AIM

TO ACQUAINT THE CLASS ABOUT INTRODUCTION TO HARDWARE AND SOFTWARE

Introduction :- A computer is a programmable electronic device capable of storing, processing, and retrieving data. It operates under the control of instructions stored in its memory unit and can perform a variety of tasks, ranging from simple arithmetic calculations to complex simulations and data analysis. Computers come in various forms, including desktops, laptops, tablets, smartphones, and servers. They consist of hardware components such as the central processing unit (CPU), memory (RAM), storage devices (hard drives or solid-state drives), input/output devices (keyboard, mouse, monitor, etc.), and networking components. Additionally, computers rely on software, which includes operating systems, applications, and utility programs, to carry out specific functions and tasks.

PART – I WHAT IS COMPUTER HARDWARE

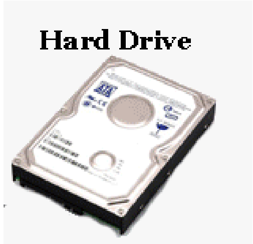
Computer hardware refers to the physical components that make up a computer system. These components are tangible and can be touched or seen. Hardware encompasses a wide range of parts, including:-

a) Central Processing Unit (CPU):- Often referred to as the brain of the computer, the CPU performs calculations and executes instructions.

b) Motherboard:- The main circuit board that houses the CPU, RAM, storage devices, and other essential components. It provides the connections between these components and allows them to communicate with each other.

c) RAM (Random Access Memory):- Temporary memory that stores data and instructions that the CPU needs to access quickly. RAM is volatile, meaning it loses its data when the computer is powered off.

d) Storage Devices:- These devices store data permanently or temporarily. Examples include Hard Disk Drives (HDDs), Solid-State Drives (SSDs), and optical drives (such as CD/DVD drives).



e) Power Supply Unit (PSU):- Converts AC power from the electrical outlet into DC power that the computer's components can use. It provides power to the motherboard, CPU, GPU, and other peripherals.

f) Cooling System:- Components such as fans, heat sinks, and liquid cooling systems are used to dissipate heat generated by the CPU, GPU, and other components to prevent overheating.

g) Peripheral Devices:- Input and output devices that enable interaction with the computer. Examples include keyboards, mice, monitors, printers, scanners, and external storage devices.

h) Expansion Cards:- Additional circuit boards that can be installed on the motherboard to add functionality. Examples include sound cards, network interface cards (NICs), and expansion cards for additional USB or PCIe slots

Expansion Card

i) Cables and Connectors:- Used to connect various hardware components to each other and to external devices. Examples include SATA cables for connecting storage drives, power cables, USB cables, and HDMI cables.

1. How do work computer hardware ?

Computer hardware works together to perform various functions necessary for the operation of a computer system. Here's a general overview of how computer hardware components work together:-

a) **Central Processing Unit (CPU):-** The CPU is the primary component responsible for executing instructions and performing calculations. It fetches instructions from memory, decodes them, executes them, and then stores the results. The CPU communicates with other components via the motherboard's data bus.

b) **Motherboard:-** The motherboard serves as the central hub that connects all hardware components together. It provides slots and sockets for attaching the CPU, RAM, expansion cards, storage devices, and other peripherals. Additionally, the motherboard contains controllers and interfaces for managing data transfer between components.

c) **RAM (Random Access Memory):-** RAM stores data and instructions that the CPU needs to access quickly. When a program is running, its data and instructions are loaded into RAM for fast access. RAM is volatile, meaning it loses its contents when the computer is powered off.

d) **Storage Devices:-** Storage devices, such as hard disk drives (HDDs) and solid-state drives (SSDs), store data permanently or temporarily. Operating systems, applications, and user files are stored on these devices. When data is needed, it is retrieved from storage and loaded into RAM for processing by the CPU.

e) **Graphics Processing Unit (GPU):-** The GPU is responsible for rendering images, videos, and animations. It offloads graphical processing tasks from the CPU, allowing for smoother graphics performance in games, video editing, and graphical applications.

f) **Power Supply Unit (PSU):-** The PSU converts AC power from the electrical outlet into DC power that the computer's components can use. It provides power to the motherboard, CPU, GPU, storage devices, and other peripherals.

g) **Cooling System:-** The cooling system, which includes fans, heat sinks, and sometimes liquid cooling solutions, helps dissipate heat generated by the CPU, GPU, and other components. This prevents overheating and ensures the reliable operation of the hardware.

h) **Peripheral Devices:-** Input and output devices, such as keyboards, mice, monitors, printers, and scanners, enable interaction with the computer. They allow users to input commands and receive feedback from the system.

i) Expansion Cards:- Expansion cards, such as sound cards, network interface cards (NICs), and graphics cards, add functionality to the computer beyond what is provided by the motherboard's built-in components. They are inserted into expansion slots on the motherboard and communicate with other hardware components via the motherboard's data bus.

j) Cables and Connectors:- Cables and connectors are used to connect hardware components to each other and to external devices. They transmit data, power, and signals between components, enabling communication and functionality.

