OS Solved Model Paper

Q-Virus?

Ans- A computer virus is a kind of malicious computer program, which when executed, replicates itself and inserts its own code. When the replication is done, this code infects the other files and program present on your system.

These computer viruses are present in various types and each of them can infect a device in a different manner.

In this article, we shall discuss in detail what is a computer virus and what are its different types. Also, we will read on to know what is an Anti-virus and how it can nullify a virus in our computer devices, along with some sample questions from the competitive exam point of view.

Apart from being aware of what a computer virus is, this topic is even important for candidates preparing for Government exams. Major competitive exams in the country comprise Computer Knowledge as an integral part of the syllabus and questions based on virus and anti-virus can also be expected in these exams.

Thus, to excel in the upcoming Govt exams, aspirants must go through this article in detail and carefully study the different types of viruses.

What is a Computer Virus?

A computer virus is a program which can harm our device and files and infect them for no further use. When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding. This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.

Types of Computer Virus

- **Boot Sector Virus –** It is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks. The Boot sector comprises all the files which are required to start the Operating system of the computer. The virus either overwrites the existing program or copies itself to another part of the disk.
- **Direct Action Virus –** When a virus attaches itself directly to a .exe or .com file and enters the device while its execution is called a Direct Action Virus. If it gets installed in the memory, it keeps itself hidden. It is also known as Non-Resident Virus.
- **Resident Virus –** A virus which saves itself in the memory of the computer and then infects other files and programs when its originating program is no longer working. This virus can easily infect other files because it is hidden in the memory and is hard to be removed from the system.
- **Multipartite Virus –** A virus which can attack both, the boot sector and the executable files of an already infected computer is called a multipartite virus. If a multipartite virus attacks your system, you are at risk of cyber threat.

- **Overwrite Virus –** One of the most harmful viruses, the overwrite virus can completely remove the existing program and replace it with the malicious code by overwriting it. Gradually it can completely replace the host's programming code with the harmful code.
- **Polymorphic Virus –** Spread through spam and infected websites, the polymorphic virus are file infectors which are complex and are tough to detect. They create a modified or morphed version of the existing program and infect the system and retain the original code.
- **File Infector Virus –** As the name suggests, it first infects a single file and then later spreads itself to other executable files and programs. The main source of this virus are games and word processors.
- **Spacefiller Virus –** It is a rare type of virus which fills in the empty spaces of a file with viruses. It is known as cavity virus. It will neither affect the size of the file nor can be detected easily.
- **Macro Virus –** A virus written in the same macro language as used in the software program and infects the computer if a word processor file is opened. Mainly the source of such viruses is via emails.

Q-What is logic Bomb?

Ans-

A logic bomb is a type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system with the goal of causing harm to a network when certain conditions are met. It is triggered at a specific event and used to devastate a system by clearing hard drives, deleting files, or corrupting data. An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system.

In order to maximize damage before being noticed, logic bombs are mainly used with trojan horses, worms, and viruses. The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system. The devastation caused by a logic bomb can be a huge level.

Is a logic bomb malware?

Logic bombs are a small piece of code that is contained by other programs. They are not technically malware; however, they might be malicious. There are various kinds of malware; common types include worms and viruses that can have a logic bomb in terms of their attack policy.

To perform various unauthorize activities, logic bombs can be programmed by someone; some malicious activities are as follows:

- Consume system resources
- Delete data
- Restrict or prevent user access
- Create backdoors for hackers
- Corrupting data
- Steal data

Q- Program Threat?

Ans-

A **program threat** is a program written to **hijack** the security or **change the behaviour** of the process.
Types of program threats are as follows:

- **Virus**

A virus is a **self-replicating** and **malicious thread** that attaches itself to the system file and then rapidly replicates itself changing the essential files leading to a **system breakdown.**

Various types of computer viruses are as follows:

- **file/parasitic:** It attaches itself to a file.
- **Macro:** It affects the MS Office files and is written in a high-level language.
- **Source code:** It modifies the source code.
- **Multipartite:** It infects multiple parts of the system.
- **boot/memory:** It infects the boot sector,
- **Polymorphic:** It makes changes in copies every time.
- **Encrypted:** It is an encrypted virus and decrypts the code.
- **Tunnelling:** It installs itself in interrupt service routines and device drivers.
- **Stealth:** It modifies parts of the system so that they cannot be detected.

