since the backups are always close at hand they are fast and convenient to restore.

Offsite backup

When the backup storage media is kept at a different geographic location from the source, this is known as an offsite backup. The backup may be done locally at first but once the storage medium is brought to another location, it becomes an offsite backup. Examples of offsite backup include taking the backup media or hard drive home, to another office building or to a bank safe deposit box.

Beside the same protection offered by local backups, offsite backups provide additional protection from theft, fire, floods and other natural disasters. Putting the backup media in the next room as the source would not be considered an offsite backup as the backup does not offer protection from theft, fire, floods and other natural disasters.

Online backup

These are backups that are ongoing or done continuously or frequently to a storage medium that is always connected to the source being backed up. Typically the storage medium is located offsite and connected to the backup source by a network or Internet connection. It does not involve human intervention to plug in drives and storage media for backups to run. Many commercial data centres now offer this as a subscription service to consumers. The storage data centres are located away from the source being backed up and the data is sent from the source to the storage data centre securely over the Internet.

Remote backup

Remote backups are a form of offsite backup with a difference being that you can access, restore or administer the backups while located at your source location or other location. You do not need to be physically present at the backup storage facility to access the backups. For example, putting your backup hard drive at your bank safe deposit box would not be considered a remote backup. You cannot administer it without making a trip to the bank. Online backups are usually considered remote backups as well.

Cloud backup

This term is often used interchangeably with Online Backup and Remote Backup. It is where data is backed up to a service or storage facility connected over the Internet. With the proper login credentials, that backup can then be accessed or restored from any other computer with Internet Access.

FTP backup

This is a kind of backup where the backup is done via FTP (File Transfer Protocol) over the Internet to an FTP Server. Typically the FTP Server is located in a commercial data centre away from the source data being backed up. When the FTP server is located at a different location, this is another form of offsite backup.

Managing network traffic & types of server services

Objectives: At the end of this lesson you shall be able to
- **understand the concepts network traffic**
- **explain tools and techniques used to manage network traffic**
- **understand the internet connectivity problems**
- **understand the types and working of server services.**

Introduction

Computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs, or WANs.

Network traffic can be defined in a number of ways. But in the simplest manner we can define it as the density of data present in any Network. In any computer Network, there are a lot of communication devices trying to access resources and at the same time getting requests to carry out some work for some other device.

Also at the same time certain types of communication devices may be busy to respond to the request being made to them. So there is lot of information exchange in the Network in form of request, response and control data. This data is basically in the form of a huge number of packets floating around in the Network.

This huge amount of data acts as a load on the Network, which results in slowing down the operations of other communication devices. Due to this there is a lot of delay in communication activities. This ultimately results in congestion of the Network.

This is the description of Network Traffic in its simplest form. In other words we can say that Network traffic is the load on the communication devices and the system.

This traffic on the network has now resulted in mid-sized and large organizations realizing that they must control network traffic behavior to ensure that their strategic applications always get the resources they need to perform

optimally. Controlling network traffic requires limiting bandwidth to certain applications, guaranteeing minimum bandwidth to others, and marking traffic with high or low priorities. This is called traffic management.

General processes for traffic management

Traffic Management consists of the amalgamation of a number of activities as shown below: (Fig 1)

Technique for measure network traffic

One of the easiest ways to comprehend Network Traffic is to consider an analogy with the road traffic. Consider that there is an emergency and someone has fallen sick and has to be rushed to the hospital. But when the ambulance tries to make its way through the roads of the city, it finds the roads totally blocked with cars n busses. The solution to this situation would be for a traffic policeman to step in and manage the traffic. He will first gauge the traffic, and then prioritize the traffic. The ambulance will get the highest priority and the road will be made empty for the ambulance to pass. Similar is the case with Network Traffic.

Fig 1

When you send a request on the network, it is possible that due to some problem or other requests you have to wait for some time. If over a period of time a number of packets queue up and wait then it results in traffic.

Once traffic is created, you must wait till it is over, which can be for any length of time, depending on the situation. So, there has to be some way to deal with this situation. The solution for this is Network Traffic Management and this process starts first with measuring the traffic on the network.