Overall, computer hardware components work together seamlessly to execute instructions, store and retrieve data, render graphics, provide power, and enable user interaction, resulting in the operation of a fully functional computer system.

Part – II What is computer software ?

Computer software refers to a collection of instructions, programs, and data that enable a computer system to perform specific tasks or functions. Unlike hardware, which consists of physical components, software is intangible and exists as code written in programming languages.

Software can be broadly categorized into two main types:-

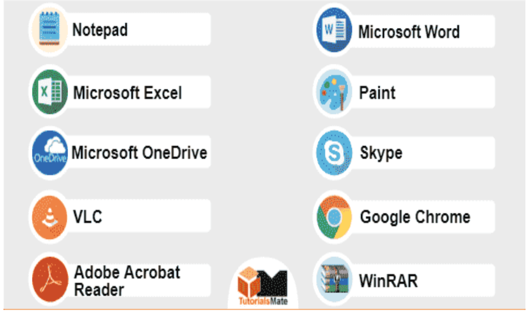
1. System Software:- System software serves as a platform for running application software and provides essential functions for the operation of a computer system. Examples of system software include:-

a) **Operating Systems (OS):-** An operating system is the fundamental software that manages hardware resources, provides user interfaces, and supports the execution of applications. Popular operating systems include Microsoft Windows, macOS, Linux, and Unix.

b) **Device Drivers:-** Device drivers are software components that facilitate communication between the operating system and hardware devices. They allow the operating system to control and interact with devices such as printers, graphics cards, and network adapters.

c) **Utility Programs:-** Utility programs perform specific tasks related to system maintenance, optimization, and security. Examples include antivirus software, disk cleanup tools, backup software, and system monitoring utilities.

2. Application Software:- Application software is designed to perform specific tasks or provide solutions for end-users. It includes a wide range of programs tailored to various purposes and industries. Examples of application software include:-



a) Word Processors:- Programs like Microsoft Word, Google Docs, and LibreOffice Writer are used for creating, editing, and formatting documents.

b) Spreadsheets:- Applications like Microsoft Excel, Google Sheets, and Libre Office Calc enable users to create and manipulate spreadsheets for numerical analysis and data management.

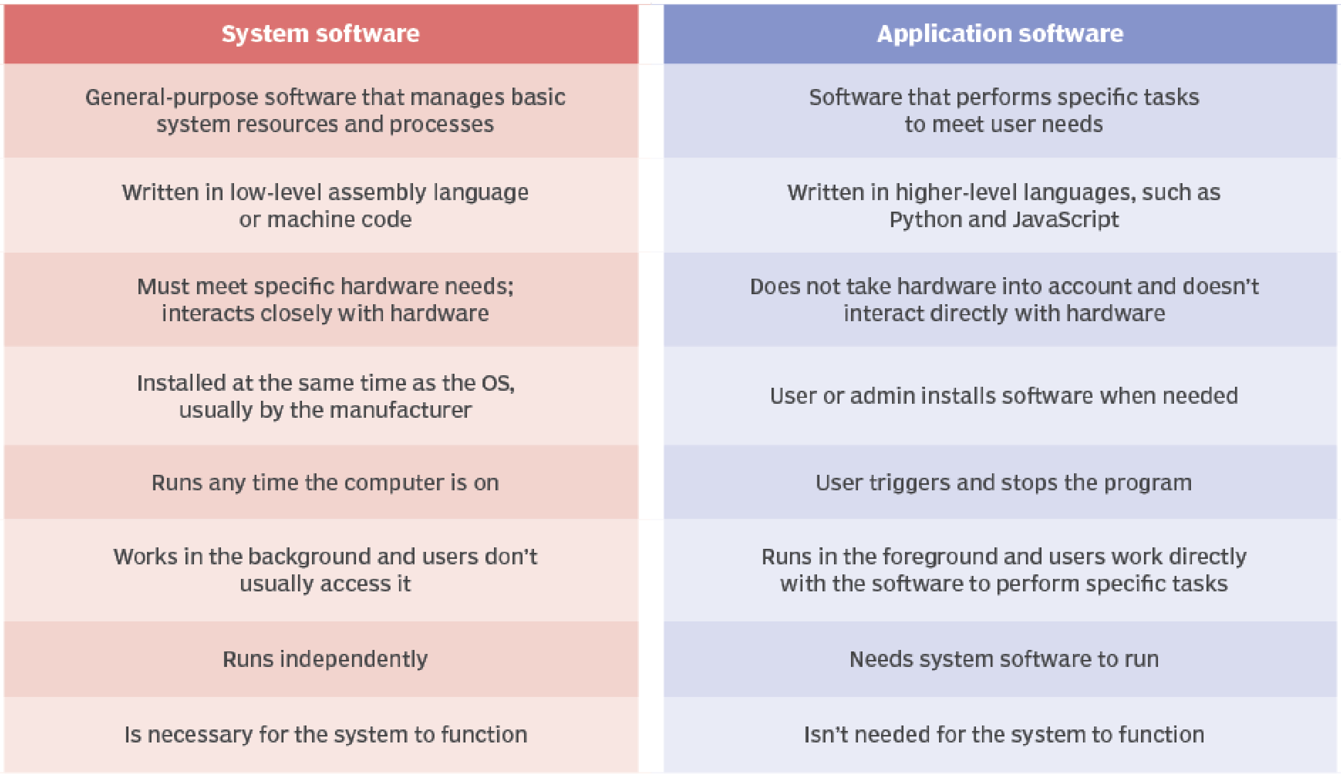
c) Graphics and Multimedia Software:- Software such as Adobe Photoshop, Adobe Premiere Pro, and Corel DRAW allows users to create, edit, and manipulate images, videos, and other multimedia content.