Q-Level of Security Management

Ans-

The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy. The information and procedures developed as part of security management processes will be used for data classification, risk management, and threat detection and response.

These procedures enable an organization to effectively identify potential threats to the organization's assets, classify and categorize assets based on their importance to the organization, and to rate vulnerabilities based on their probability of exploitation and the potential impact to the organization.

Types of Security Management

Security management can come in various different forms. Three common types of security management strategies include information, network, and cyber security management.

#1. Information Security Management

Information security management includes implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/IEC 27000 family of standards. Information security management programs should ensure the confidentiality, integrity, and availability of data.

Many organizations have internal policies for managing access to data, but some industries have external standards and regulations as well. For example, healthcare organizations are governed by the Health Insurance Portability and Accessibility Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) protects payment card information.

#2. Network Security Management

Network security management is a vital component of a network management strategy. The network is the vector by which most cyberattacks reach an organization's systems and its first line of defense against cyber threats. Network security management includes deploying network monitoring and defense solutions, implementing network segmentation, and controlling access to the network and the devices connected to it.

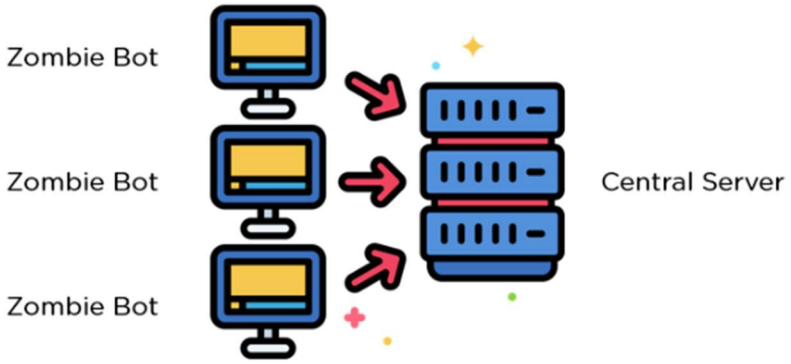
#3. Cybersecurity Management

Cybersecurity management refers to a more general approach to protecting an organization and its IT assets against cyber threats. This form of security management includes protecting all aspects of an organization's IT infrastructure, including the network, cloud infrastructure, mobile devices, Internet of Things (IoT) devices, and applications and APIs.

Q- DDOS , Working of DDOS , Prevntion of DDOS

Ans-

What Is a DDoS Attack?



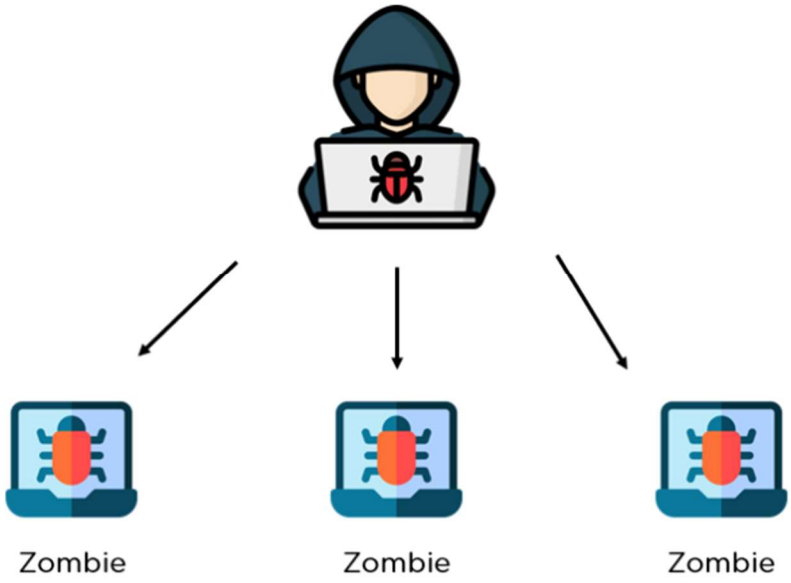
To understand how a DDoS attack works, you must know what a denial of service attack or a DOS attack is.

In a DOS attack, the hacker seeks to make the resources of a particular server, database, or router inaccessible to its users. This can be done by clogging the available bandwidth of the target, be it via continuous web requests or indefinite ping commands. Analogous to how blocking a shop's door prevent potential clients from entering it, DOS attacks were complete distress in the early days of network security.