Reasons to measure network traffic

The following are the reasons for which we have measure the network traffic.

a **Service monitoring -** Making sure things keep working.

b **Network planning -** Deciding when more capacity is needed.

c **Cost recovery -** Session times and traffic volumes can provide billing data.

d **Research -** An improved understanding of what's happening should allow us to improve network performance.

Internet traffic

The basic performance metrics of Internet traffic can be listed as:

- Packet loss
- Delay
- Throughput
- Availability

Drivers for measurement

There are number of other drivers strongly deals with requirement of measurement are:

- Pricing
- Service level agreements
- New services
- Applications

Network Traffic Measure

Usually, traffic management is deployed at the WAN edge of an enterprise site. This is where the high-speed LAN meets the lower-speed WAN access link. The LANWAN

juncture is also where both Internet and intranet traffic enter and exit the enterprise. So it is the ideal place to "tame" traffic and to mitigate the impact of noncritical and even suspicious traffic picked up on the Internet.

Limiting or blocking the network resources available to frivolous or undesirable traffic boosts the performance of enterprise resource planning (ERP), customer relationship management (CRM), and other strategic, business critical applications.

In addition to monitoring traffic at the network edge, there are pure performance issues to consider. The WAN access network is usually slower than the LAN, generally for budgetary reasons.

Also Businesses pay recurring monthly fees for WAN services, while LAN bandwidth is free (after the initial equipment investments have been made). With high-speed LAN traffic slowing down at the lower-speed access circuit, the LAN-WAN edge is where congestion is most likely to occur.

Another important factor to consider here is that most applications have been developed to run on LANs. Now, local networks are generally free from congestion and fall under the total control of an internal IT department.

These LAN-optimized applications behave differently in the WAN environment. Not only is the WAN access link slower, but WAN service also can fall under the management purview of multiple network providers. Managing traffic in this network segment aids distributed organizations that depend on the WAN to serve remote users with centralized resources.

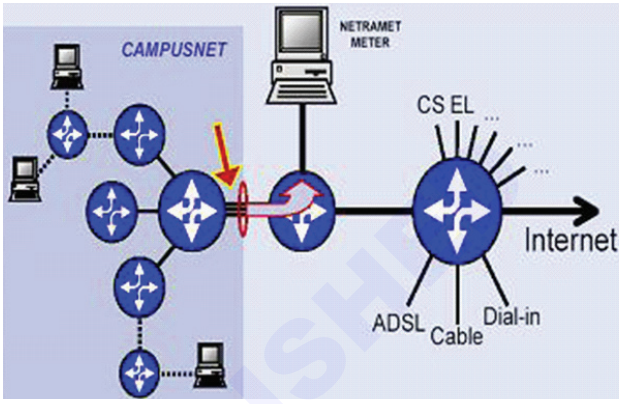
Doing so is a reasonably simple matter. In most cases, a network administrator uses a GUI to set parameters for some business-critical policies in plain English. The administrator then pushes a button to propagate those policies to the various network segments where they should be enforced.

Approaches for traffic measurement

There are some approaches for traffic measurement as follows

Active Measurement of Traffic (Fig 2)

Fig 2



As name indicates, in this measurement approach users or providers are directly related to the activities to the measurement. There are number of different ways to carry out this measurement like.

i Injection of probes into network by users and providers.

ii Ping and Trace out the Path connectivity and Roundtrip delay.

iii User-application performance as seen from hosts like Loss, Delay and Throughput.

iv Distribute on measurement servers makes the Probes are spread across mesh of paths through network to check scalability and growth of probe traffic.

Passive Measurement of Traffic

In this approach user is indirectly deal with system using some hardware or software tools. Basically some historical data is used to find the current traffic measurement. The currently used techniques for this type of measurement are as follows..

i **Packet monitors:** This can be achieved by recording packet headers on link. It requires unique detail of protocol and architecture studies

ii **Router / Switch traffic statistics:** Analyzing router or switch, the intelligent devices installed at network, can provide network internal behavior. Using these devices we can get information about Packet drops, Counts and Flow statistics.

iii **Server and router logs:** These records or logs can perform well work in measuring. They provide summaries of dial session, routing updates or web-server log.

