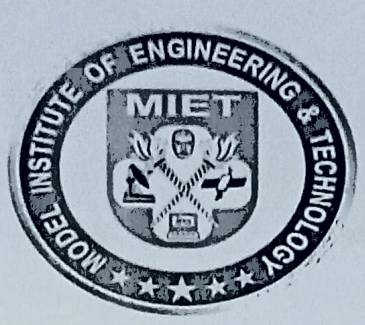


MIET

FUTURE BEGINS HERE....

NAME :	SURAJ PANDIT
BRANCH:	CSE
ROLL NO.:	2021A1R164
COURSE NAME :	Operating Systems
COURSE CODE :	COM-302
SUBMITTED TO :	Miss Pragti Jaiwal
ASSIGNMENT :	01

Name : Suraj Pandit
Roll No : 2021AIR164
Course Name : Operating System

INDEX

Assignment -1

Roll No: 2021AIR164

Ques1(a) Elaborate the concept of Multiprocess Architecture in Google Chrome Web browser.

Ans Multiprocessing refers to the use of two or more central processing units, within a single computer system. The term also refers to the ability of a system to support more than one processor or the ability to allocate tasks between them. Google chrome puts web apps and plug-ins in separate processes from the browser itself. This means that a rendering engine crash in one webapp won't affect the web apps in parallel to increase their responsiveness, and it means the browser itself won't lock up if a particular web app or plug-ins stops responding.

Google chrome creates three different types of processes: browser, renderers and plug-ins.

Browser :- There's only one browser process, which manages the tabs, windows and "chrome" of the browser. This process also handles all the interactions with the disk, network, user input and display, but it makes no attempt to parse or render any content from the web.

Renderers : The browser process creates many renderer processes, each responsible for rendering web pages. The renderer processes contain all the complex logic for handling HTML, Javascript, CSS, images and so on. All interactions with web apps, including user input and events and screen painting, must go through the browser process. This lets the web process monitor the

renderers for suspicious activity, killing them if it suspects an exploit has occurred.

Plug-ins :- The browser process also creates one process for each type of plug-in that is in use, such as Flash, Quicktime or Adobe Reader. These processes just contain the plug-ins themselves along with some glue code to let them interact with the browser and renderers.

Once google chrome has created its browser process, it will generally create on renderer process for each instance of a web site you visit. This approach aims to keep pages from different web sites isolated from each other.

You can think of this using a different process for each tab in the browser but allowing two tabs to share a process if they are related to each other and are showing the same site. For example, if one tab opens another tab using Javascript, or if you open a link to the same site in a new tab, the tabs will share a renderer process. Conversely, if you type the URL of a different site into the location bar of a tab, we will swap in a new renderer process for the tab.

For each type of plug-in, Google Chrome will create a plug-in process when you first visit a page that uses it. A short time after you close all pages using a particular plug-in, we will destroy its process.

R.No :- 2021A1R164

b) Keeping the mind the various definitions of operating system, consider whether the operating system should include applications such as web browsers, and mail programs. Argue that ~~the~~ it should and that it should not, and support your answer.

Ans Operating system should include applications such as web browsers and mail programs.

It is generally accepted today that almost all users will want web access and email capability, to this end, it is of greater convenience to the user if a web browser and email client are packaged with the OS. Furthermore, coupling a web browser (or other applications) with the OS can provide certain performance advantages. For eg:- because I.E is coupled with Windows, it is cached while windows boots up - this makes faster program loading, this is opposed to Mozilla which is not (by default) cached by linux, and so loads slowly every time it is invoked.