How Does a DDoS Attack Work?

A DDoS attack is a two-phase process.

Phase 1: The hacker creates a botnet of devices. Simply put, a vast network of computers is hacked via malware, ransomware, or simple social engineering. These devices are a part of a botnet network, which can be triggered anytime to start bombarding a system or a server on the instruction of the hacker that created the botnet. The devices in this network are called bots or zombies.



Prevention of DDoS Attacks

- Load Balancers & Firewalls: Load balancers re-route the traffic from one server to another in a DDoS attack. This reduces the single point of failure and adds resiliency to the server data. Firewalls block unwanted traffic into a system and manage the number of requests made at a definite rate. It checks for multiple attacks from a single IP and occasional slowdowns to detect a DDoS attack in action.

- Detection & Mitigation: Having a response plan for DDoS attacks is highly crucial. The sooner such a breach is noted, the easier it is to clear the clogging. One can also employ DDoS prevention tools like Imperva to lessen their load under high-pressure situations.

- Switch to Cloud Service: With many organizations already aboard, cloud computing giants like Amazon web services (AWS) and Microsoft Azure have advanced DDoS protection tools in place. Furthermore, this eliminates the need for having a response plan to combat an attack since the engineers at the respective cloud providers will bear the brunt of the breach.

Q-Difference between Security and Protection

Ans-

There are various head-to-head comparisons between the security and protection in the operating system. Some comparisons of security and protection are as follows:

Features	Security	Protection
Definition	It is a technique used in operating systems to address threats from outside the system to maintain its proper functioning.	It is a technique used in operating systems to control hazards and maintain the system's proper functioning.
Focus	It mainly focuses on external threats to the system.	It mainly focuses on the internal threats of the system.
Policy	It specifies whether or not a specific user is allowed to access the system.	It outlines which users are permitted to access a certain resource.
Functionality	It offers a technique for protecting system and user resources from unauthorized access.	It offers a technique for controlling access to processes, programs, and user resources.
Mechanism	Security techniques include adding, deleting users, determining whether or not a certain user is authorized, employing anti-malware software, etc.	It includes techniques like modifying a resource's protection information and determining whether a user may access it.
Queries	It is a wide phrase that handles more complicated queries.	It comes with security and covers less complex queries.

Q- Topologies all everything about it

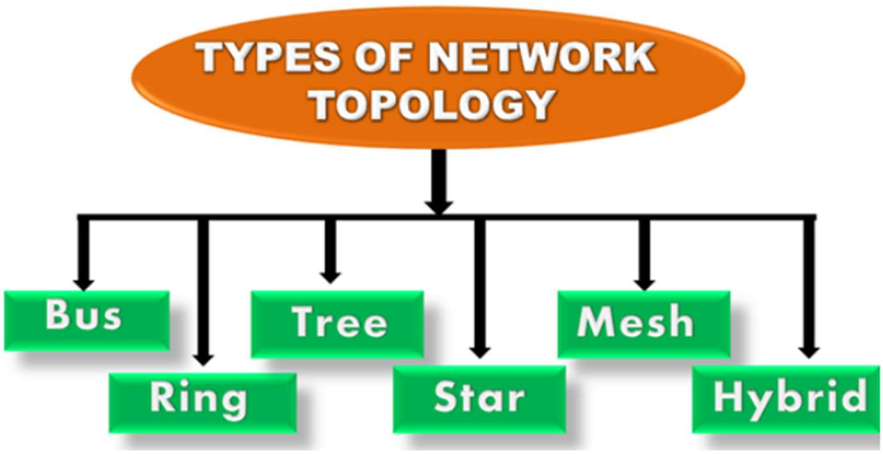
Ans-

What is Topology?

← Prev Next →

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Physical topology is the geometric representation of all the nodes in a network.



Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

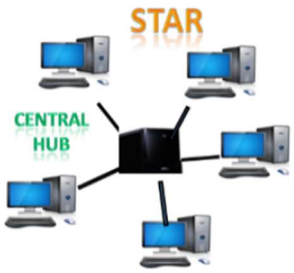
Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:
  Number of cables = (n*(n-1))/2;

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

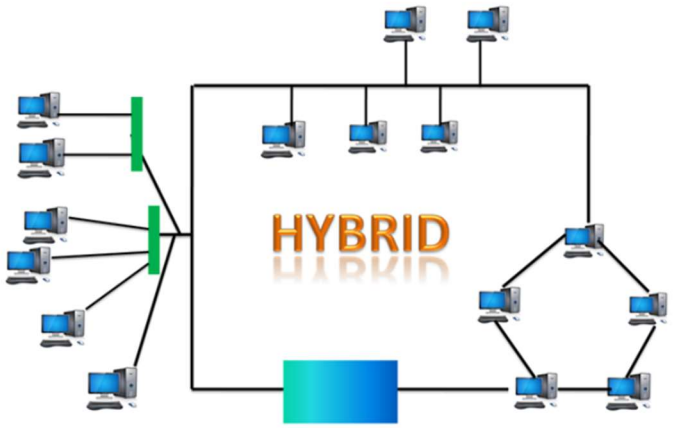
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Q-Session Hijacking

Ans-

What is Session Hijacking?

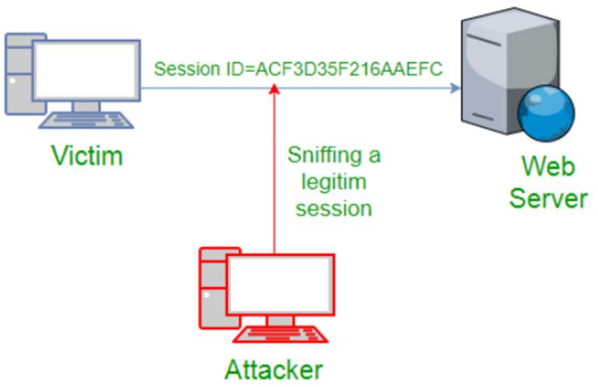
TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

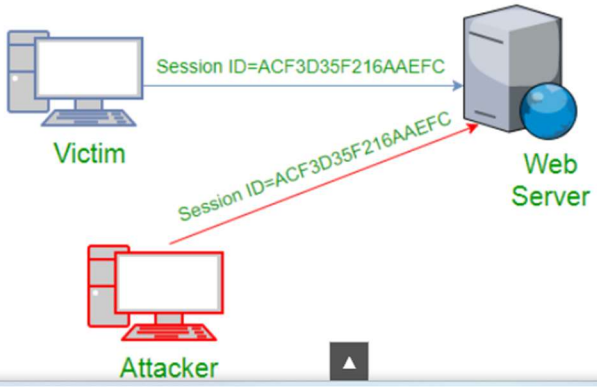
Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking :

There are many ways to do Session Hijacking. Some of them are given below –

- **Using Packet Sniffers**





- **IP Spoofing**
  Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.
- **Blind Attack**
  If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Q-client service architect

Ans-

What is Client-Server Architecture?

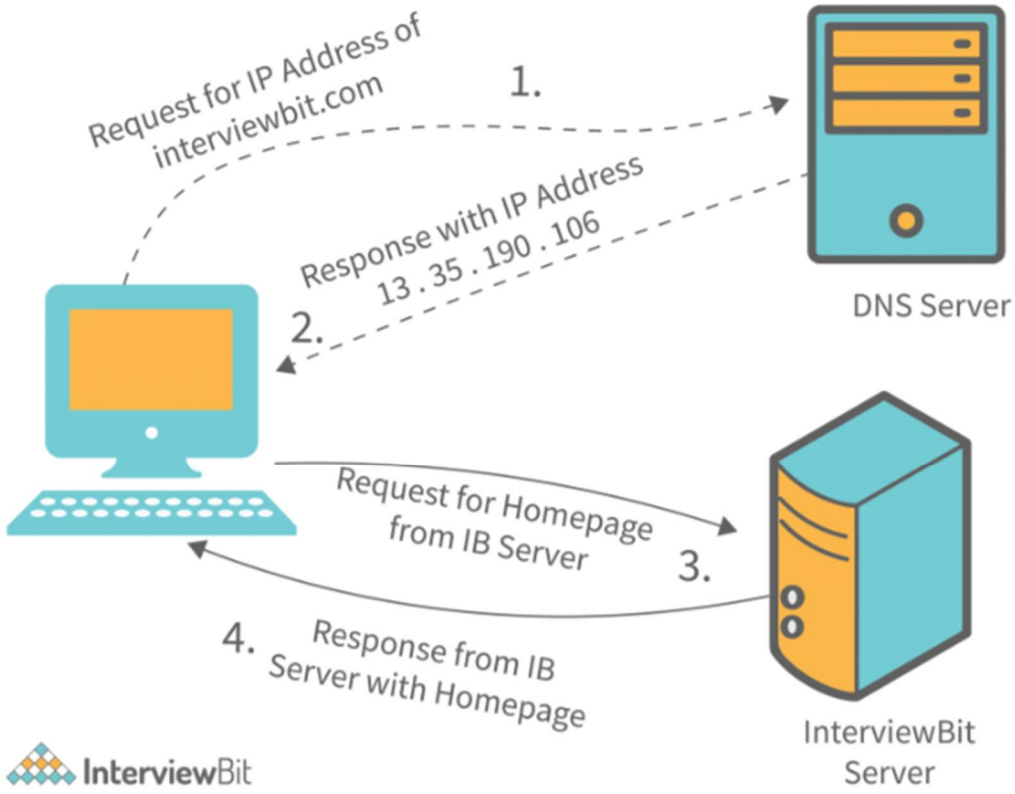
The client-server architecture or model is an application network separating tasks between clients and servers that are either within the same system or need to communicate over a network. In order to access the service provided by the server, the server-client sends the request to another program, which runs a few programs that distribute work among the clients & share resources with them.