d) Web Browsers:- Web browsers like Google Chrome, Mozilla Firefox, and Microsoft Edge enable users to access and interact with content on the World Wide Web.

e) Enterprise Software:- Business applications like customer relationship management (CRM) software, enterprise resource planning (ERP) systems, and accounting software provide solutions for managing various aspects of business operations.

Software plays a critical role in enabling computers to perform diverse tasks and fulfill user needs. It interacts with hardware components to execute instructions, process data, and provide functionality, thereby enabling users to accomplish specific objectives efficiently and effectively.

Difference between system software & Application software



System software	Application software
General-purpose software that manages basic system resources and processes	Software that performs specific tasks to meet user needs
Written in low-level assembly language or machine code	Written in higher-level languages, such as Python and JavaScript
Must meet specific hardware needs; interacts closely with hardware	Does not take hardware into account and doesn't interact directly with hardware
Installed at the same time as the OS, usually by the manufacturer	User or admin installs software when needed
Runs any time the computer is on	User triggers and stops the program
Works in the background and users don't usually access it	Runs in the foreground and users work directly with the software to perform specific tasks
Runs independently	Needs system software to run
Is necessary for the system to function	Isn't needed for the system to function

What is Windows based operating system? Windows_Operating System (OS) is a graphical user interface (GUI) based operating system developed by Microsoft Corporation. It is designed to provide users with a user-friendly interface to interact with their computers.

Editions of MIcrosoft Windows

What is Linux OS?

Linux is a Unix-like, open source and community-developed operating system (OS) for computers, servers, mainframes, mobile devices and embedded devices. It is supported on almost every major computer platform, including x86, ARM and SPARC, making it one of the most widely supported operating systems.

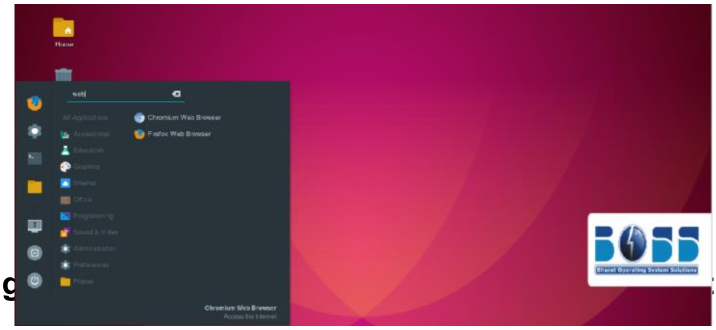
```
alex  ~  Apricity-OS-Git  git push origin master                        master
Username for 'https://github.com': agajews
Password for 'https://agajews@github.com':
Counting objects: 2862, done.
Delta compression using up to 4 threads.
Compressing objects: 100% (2604/2604), done.
Writing objects: 100% (2862/2862), 198.74 MiB | 5.22 MiB/s, done.
Total 2862 (delta 475), reused 0 (delta 0)
remote: warning: GH001: Large files detected. You may want to try Git Large File
 Storage - https://git-lfs.github.com.
remote: warning: See http://git.io/iEPt8g for more information.
remote: warning: File nylas-n1/data.tar.gz is 66.21 MB; this is larger than GitH
ub's recommended maximum file size of 50.00 MB
remote: warning: File nylas-n1/pkg/nylas-n1/usr/share/nylas/nylas is 52.63 MB; t
his is larger than GitHub's recommended maximum file size of 50.00 MB
remote: warning: File nylas-n1/pkg/nylas-n1/usr/share/nylas/resources/app.asar i
s 69.02 MB; this is larger than GitHub's recommended maximum file size of 50.00
MB
remote: warning: File nylas-n1/src/usr/share/nylas/nylas is 52.63 MB; this is la
rger than GitHub's recommended maximum file size of 50.00 MB
To https://github.com/agajews/ApricityOS.git
   6e82bcf..f179e2c  master -> master
alex  ~  Apricity-OS-Git  cd build                                      master
alex  ~  Apricity-OS-Git  build                                         master
```

Sr No	**Advantages**	**Sr No**	**Disadvantages**
1.	Graphical User Interface (GUI)	1.	Security Concerns
2.	Unser Friendly Interface and Easy to Use	2.	Paid Software
3.	Compatible to All Hardware	3.	Expensive
4.	Support Plug and Play Feature	4.	Poor Technical Support
5.	Provide Software Development Support	5.	Need of System Rebooting
6.	Have Both Desktop and Touch Screen Support		

Sr No	Advantages	Sr No	Disadvantages
1.	Open source operating sys	1.	Command line interface (CLI)
2.	Linux is more secure	2.	It is not very user friendly
3.	The software updates in linux are easy	3.	It may be confusing begginers
4.	Free avlb on internet	4.	It has small peripheral drivers
5.	It has large community support		
6.	It provide high stability		

What is a BOSS operating system ?