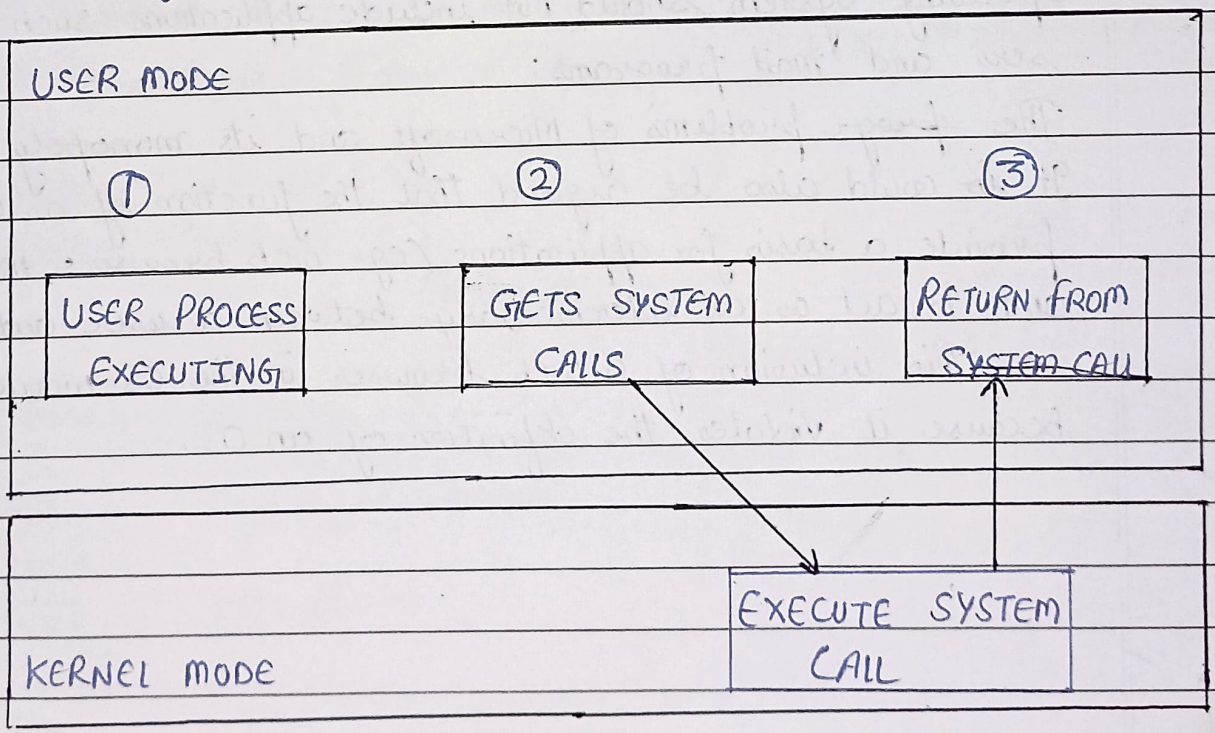
Operating System should not include applications such as web browsers and mail programs:

The ~~progr~~ problems of Microsoft and its monopoly are evident. It ~~is~~ could also be argued that the function of an OS is to provide a basis for applications (eg. web browsers, mail programs) and to act as an intermediary between a user and the hardware. This inclusion of a web browser in the OS would be wrong because it violates the definition of an OS.

Que 2: Operating system gurantees that there will be a system call or interrupt, so that it will regain control. Justify your answer with diagrammatic representation.

Ans A system call is a mechanism that provides an interface between a process and the operating system. It is a programmatic method in which a computer program requests a service from the kernel of the OS. For eg:, if we need to write a program code to read data from one file, copy that data into another file. The first information that the program required is the name of two files, the input and the output files. In an interactive system, this types of program execution requires some system call by OS.

→ First call is to write a prompting message on the screen.
→ Second, to read from the keyboard, the characters which define the two files.



Step 1: To processes executed in the user mode till the time a system call interrupts it.

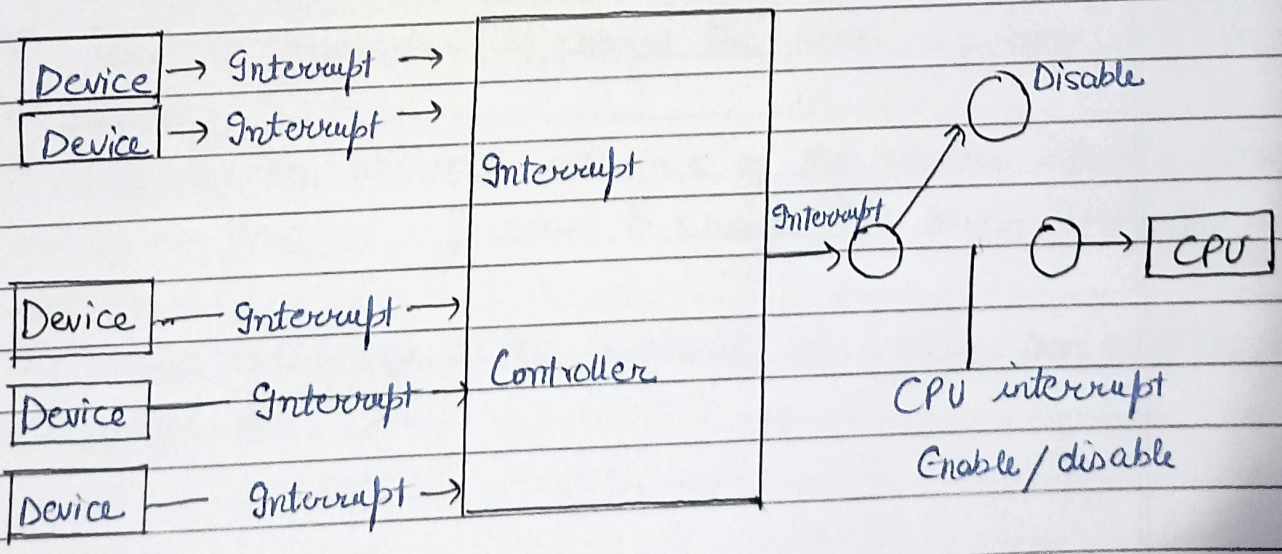
Step 2: After that, the system call is executed in the kernel mode on a priority basis.