A client-server relationship corresponds to the request-response pattern and should adhere to a standard communications protocol that defines the language and rules used for the communications. The client-server communication adheres to the TCP protocol suite.

Client/server messages are exchanged via the TCP protocol until the connection is complete. TCP protocol determines how data should be distributed in packets that networks will deliver, transfers packets to and receives packets from networks, and manages flow control or retransmission of garbled and dropped packets.

How Does Client-Server Architecture Work?

We already have studied what is the client and what is the server. Now let's understand the working of this architecture.



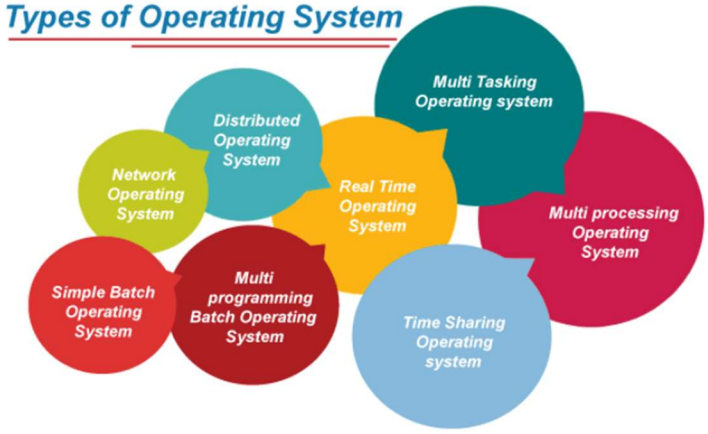
Q-Types of OS

Ans-

Types of Operating Systems

← Prev Next →

An operating system is a well-organized collection of programs that manages the computer hardware. It is a type of system software that is responsible for the smooth functioning of the computer system.



Batch Operating System

In the 1970s, Batch processing was very popular. In this technique, similar types of jobs were batched together and executed in time. People were used to having a single computer which was called a mainframe.

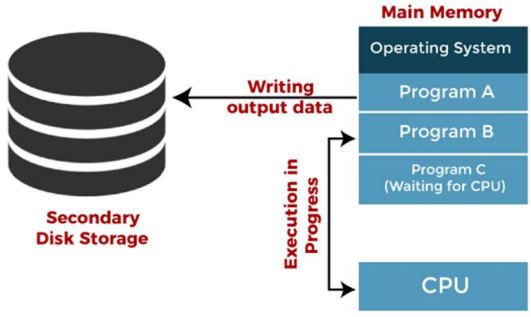
In Batch operating system, access is given to more than one person; they submit their respective jobs to the system for the execution.

The system put all of the jobs in a queue on the basis of first come first serve and then executes the jobs one by one. The users collect their respective output when all the jobs get executed.

Multiprogramming Operating System

Multiprogramming is an extension to batch processing where the CPU is always kept busy. Each process needs two types of system time: CPU time and IO time.