Traffic analysis

After consecutive monitoring over a number of years, LAN and WAN traffic have been seen to follow different patterns.

LAN Traffic

Traffic on a LAN has shown to be self similar in nature. Those means if I measure the traffic over a period of one hour and plot it, it will be similar to the graph for the

traffic plotted over a period of one day. In the same manner the day graph will be similar to the traffic graph plotted over a week and the week graph for that of a month.

The patter of the variation of the traffic repeats itself over regular intervals.

WAN Traffic

Traffic on the WAN has been found to vary as per the following models.

Random Traffic: The traffic here seems to follow no fixed pattern.

Poisson's Model: Traffic Nature in Internet has been identified to confirm to the Poisson's Model. This model gives us a rough idea of the characteristics of Internet Traffic.

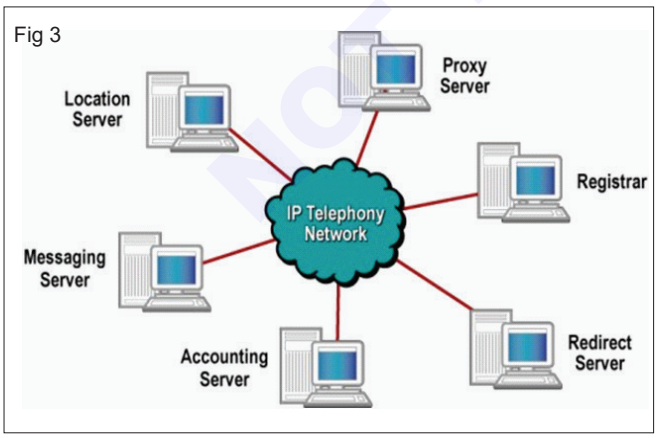
The model estimates the probability of the number of packets that should be present on the network after a given time if the average arrival rate of the packets is specified.

Bursty Traffic: This model states that, the average traffic over the network stays roughly constant, except for the sudden bursts (long and short).

Types of Servers and its functions

The history of servers moves parallel to the history of computer networks. The computer networks allow multiple computer systems to communicate with each other at the same time. Its evolution was expected to assign some computers with some serving role where all other computers that are in direct interaction with the human users, perform as clients. (Fig 3)

Fig 3



There are multiples types of servers that have grown along with the development and rapid growth of the types of networks. To do the job of serving, servers and associated software are manufactured.

The origin of the server is to 'serve' - technically it means that the specific computer is serving all those computers that are present in its network. It facilitates them by making a queue of the printing command of several computers at a time and also acts as a file server for those applications that are accessed by the online terminals.

Today, the role of the server is similar to that of microcomputers of the past which are now substituted. For this role, many servers are appointed but this allocation does not limit the role of a server as many other roles can be assigned to the server simultaneously. For instance, we can take the example of a small office where a desktop computer can serve all other computers present within the office while simultaneously serving as a workstation for some employee.

For this role, many servers are appointed but this allocation does not limit the role of a server as many other roles can be assigned to the server simultaneously. For instance, we can take the example of a small office where a desktop computer can serve all other computers present within the office while simultaneously serving as a workstation for some employee.

Types of servers: What are the types of servers available with brief information

Typically servers are of four types, but due to an exponential growth in networking technologies, we are witnessing multiple other server types. I've taken a liberty it explain most of them below.

Traditionally know servers are:

1 FTP servers

2 Proxy servers,

3 Online game servers

4 Web servers.

1 FTP Server

File Transfer Protocol (FTP) is one of the oldest server types. It is responsible for transferring files from server to a computer and vice versa. FTP server ensures the security and integrity of data during the transfer. It is commonly used by web servers, it enables user to upload, edit or delete files from websites using FTP clients.