Bharat Operating System Solutions, commonly referred to as BOSS, is a group of several Open Source operating system derivatives, all of which are developed by CDAC, Chennai in order to benefit the usage of Free/Open Source Software in India. BOSS GNU/Linux is a key deliverable of NRCFOSS.



Bharat Operating **ion based on Debian**

Initial release **: 10 January 2007 (17 years ago)**

Developer **: Centre for Development of Advanced Computing**

Available in **: 19 languages**

Latest release **: 9.0 ("Urja") / 19 February 2021**

OS family **: Linux (Unix-like)**

Source model **: Open source**

Sr No	Advantages	Sr No	Disadvantages
1.	Its an open source	1.	Unavailability of hardware drivers
2.	No antivirus required	2.	Difficult to learn LINUX language
3.	Command prompt is efficient	3.	Insufficient software tools

4.	No reboot required	4.	Cannot run all the games
5.	Less space and multitasking	5.	Support issue

Difference of Window server OS & Linux Server OS

Win OS	Linux OS
Is a graphical user interface	Is a command line interface
OS developed & published by Microsoft	OS developed of the free open source foundation also helped Linus Torvalds in making of Linux
Released on Nov 20, 1985	Was initially released by Linus Torvalds on Sep 17, 1991
Not open source OS	Open source OS
Costly	Free of cost
Less secure	More Secure
Win is known slow & slow over time	Runs faster than win
Distributed under a PCS license (Proprietary commercial software)	Distributed under the GPL license (General public license)

AIM

TO ACQUAINT THE CLASS ABOUT INTRO TO SERVER OS AND VIRTUALIZATION

What is Server OS ?

A server-based operating system is an operating system designed specifically to run on servers, which are specialized computers designed to handle large amounts of data, requests and network traffic. These operating systems are optimized for reliability, performance, and security in server environments.

There are several types of Windows Server operating systems, each tailored to different use cases and business needs. Here are some of the main versions:

a) **Windows Server Essentials:-** Designed for small businesses with up to 25 users and 50 devices, Windows Server Essentials offers simplified management, built-in security features, and integration with cloud services like Microsoft 365.

b) **Windows Server Standard:-** This version is suitable for physical or minimally virtualized environments. It provides core features such as Active Directory, DNS, DHCP, file and print services, and more. It supports up to two virtual instances when all physical cores in the server are licensed.

c) **Windows Server Datacenter:-** Datacenter is designed for highly virtualized environments and offers unlimited virtualization rights. It provides all the features of Windows Server Standard, plus additional capabilities like Shielded Virtual Machines, Software-defined Networking (SDN), and Storage Spaces Direct.

d) **Windows Server IoT (Internet of Things):-** This edition is optimized for Internet of Things devices and scenarios, offering capabilities like enhanced security, device management, and support for both ARM and x64 architectures.

e) **Windows Server Nano:-** Nano Server is a lightweight, headless version of Windows Server designed for cloud-native applications and containerized workloads. It provides a minimal footprint, improved security, and faster deployment times.

f) **Windows Server Core:-** Similar to Nano Server, Server Core is a minimal installation option without a graphical user interface (GUI). It is optimized for running specific server roles, reducing resource consumption and attack surface.

g) **Windows Server for Azure:**- This version is specifically optimized for running Windows Server workloads in the Microsoft Azure cloud platform. It offers integration with Azure services, simplified management, and flexible pricing options.

Each version of Windows Server is designed to meet specific requirements, whether it's for small businesses, large enterprises, cloud environments, or specialized IoT deployments. Choosing the right edition depends on factors such as the size of the organization, the workload requirements, virtualization needs, and budget considerations.

What type of servers ?