Step 3: Once system call execution is over, control returns to the user mode.

Step 4: The execution of user processes resumed in kernel mode.

Interrupt: An interrup is a signal emitted by a device attached to a computer ~~es~~ or from a program within the computer. It requires the operating system (OS) to stop and figure out what to do next. An interrupt com stops or terminates a service or a current process.

When the interrupts occur, the CPU completes the execution of ongoi-ng instruction and handles the ISR. But ~~one~~ once the interrupts is resolved, the CPU continues to execute from where an execution was stopped prior to the interrupt.



The following steps are involved while the interrupts:-

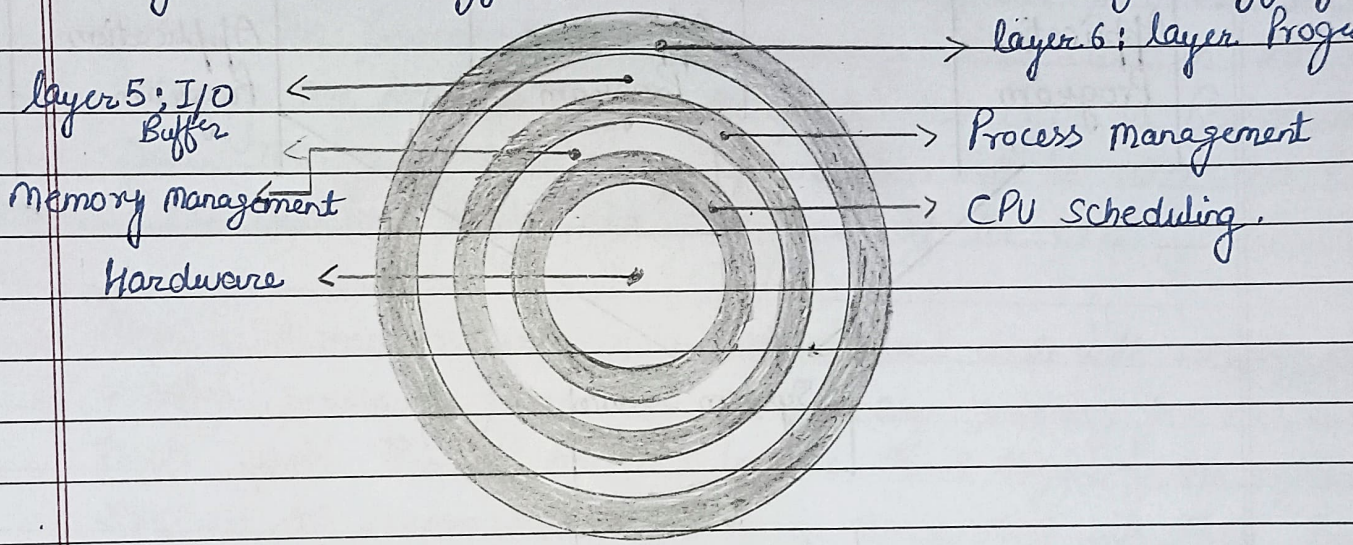
1. The first step involved in handling the interrupt is to check the priority of the interrupt.
2. If the priority is low compared to the current process under execution, then interrupt is ~~solved~~ saved in the memory.
3. If the priority is high compared to the current process under execution, CPU saves the context of the current process.
4. CPU loads the new process which invoked the interrupt and executes that.
5. On completion of the requested service, CPU loads the process which was under execution prior to the interrupt and resume

es)

R.No : 2021A1R164

Q3 Explain the layered structure of an operating system and discuss the functionality of each layer in detail.

Ans The layered structure approach breaks up the operating system into different layers and retains much more control on the system. The bottom layer (layer 0) is the hardware, and the topmost layer (layer N) is the user interface. These layers are so designed that each layer uses the functions of the lower-level layers only. It simplifies the debugging process as if lower-level layers are debugged, and an error occurs during debugging.