2 Proxy Servers

The Proxy server is responsible for a connection between a client(web browser or an app) with and an external server to entertain the request for connection, performance enhancement, and accessibility.

Consider an example of the restricted website or an app, if you connect your computer/ smartphone with a proxy server, it will update its IP geographical location and let you access the restricted data.

3 Online Gaming Server

Gaming server has gained its popularity in a recent decay. This type of server is responsible for connecting hundreds of gamers around the world to an external server(s) for accessing gaming data.

> **Xbox live is one of the examples for gaming servers. We can also develop our own gaming servers at home to play games with our friends under one roof. A normal computer can perform as a server, every other computer will make a connection to a gaming server and access gaming data and play a game.**

4 Web servers

The web server is responsible for hosting website files and serve it up through a web browser. It loads an individual file of a web page and loads it to display in the browser as one complete page. HTTP or HTTPS (Hypertext Transfer Protocol or Hypertext Transfer Protocol Secure) communicate between server and web browser to load a web page.

As an example consider this:

> **Right now the browser is accessing a web page "http://wifinotes.com/computer-networks/server-types.html". When clicked this page in search engine, the web browser communicated with a web server downloaded individual files on the computer and displayed it for to read.**

You can convert any computer into a web server by installing server software and connect that machine to the internet.

Here are some other types of servers that you should read about.

Application Servers

Application servers have lion's share in computer territory between database servers and the end user, where servers are often connected to the two. They are often referred as middleware. Middleware is that software which establishes a connection between two separate applications that are otherwise apart. A number of middleware products can link a database system to a Web server. It enables users to request data from database by the help of those forms that are displayed on a Web browser and based on the users' profile and request, allowing the Web server to return dynamic Web pages.

Middleware is that software which establishes a connection between two separate applications that are otherwise apart. A number of middleware products can link a database system to a Web server. It enables users to request data from database by the help of those forms that are displayed on a Web browser and based on the users' profile and request, allowing the Web server to return dynamic Web pages.

List Servers

List servers are used to enhance the functionality & management of mailing lists. Whether they are an interactive database that is open to the public or one-way lists that deliver newsletters, announcements or advertising.

Chat Servers

This server enables a number of people to share information in the environment of an internet newsgroup that offer real-time discussion capabilities. It is used to refer to a number of different features of a computer. To immediately respond to the input real-time operating systems are used.

IRC Servers

Internet Relay Chat is comprised of various independent networks of servers that allow users to connect to each other via an IRC network. It is an option for those who are seeking real-time competence.

Fax Servers

Those organizations that want to reduce the incoming and outgoing telephone resources; a fax server is an ideal solution. However, there is a need to fax the actual document.

Groupware Servers

It is software that is designed to make the users able to work together, regardless of their location, through the Internet or a corporate Intranet and to work together in a virtual environment.

Mail Servers

The mail server just is as important as a web server is. A mail server is to send/receive and store emails on the corporate networks through LANs and WANs and across the internet.

Telnet Servers

By the help of it, users log on to a host computer and perform work as if they are working on an isolated computer.

News Servers

They work as a source of distribution and delivery for hundreds of available public newsgroups accessible over the USENET news network. USENET is global bulletin board system that can be approached via the internet or via a variety of online services

The role played by the servers in a networking is very significant. An out of order server can halt the interconnectivity of all computers on its network. The rise in the usage of internet in homes and office users along with the increase in corporate computer networks are responsible for boosting the development of server and its types.

Functions of Linux Server

Objectives: At the end of this lesson you shall be able to
- **understand the linux server installation and configuration**
- **understand the concept of public and data directory**
- **understand the concept of SWAT and telnet.**

Linux Server Introduction

A Linux server is an efficient, powerful variant of the Linux open source operating system (OS). Linux servers are designed to handle the more demanding requirements of business applications like system and network administration, Web services and database management. Linux servers are often preferred over other server operating systems because of their reputation for security, consistency and flexibility. It is a computer that runs the Linux operating system and is dedicated to serving other computers or clients on a network. Some examples of Linux server operating systems are CentOS, Ubuntu Server, Gentoo, Debian, Slackware, Suse and so on.