Servers come in various types, each serving different purposes and catering to specific needs. Here are some common types of servers:

a) Web Server:- Web servers are designed to host websites and web applications. They respond to requests from web browsers and deliver web pages, files, and multimedia content to users over the internet.

b) File Server:- File servers store and manage files and folders accessible to users within a network. They facilitate file sharing, collaboration, and centralized data storage.

c) Database Server:- Database servers manage and store data in databases. They handle queries, transactions, and data retrieval operations, providing access to databases for applications and users.

d) Application Server:- Application servers provide a runtime environment for running and executing applications. They handle tasks such as transaction processing, business logic execution, and data processing for client-server applications.

e) Mail Server:- Mail servers manage email communication, including sending, receiving, and storing emails. They handle SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), and POP3 (Post Office Protocol) protocols for email delivery and retrieval.

f) DNS Server:- DNS (Domain Name System) servers translate domain names into IP addresses and vice versa, enabling users to access websites and services using human-readable domain names.

g) Proxy Server:- Proxy servers act as intermediaries between clients and other servers, forwarding requests and responses between them. They can be used for caching, filtering, and improving network performance and security.

h) FTP Server:- FTP (File Transfer Protocol) servers enable the transfer of files between computers over a network. They provide a secure and efficient way to upload, download, and manage files remotely.

i) Print Server:- Print servers manage and control printers on a network, allowing users to send print jobs from their computers to designated printers for output.

j) Virtual Server:- Virtual servers are software-based servers created by partitioning physical servers into multiple virtual instances. They enable efficient resource utilization, scalability, and flexibility in deploying and managing workloads.

These are just some of the common types of servers, and there are many other specialized server types catering to specific needs and use cases in various industries and environments.

Some characteristics of server-based operating systems include:-

a) **Stability and Reliability:-** Server operating systems are engineered to be stable and reliable, minimizing downtime and ensuring continuous operation of critical services.

b) **Networking Capabilities:-** They typically have robust networking capabilities to handle a large number of network connections and efficiently manage network traffic.

c) **Resource Management:-** Server operating systems are designed to efficiently manage system resources such as CPU, memory, and storage to ensure optimal performance for multiple concurrent tasks and services.

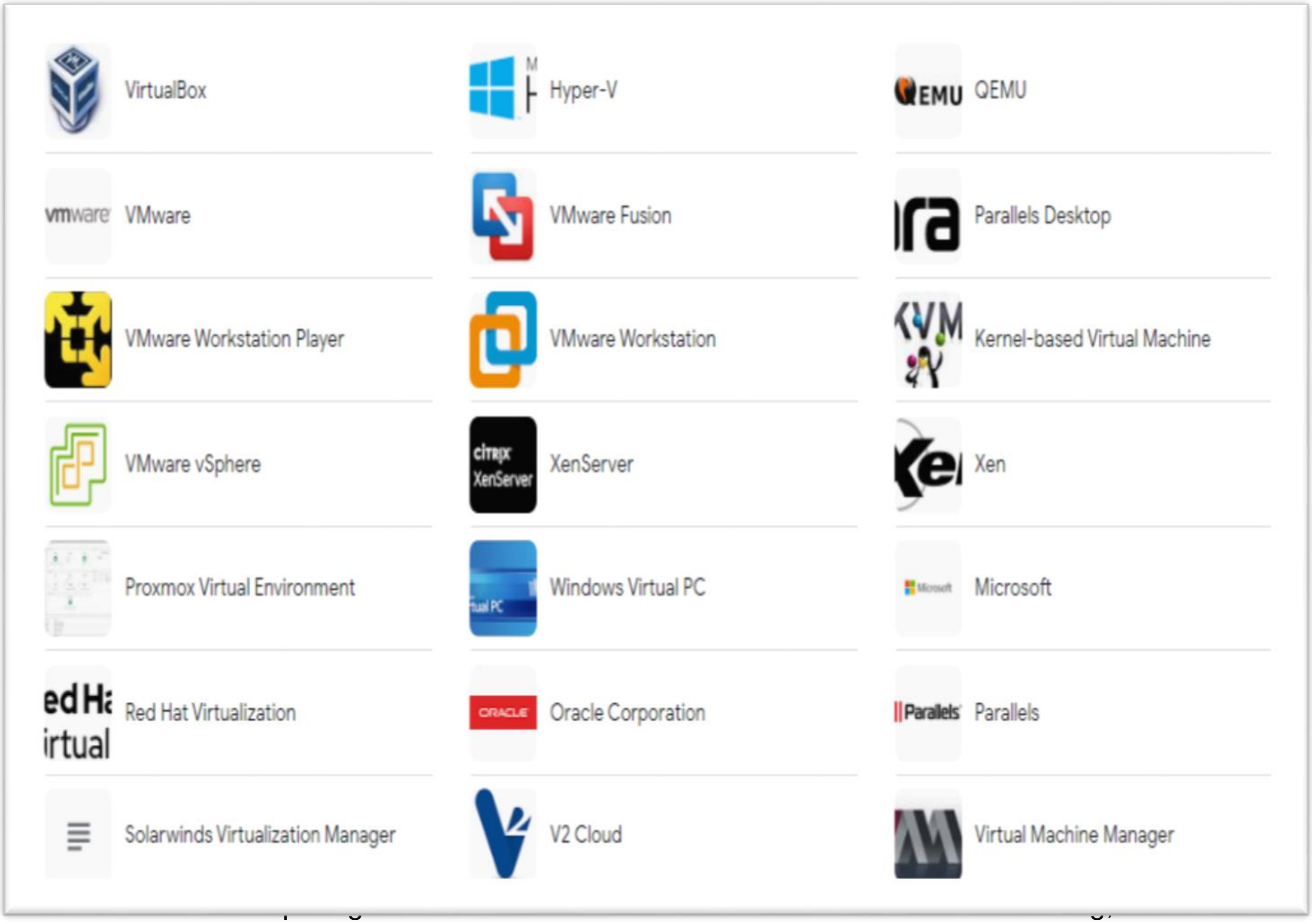
d) **Security Features:-** Security is a top priority for server operating systems, with features such as access controls, encryption, firewalls, and intrusion detection systems built-in or readily available.

e) **Remote Administration:-** They often include tools for remote administration and management, allowing system administrators to monitor, configure, and troubleshoot servers from a central location**.**

What is Virtualization?