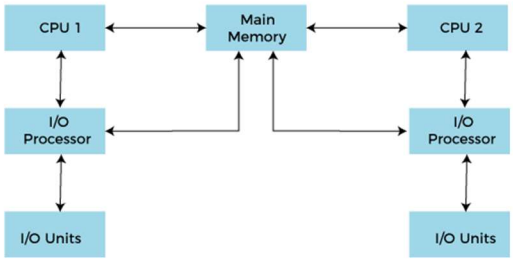
In a multiprogramming environment, when a process does its I/O, The CPU can start the execution of other processes. Therefore, multiprogramming improves the efficiency of the system.



Jobs in multiprogramming system

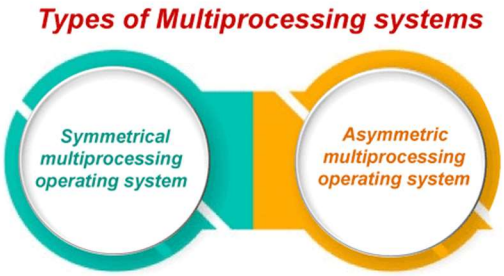
Multiprocessing Operating System

In Multiprocessing, Parallel computing is achieved. There are more than one processors present in the system which can execute more than one process at the same time. This will increase the throughput of the system.

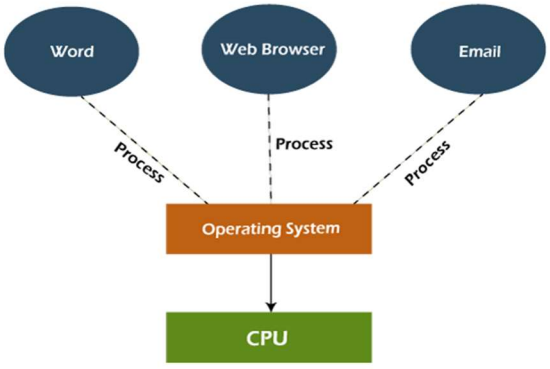


Working of Multiprocessor System

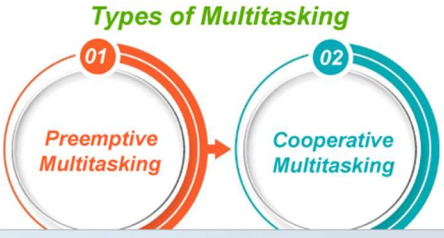
In Multiprocessing, Parallel computing is achieved. More than one processor present in the system can execute more than one process simultaneously, which will increase the throughput of the system.



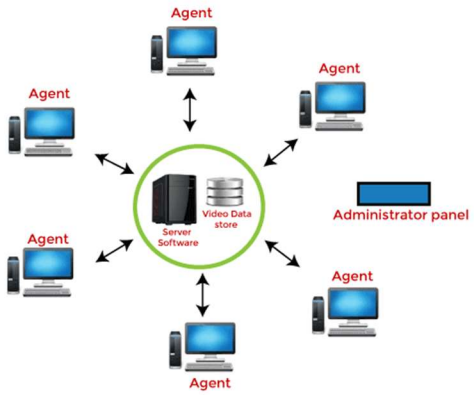
Multitasking Operating System



The multitasking operating system is a logical extension of a multiprogramming system that enables **multiple** programs simultaneously. It allows a user to perform more than one computer task at the same time.

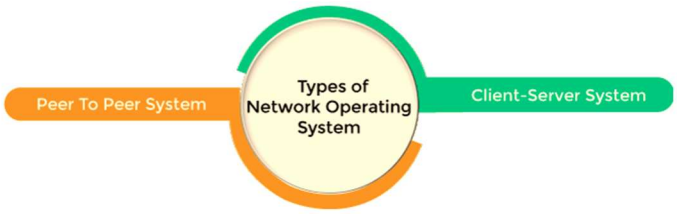


Network Operating System



Network Operating Systems

An Operating system, which includes software and associated protocols to communicate with other computers via a network conveniently and cost-effectively, is called Network Operating System.



Advantages of Network Operating System

- In this type of operating system, network traffic reduces due to the division between clients and the server.
- This type of system is less expensive to set up and maintain.

Disadvantages of Network Operating System

- In this type of operating system, the failure of any node in a system affects the whole system.
- Security and performance are important issues. So trained network administrators are required for network administration.