Features of Linux servers

1 **Open-Source:** Linux is an open-source operating system. Linux is an attractive choice for servers because it provides more flexibility, customizability, and cost-effectiveness.

2 **Stability:** Linux is known for its stability and reliability. It can run for months or even years without needing to be restarted, making it a popular choice for critical applications such as web servers, database servers, and mail servers.

3 **Security:** Linux is more secure than other operating systems because it is less prone to viruses, malware, and other security threats. It also has built-in security features which prevent unauthorized access and attacks.

4 **Flexibility:** Linux is highly customizable and can be configured to suit a wide range of needs. It supports a variety of programming languages and applications.

5 **Cost-effectiveness:** Linux is free to download, use, and distribute, which makes it a cost-effective choice for servers. It also has lower hardware requirements compared to other operating systems, which can save on hardware costs.

6 **Performance:** Linux is known for its excellent performance, especially when it comes to running multiple processes simultaneously. This makes it ideal for servers that need to handle a high volume of traffic.

7 **Community Support:** Linux has a large and active community of developers and users who provide support, guidance, and resources.

8 **Multitasking:** Multitasking, or the ability to run multiple programs or tasks simultaneously, is supported by Linux.

9 **No Downtime:** Virtually all updates are applied without taking the system offline. In addition, Linux-run servers rarely require a restart to correct errors or complete updates. This means practically no downtime.

Configuration Plan

A configuration plan for a server is the methods and procedures necessary to configure and set up a server to satisfy certain needs and requirements are described in depth in a configuration plan for a server. A list of the hardware and software parts, network settings, security precautions, user accounts, and backup and recovery processes are usually included. The configuration plan is a crucial tool for making sure the server is configured properly and functions consistently and effectively. It also serves as a reference guide for troubleshooting and maintenance activities. The steps are as follows:-

1 **Choose a Linux distribution**: There are many Linux distributions available, such as Ubuntu, CentOS, Debian, and Fedora. Choose the one that best fits your needs and expertise.

2 **Install the operating system**: Install the server operating system using a CD or DVD, USB drive, or network boot.

3 **Update the operating system**: Update Operating system to the latest version. This ensures that your system has the latest security patches and bug fixes.

4 **Configure network settings**: Configure your network settings, such as IP address, DNS, and gateway. This is important for your server to communicate with other devices on the network.

5 **Install necessary software**: Install the necessary software packages for your server. This includes web servers, database servers, mail servers, etc. You can use package managers like apt-get or yum to install software.

6 **Configure security**: Configure firewalls, secure shell (SSH), and other security settings to protect your server from unauthorized access.

7 **Create user accounts**: Create user accounts for users who will be accessing your server. This allows them to log in and perform their tasks.

8 **Backup and recovery:** Set up a backup and recovery system for your server to prevent data loss in case of any disaster.

9 **Monitor and maintain:** Monitor your server regularly and perform maintenance tasks such as disk cleanup, log management, and performance tuning.

Public and Data directory

Public directory

It is a directory that can be accessed by all users on the server or on the network. It is typically used to share files and resources that can be accessed by anyone. For example, if you have a file that you want to make available to other users on the server, you can place it in the public directory. By default, the public directory has read-only permissions for others, but you can change the permissions to allow users to modify the files in the directory.

Data directory

It is a directory where data files are stored. It is typically used to store application data, database files, log files, and other types of data that are required for the server to function. The data directory may be specific to a particular application or used as a general storage location for data files.

Depending on the server's particular configuration and requirements, the public and data directories may be placed in various places. These directories can be manually established and configured afterwards or specified during the server setup or installation procedure.

Host File

All operating systems with network support have a hosts file to translate hostnames to IP addresses. Whenever you open a website by typing its hostname, your system will read through the hosts file to check for the corresponding IP and then open it. The hosts file is a simple text file located in the /etc folder on Linux and Mac OS (/etc/hosts). Windows has a hosts file as well, on Windows you can find it in Windows\System32\drivers\etc\.