Virtualization is technology that you can use to create virtual representations of servers, storage, networks, and other physical machines. Virtual software mimics the functions of physical hardware to run multiple virtual machines simultaneously on a single physical machine.

Virtualization applications:-



VirtualBox

VMware

VMware Workstation Player

VMware vSphere

Proxmox Virtual Environment

Red Hat Virtualization

Solarwinds Virtualization Manager

Hyper-V

VMware Fusion

VMware Workstation

XenServer

Windows Virtual PC

Oracle Corporation

V2 Cloud

QEMU

Parallels Desktop

Kernel-based Virtual Machine

Xen

Microsoft

Parallels

Virtual Machine Manager

operating system, a server, a storage device, or a network resource. This virtual version behaves like a physical entity but is actually simulated by software running on a physical computer or server. Virtualization allows multiple virtual instances of resources to run on a single physical machine, enabling better resource utilization, improved scalability, and easier management. Here's how it generally works:

1. HyperV Installation: Virtualization is typically facilitated by a software called a hyperV. This software is installed directly on the physical hardware of a computer or server. The hyperV acts as a layer between the physical hardware and the virtualized environments.

2. Creation of Virtual Machines (VMs): Once the hyperV is installed, you can create virtual machines. A virtual machine is essentially a software-based emulation of a physical computer that runs its own operating system and applications. Multiple VMs can run concurrently on a single physical server.

3. Resource Allocation: When setting up a virtual machine, you allocate resources from the physical hardware to the VM, such as CPU cores, RAM, disk space, and network bandwidth. The hyperV manages the allocation and ensures that each VM gets its fair share of resources.

4. Isolation: Each virtual machine is isolated from the others running on the same physical server. This isolation prevents one VM from affecting the others in case of software failures or security breaches.

5. Virtual Networking: Virtualization allows for the creation of virtual networks within the physical network infrastructure. This enables VMs to communicate with each other and with external networks as if they were physical machines.

6. Snapshotting and Cloning: Virtualization platforms often offer features like snapshotting and cloning. Snapshots capture the current state of a VM, allowing you to revert to that state later if needed. Cloning enables you to create identical copies of VMs, which is useful for deploying multiple instances of the same environment.

7. Live Migration: Some advanced virtualization platforms support live migration, which allows you to move a running VM from one physical server to another without interrupting its operation. This is useful for load balancing, hardware maintenance, and disaster recovery.

8. Management Tools: Virtualization environments typically come with management tools that allow administrators to monitor and manage the virtual infrastructure, including tasks such as provisioning new VMs, allocating resources, and monitoring performance.

Overall, virtualization provides flexibility, efficiency, and cost savings by allowing multiple virtual instances to run on a single physical server, thereby optimizing resource utilization and simplifying management.

Here are some advantages and disadvantages of virtualization:-

Advantages:-

1. Resource Utilization: Virtualization allows for better utilization of physical hardware resources by running multiple virtual machines (VMs) on a single physical server. This helps to maximize the efficiency of CPU, memory, storage, and networking resources.

2. Cost Savings: By consolidating multiple physical servers into fewer physical machines hosting multiple virtual servers, organizations can reduce hardware, power, cooling, and space costs. Additionally, virtualization often simplifies management and maintenance tasks, leading to lower operational expenses.

3. Scalability: Virtualization enables easy scalability by allowing administrators to quickly provision and deploy new virtual machines as needed. This flexibility helps organizations adapt to changing business demands without significant upfront investments in new hardware.

4. Improved Disaster Recovery: Virtualization facilitates faster and more reliable disaster recovery solutions by enabling features such as VM snapshots, replication, and live migration. In the event of hardware failure or other disasters, virtual machines can be easily migrated to alternate hardware with minimal downtime.

5. Isolation and Security: Virtualization provides strong isolation between virtual machines, preventing applications or processes running on one VM from affecting others. This isolation enhances security by limiting the impact of security breaches and malware infections.

6. Testing and Development: Virtualization simplifies testing and development processes by allowing developers to create and deploy isolated virtual environments quickly. This enables rapid prototyping, testing of software compatibility, and easier collaboration among development teams.

Disadvantages:-

1. Performance Overhead: Virtualization introduces a performance overhead because of the additional layer of abstraction between virtual machines and physical hardware. While this overhead is often minimal, it can become significant in high-performance computing or real-time applications.