Q-PCB , States of Process , Shortest Job First(Numerical)

Ans-

Process Control Block is a data structure that contains information of the process related to it. The process control block is also known as a task control block, entry of the process table, etc.

It is very important for process management as the data structuring for processes is done in terms of the PCB. It also defines the current state of the operating system.

Structure of the Process Control Block

The process control stores many data items that are needed for efficient process management. Some of these data items are explained with the help of the given diagram −

Process Control Block (PCB)

Process State

This specifies the process state i.e. new, ready, running, waiting or terminated.

Process Number

This shows the number of the particular process.

Program Counter

This contains the address of the next instruction that needs to be executed in the process.

Registers

This specifies the registers that are used by the process. They may include accumulators, index registers, stack pointers, general purpose registers etc.

List of Open Files

These are the different files that are associated with the process

CPU Scheduling Information

The process priority, pointers to scheduling queues etc. is the CPU scheduling information that is contained in the PCB. This may also include any other scheduling parameters.

Shortest job first Numerical

The shortest job first (SJF) or shortest job next, is a scheduling policy that selects the waiting process with the smallest execution time to execute next. SJN, also known as Shortest Job Next (SJN), can be preemptive or non-preemptive.

Characteristics of SJF Scheduling:

- Shortest Job first has the advantage of having a minimum average waiting time among all scheduling algorithms.
- It is a Greedy Algorithm.
- It may cause starvation if shorter processes keep coming. This problem can be solved using the concept of ageing.
- It is practically infeasible as Operating System may not know burst times and therefore may not sort them. While it is not possible to predict execution time, several methods can be used to estimate the execution time for a job, such as a weighted average of previous execution times.
- SJF can be used in specialized environments where accurate estimates of running time are available.

Algorithm:

- Sort all the processes according to the arrival time.
- Then select that process that has minimum arrival time and minimum Burst time.
- After completion of the process make a pool of processes that arrives afterward till the completion of the previous process and select that process among the pool which is having minimum Burst time.

Q- Context switching

Ans-

What is the context switching in the operating system?

← Prev Next →

The Context switching is a technique or method used by the operating system to switch a process from one state to another to execute its function using CPUs in the system. When switching perform in the system, it stores the old running process's status in the form of registers and assigns the CPU to a new process to execute its tasks. While a new process is running in the system, the previous process must wait in a ready queue. The execution of the old process starts at that point where another process stopped it. It defines the characteristics of a multitasking operating system in which multiple processes shared the same CPU to perform multiple tasks without the need for additional processors in the system.

The need for Context switching

A context switching helps to share a single CPU across all processes to complete its execution and store the system's tasks status. When the process reloads in the system, the execution of the process starts at the same point where there is conflicting.

Following are the reasons that describe the need for context switching in the Operating system.

1. The switching of one process to another process is not directly in the system. A context switching helps the operating system that switches between the multiple processes to use the CPU's resource to accomplish its tasks and store its context. We can resume the service of the process at the same point later. If we do not store the currently running process's data or context, the stored data may be lost while switching between processes.
2. If a high priority process falls into the ready queue, the currently running process will be shut down or stopped by a high priority process to complete its tasks in the system.
3. If any running process requires I/O resources in the system, the current process will be switched by another process to use the CPUs. And when the I/O requirement is met, the old process goes into a ready state to wait for its execution in the CPU. Context switching stores the state of the process to resume its tasks in an operating system. Otherwise, the process needs to restart its execution from the initials level.
4. If any interrupts occur while running a process in the operating system, the process status is saved as registers using context switching. After resolving the interrupts, the process switches from a wait state to a ready state to resume its execution at the same point later, where the operating system interrupted occurs.
5. A context switching allows a single CPU to handle multiple process requests simultaneously without the need for any additional processors.

Q- Premitive and non primitive in Operating system

Ans-

1. Preemptive Scheduling:

Preemptive scheduling is used when a process switches from running state to ready state or from the waiting state to ready state. The resources (mainly CPU cycles) are allocated to the process for a limited amount of time and then taken away, and the process is again placed back in the ready queue if that process still has CPU burst time remaining. That process stays in the ready queue till it gets its next chance to execute.

Algorithms based on preemptive scheduling are: Round Robin (RR),Shortest Remaining Time First (SRTF), Priority (preemptive version), etc.