In a Linux server, the hosts file is a plain text file that maps hostnames to IP addresses. It is used to resolve hostnames to IP addresses locally, without requiring a DNS server. The hosts file is located in the /etc directory and is named hosts.

By editing the hosts files, you can achieve the following things:

- Block a website
- Handle an attack or resolve a prank
- Create an alias for locations on your local server
- Override addresses that your DNS server provides
- Control access to network traffic

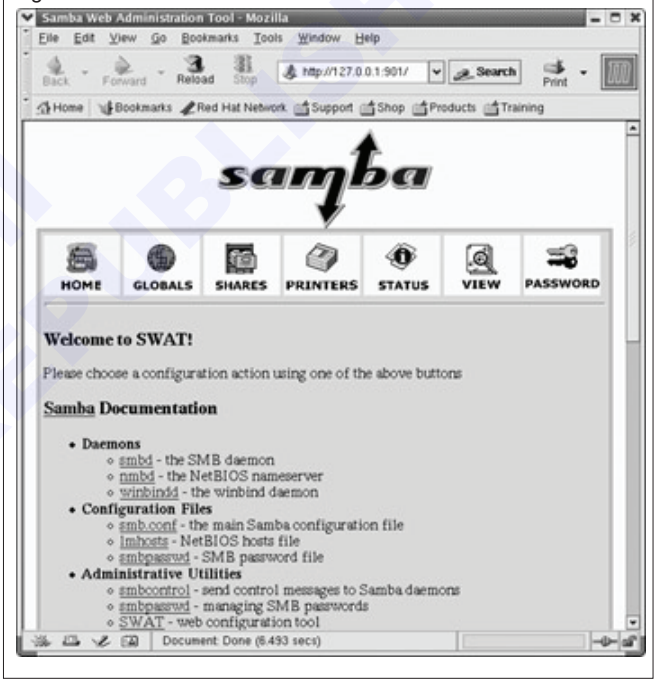
You can edit the hosts text file located at /etc/hosts only as a superuser. You will first have to open it in text editors such as VI editor, Nano editor or gedit, etc. in the Linux terminal. You will then make the required changes and save the file for these changes to take effect. Use the vi editor to edit the file. Please type the following command:

```
$ sudo vi  /etc/hosts
```

Samba Web Administration Tool (SWAT)

SWAT stands for "Samba Web Administration Tool," which is a web-based graphical user interface (GUI) that allows you to manage Samba server configurations on Linux and other Unix-like operating systems. Samba is an open-source software suite that provides file and print services to Windows clients, allowing Linux servers to act as file servers and printers for Windows clients. (Fig 1)

Fig 1



SWAT is a network-based Samba configuration tool that uses a Web page interface to enable you to configure your smb.conf file. SWAT is, by far, the easiest and simplest way to configure your Samba server. SWAT provides a simple-to-use Web page interface with buttons, menus, and text boxes for entering values. A simple button bar across the top enables you to select the sections you want to configure. A button bar is even there to add passwords. To see the contents of the smb.conf file as SWAT changes it, click View. The initial screen (HOME) displays the index for Samba documentation. One of SWAT's more helpful features is its context-sensitive help.

To use SWAT in Linux server, you need to follow these steps:

1 Install Samba on your Linux server using the appropriate package manager for your Linux distribution.

2 Install the SWAT package on your Linux server using the appropriate package manager for your Linux distribution.

3 Enable the SWAT service in samba configuration file (smb.conf)

4 Start the Samba service for your Linux distribution.

5 Open a web browser and navigate to the SWAT URL, which is typically http://localhost:901/.

6 If you are accessing SWAT from a remote computer, replace “localhost” with the IP address of your Linux server.

7 Log in to SWAT using the root user credentials or a user with sudo privileges.

8 Use the web-based interface to manage and configure your Samba server settings, including shares, users, printers, and more.

Telnet

Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Telnet was initially developed for private use where security was not primary concern. Telnet protocol has serious security issue. Security expert recommend that the use of Telnet for remote login should be discontinued under all normal circumstances.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host, including most network equipment and operating systems with a configuration utility (including systems based on Windows NT).

Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often feasible to eavesdrop on the communications and use the password later for malicious purposes; anybody who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login, password and whatever else is typed with a packet analyzer.

Security issue with Telnet

- Telnet by default does not encrypt any data sent over the connection.
- Anyone who has access to network device located on the network between the two hosts like router, switch, hub or gateway where Telnet is being used can intercept the packets passing by and obtain login, password and whatever else is typed with a packet sniffer software.
- Telnet protocol have no implementations that would ensure that communication is carried out between the two hosts is not intercepted in the middle.

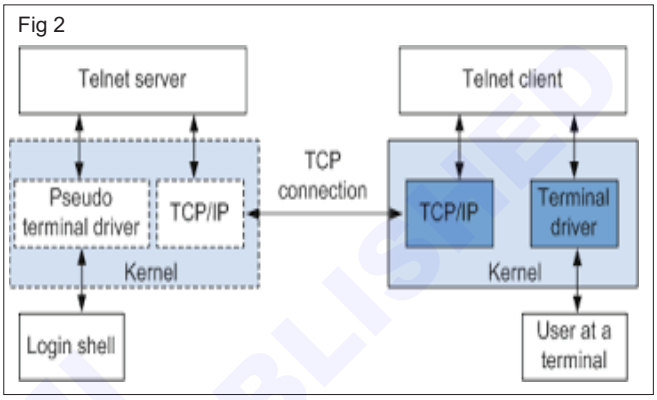
Telnet sever

Telnet server software is installed on remote host. To configure it before client can connect with it.

Telnet client

Telnet client software allows connecting to a telnet server. Once telnet client establishes a connection to the remote host, client becomes a virtual terminal, allowing communicating with the remote host from the computer. (Fig 2)

Fig 2



The Telnet program runs on the computer and connects a PC to a server on the network. Then enter commands through the Telnet program and they will be executed as directly on the server console. This enables to control the server and communicate with other servers on the network. To start a Telnet session, log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Establishing Telnet connection

Telnet client contacts the host using its internet address. When contact to a host, the distant computer and client computer negotiate how they will communicate with each other. They decide which terminal emulation will be used. Telnet emulation determines how the keyboard will transmit information to the distant computer and how information will be displayed on the screen.

Enabling Telnet in ubuntu server 14.04

Install the Telnet server with sudo apt-get install xinetd telnetd.

The service should be fired-up automatically once the installation is done. Check the service status if it is required using the command sudo /etc/init.d/xinetd status.

To Telnet an IP use the command telnet server ip

To change the telnet ports edit the file /etc/services with the line ; telnet 23/tcp.

Once changed, to apply the changes restart the telnet service by the command sudo /etc/init.d/xinetd restart.

Password Authentication

The Password Authentication Protocol (PAP) provides a simple method for the peer to establish its identity using a two-way handshake. After the link is established, an ID and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated. This is done only upon initial link establishment.

For interfaces with PPP encapsulation, you can configure interfaces to support the PAP, as defined in RFC 1334, PAP Authentication Protocols. If authentication is configured, the PPP link negotiates using CHAP or PAP protocol for authentication during the Link Control Protocol (LCP) negotiation phase. PAP is only performed after the link establishment phase (LCP up) portion of the authentication phase.

During authentication, the PPP link sends a PAP authentication-request packet to the peer with an ID and password. The authentication-request packet is sent every 2 seconds, similar to the CHAP challenge, until a response (acknowledgment packet or non acknowledgment packet) is received. If an acknowledgment packet is received, the PPP link transitions to the next state, the network phase. If a non acknowledgment packet is received, an LCP terminate request is sent, and the PPP link goes back to the link establishment phase.

If no response is received, and an optional retry counter is set to true, a new request acknowledgment packet is resent. If the retry counter expires, the PPP link transitions to the LCP negotiate phrase.

You can configure the PPP link with PAP in passive mode. By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation. In passive mode, the interface does not authenticate the peer.