2. Complexity: Managing a virtualized environment can be more complex than managing a traditional physical infrastructure. Administrators need to deal with tasks such as VM provisioning, resource allocation, performance monitoring, and troubleshooting across multiple virtualization platforms.

3. Single Point of Failure: While virtualization can improve resilience through features like live migration and high availability, it also introduces the risk of a single point of failure. If the hypervisor or underlying hardware fails, multiple virtual machines hosted on that system may be affected simultaneously.

4. Security Risks: While virtualization can enhance security through isolation, it also introduces new attack vectors. Vulnerabilities in the hypervisor or misconfigurations of virtual networks can potentially compromise the security of the entire virtualized environment.

5. Dependency on Hardware Compatibility: Virtualization relies on hardware compatibility with virtualization technologies such as Intel VT-x or AMD-V. Not all hardware supports these features, which may limit the choice of hardware or require additional investment in compatible hardware.

--------------------------------------- PRACTICAL/ INSTALLATION ---- --------------------------------------

Why Linux is better than windows

a) Reliability
b) Can revive older computers
c) Perfect for programmer
d) Costing

AIM

TO ACQUAINT THE CLASS ABOUT INTRO TO ANTIVIRUS, ANTI MALWARE SOFT & FIREWALL

Part – I **Virus & Malware**

Part – II **Anti-virus & anti-malware soft**

Part – III **Firewall**

Virus ?

A computer virus is a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files.

Malware ?

Malware (malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems

Types of Malware

a) Virus
b) Trojan Horse
c) Worms
d) Spyware
e) Adware
f) Ransomware
g) Spam
h) Bots

a) virus

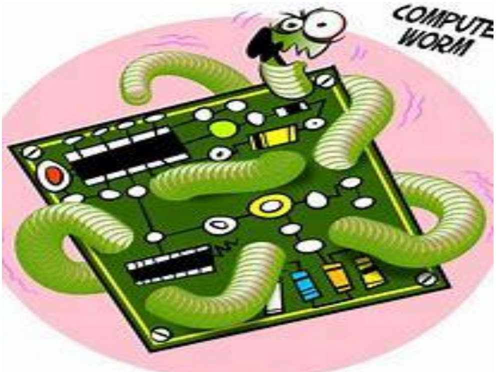
A computer virus (vital information resources under siege) is a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files.

b) **Trojan horse**

A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

c) **Worm**

The worm (write once, read many) virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm. Worms consume large volumes of memory, as well as bandwidth.



d) **Spyware**

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

e) **Adware**

Adware in cyber security refers to a type of malware that displays unwanted advertisements on your computer or device. Adware is commonly activated unknowingly when users are trying to install legitimate applications that adware is bundled with.

f) **Ransomware**

Ransomware is a type of cryptovirological malware that permanently blocks access to the victim's personal data unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Part II – Anti-virus & anti-malware soft

Anti-virus

Antivirus is a type of software program that helps in protecting the computer system from viruses. It detects the viruses in the computer system and destroys them. It protects the computer system from specific malware. It is used for protection from some traditional and simple threats that can harm the computer system. It is mostly used in personal computers for safety purposes.

Examples :- Avast, QuickHeal, AVG etc.…

Anti-malware

Antimalware is also a software program but it protects the computer systems from all kinds of malware i.e., viruses, trojans, worms, etc. It protects the computer system from all kinds of malware. It is used for protection from some new, sophisticated, and more dangerous threats that can harm the computer system. It is mostly used in organizational computers for safety purposes.

Example: MalwareBytes, Avira, Bitdefender etc…

Difference :-

Parameters	ANTIVIRUS	ANTIMALWARE
Definition	It is a software program that protects the computer system from viruses.	It is a software program that protects the computer systems from all malware i.e. viruses, trojans, worms, etc.
Protects	It protects from traditional viruses.	It protects from all malware including newer and sophisticated ones.
Rule update	It does not update its rules frequently.	It updates its rules frequently so that malware detection is easy.
Danger	It protects from predictable danger.	It protects from unpredictable danger.

Used in	It is mostly used in personal computers.	It is mostly used in organizational computers.
Cost	It is comparatively less costly.	It is more costly.
Detect	It detects and destroys viruses which is a type of malware.	It detects and destroys all malware including viruses too.
Features	• Real time scanning • Remove threats	• Sandboxing • Traffic filtering • Proactive Security
Techniques	Techniques Used by Antivirus software- • Scanning • Integrity checking • Interception • Heuristic detection.	Used by Anti-malware software- • Sandboxing • Signature-based detection • Behavior-based detection
System compatibility	It is more used as it has system compatibility.	It is less used due to its high rate and system compatibility.
Protect	It protects against common types of viruses.	It can scan and detect new iterations of infections.
Reliable	It is not reliable with the overall cyber protection of the computer system.	It is reliable with the overall cyber protection of the computer system.