- This allows implementers to change the inner workings and increases modularity.
- As long as the external interface of the routines doesn't change, developers have more freedom to change the inner workings of the routines.
- The main advantage is the simplicity of construction and ~~working~~ debugging. The

R.No : 20210IR164

1. Hardware : This layer interacts with the system hardware and coordinates with all the peripheral devices used, such as printer, mouse, keyboard, scanner etc. These types of hardware devices are managed in the hardware layer. It is attached directly to the core of the system.

2. CPU scheduling : This layer deals with scheduling the processes for the CPU. Many scheduling queues are used to handle processes. When the processes enter the system, they are put into the job queue. The processes that are ready to execute in the main memory are kept in the ready queue. This layer is Responsible for managing how many processes will be allocated to the CPU and how many will stay out of the CPU.

3. Memory Management : Memory management deals with memory and moving processes from disk to primary memory for execution and back again. This is handled by the third layer of the operating system. All memory management is associated with this layer. There are various types of memories in the computer like RAM, Ro

4. Process Management : This layer is responsible for managing the processes, i.e assigning the processor to a process and deciding how many processes will stay in the waiting schedule. The priority of the processes is also managed in this layer. The different algorithms used for process scheduling are FCFS (first come first served), SJF (shortest job first), priority scheduling round-robin scheduling etc.

5. I/O Buffer : I/O devices are very important in computer systems. They provide ex users with the means of interacting with system. This layer handles the buffers for the I/O devices and make sure that they work correctly. Suppose you are typing from the keyboard, there is a keyboard buffer attached with the keyboard, which stores data for a temporary time. Similarly all I/O devices have some buffer attached to them. The computer uses buffers to maintain the good timing speed of the processor and I/O devices.

6. User programs : This is the highest layer in the layered operating System. This layer deals with the many user programs and applications that run in an operating system, such as word processors, games, browsers, etc.

CLASSMATE
Date :
Page : 1

Roll No : 2021AIR164

Q4 What is the reason for using Virtual machines instead of original hardware? What are the different types of virtualization available?

Ans. A Virtual machine (VM) is a computer resource that uses software instead of a physical computer to run programs and deploy apps. Each virtual machine runs its own operating system and functions separately from the other VMs, even they are all running on the same host.

Main reasons for using Virtual machines instead of original hardware

- Operational Flexibility : The big draw of virtualization is to operate multiple displays and even systems - linux and Windows, for example from the same console. This allows users to toggle among applications regardless of their OS. VM's simulate the experience of using multiple computers at the same time, for complex servers with multisystem needs.

- Reducing Overhead : Overhead costs don't just happen when you purchase new hardware - they continue throughout the life of your workstation. The continuous expenses of hardware maintainence, power and licensing can take a toll on your business. But resource consumption with multiple hardware-based systems. Virtualization ensures there is no less to constantly maintain and replace hardware.

- Centralized management of diverse operating units allows you to increase efficiency and ultimately, to increase your output. VM's are useful because they offer an opportunity to consolidate.

your IT management into one console. This can be much more efficient than managing multiple physical device

- VMware enables you to add and remove apps with no physical overhead, an expanding virtual infrastructure doesn't require complex budgets for hardware resources or added floorspace.

- Disaster Recovery : VMware can be a highly effective solution for disaster recovery. Because virtual machines make regular copies of their operations history - copies that you can retrace and revisit as necessary - there is little risk for data loss in case of an unexpected hardware failure.

Types of Virtualization :

- Hardware Virtualization : When virtualizing hardware, virtual versions of computers and operating systems (VMs) are created and consolidated into a single, primary, physical server. Hardware virtualization, which is also known as server virtualization, allows hardware resources to be utilized more efficiently and for one machine to simultaneously run different operating systems.

- Software Virtualization : Software virtualization creates a computer system complete with hardware that allows one or more guest operating systems to run on a physical host machine. Applic-ations can be virtualized and delivered from a server to an end user's device, such as a laptop or smartphone. This allows employees to access centrally hosted applications when working remotely.

R.No : 202A1R164

- Storage Virtualization : Storage can be virtualized by consolidating multiple physical storage devices to appear as a single storage devices. Benefits include increased performance and speed, load balancing and reduced costs. Storage virtualization also helps with disaster recovery planning, as virtual storage data can be duplicated and quickly transferred to another location, reducing downtime.

- Network Virtualization : Multiple sub-networks can be created on the same physical network by combining equipment into a single, software-based virtual network resource. Network virtualization also divides available bandwidth into multiple, independent channels, each of which can be assigned to servers and devices in real time. Advantages include increased reliability, network, sp security and better monitoring of data usage.

- Desktop Virtualization : This common type of virtualization separa the desktop environment from the physical devices and stores a desktop on a remote server, allowing users to access the desktops from anywhere on any device.