Part III - Firewall

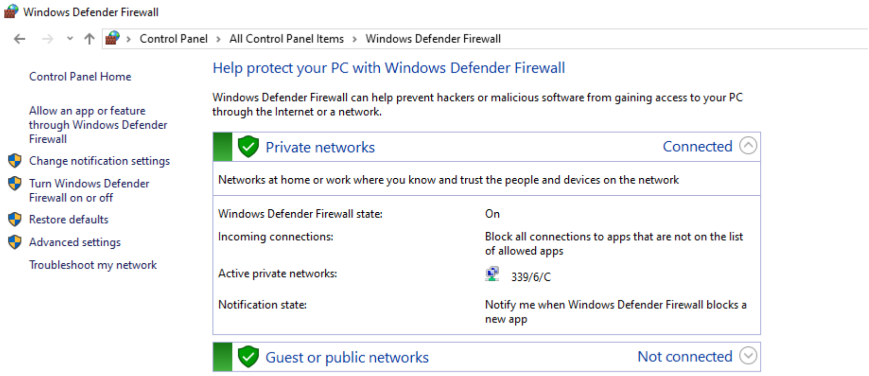
Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Types of firewall

1. Software firewall
2. Hardware firewall

Software firewall - A software firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Typically it works as an application layer firewall.



Windows Defender Firewall

Control Panel > All Control Panel Items > Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

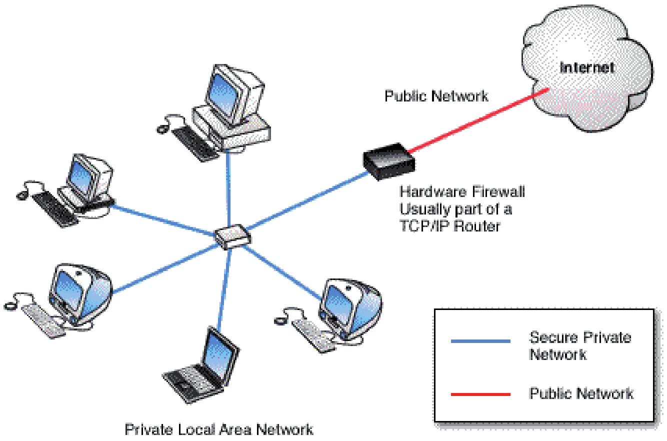
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	339/6/C
Notification state:	Notify me when Windows Defender Firewall blocks a new app

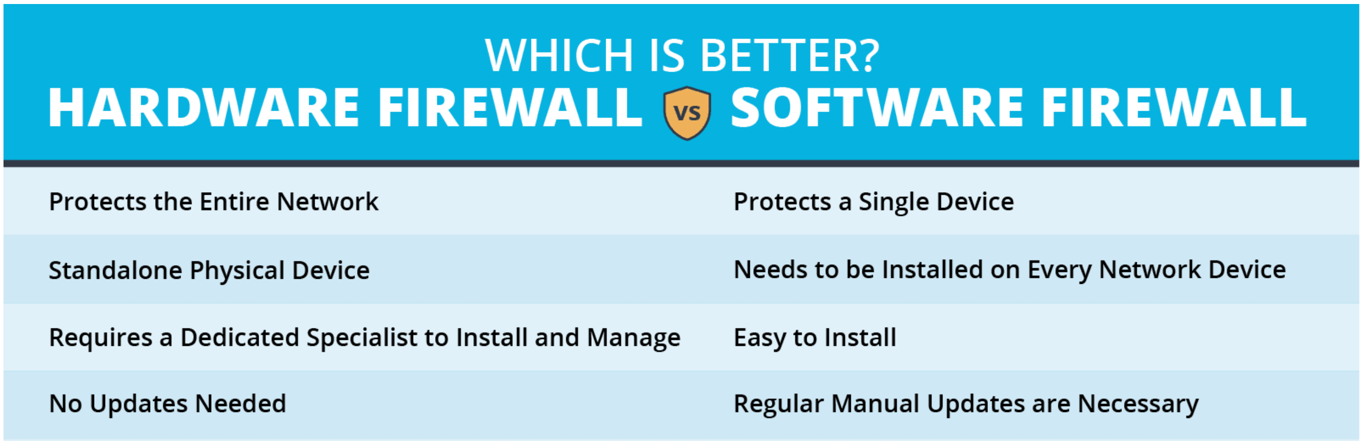
Guest or public networks — Not connected

Hardware firewall - A hardware firewall is a physical device much like a server that filters the traffic going to a computer. While a user would normally plug a network cable directly into a computer or server, with a h ardware firewall, the cable is plugged into the firewall first.


Internet
Public Network
Hardware Firewall Usually part of a TCP/IP Router
Secure Private Network
Public Network
Private Local Area Network

Difference

Hardware firewall	



WHICH IS BETTER?

HARDWARE FIREWALL	SOFTWARE FIREWALL
Protects the Entire Network	Protects a Single Device
Standalone Physical Device	Needs to be Installed on Every Network Device
Requires a Dedicated Specialist to Install and Manage	Easy to Install
No Updates Needed	Regular Manual Updates are Necessary