Process	Arrival Time	CPU Burst Time (in millisec.)
P0	3	2
P1	2	4
P2	0	6
P3	1	4

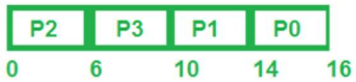
Preemptive Scheduling

2. Non-Preemptive Scheduling:

Non-preemptive Scheduling is used when a process terminates, or a process switches from running to the waiting state. In this scheduling, once the resources (CPU cycles) are allocated to a process, the process holds the CPU till it gets terminated or reaches a waiting state. In the case of non-preemptive scheduling does not interrupt a process running CPU in the middle of the execution. Instead, it waits till the process completes its CPU burst time, and then it can allocate the CPU to another process.

Algorithms based on non-preemptive scheduling are: Shortest Job First (SJF basically non preemptive) and Priority (non preemptive version), etc.

Process	Arrival Time	CPU Burst Time (in millisec.)
P0	3	2
P1	2	4
P2	0	6
P3	1	4



Non-Preemtive Scheduling

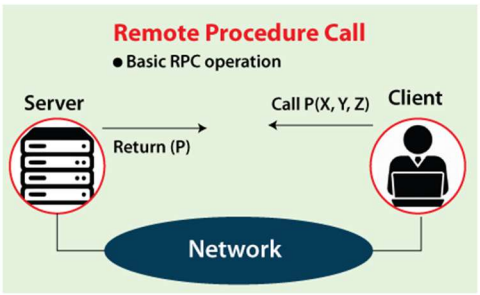
Q-Remote process control

Ans-

What is RPC in Operating System?

← Prev Next →

Remote Procedure Call or RPC is a powerful technique for constructing distributed, client-server-based applications. It is also known as a function call or a subroutine call. A remote procedure call is when a computer program causes a procedure to execute in a different address space, coded as a local procedure call, without the programmer explicitly stating the details for the remote interaction. The programmer writes essentially the same code whether the subroutine is local to the executing program or remote. This is a form of client-server interaction implemented via a request-response message-passing system.



The RPC model implies ***location transparency*** that calling procedures are largely the same, whether local or remote. Usually, they are not identical, so that local calls can be distinguished from remote calls. Remote calls are usually orders of magnitude slower and less reliable than local calls, so distinguishing them is important.

RPCs are a form of inter-process communication (IPC), in that different processes have different address spaces. They have distinct virtual address spaces on the same host machine, even though the physical address space is the same. While if they are on different hosts, the physical address space is different.

Q-Deadlock, Prevention and avoidance of Deadlock

Ans-

Introduction to Deadlock

Every process needs some resources to complete its execution. However, the resource is granted in a sequential order.

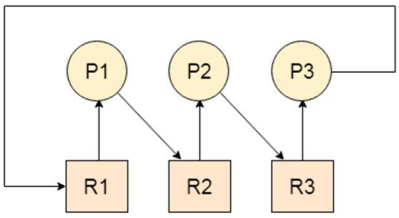
1. The process requests for some resource.
2. OS grant the resource if it is available otherwise let the process waits.
3. The process uses it and release on the completion.

A Deadlock is a situation where each of the computer process waits for a resource which is being assigned to some another process. In this situation, none of the process gets executed since the resource it needs, is held by some other process which is also waiting for some other resource to be released.

Let us assume that there are three processes P1, P2 and P3. There are three different resources R1, R2 and R3. R1 is assigned to P1, R2 is assigned to P2 and R3 is assigned to P3.

After some time, P1 demands for R1 which is being used by P2. P1 halts its execution since it can't complete without R2. P2 also demands for R3 which is being used by P3. P2 also stops its execution because it can't continue without R3. P3 also demands for R1 which is being used by P1 therefore P3 also stops its execution.

In this scenario, a cycle is being formed among the three processes. None of the process is progressing and they are all waiting. The computer becomes unresponsive since all the processes got blocked.



Head-to-head comparison between Deadlock Prevention and Deadlock Avoidance

Here, you will learn about the head-to-head comparison between Deadlock Prevention and Deadlock Avoidance. Some main differences between the Deadlock Prevention and Deadlock Avoidance are as follows:

Features	Deadlock Prevention	Deadlock Avoidance
Definition	It assures that at least one of the four deadlock conditions never occurs.	It prevents the system from coming to an unsafe state.
Procedure	It prevents deadlock by limiting the resource request process and resource handling.	It automatically evaluates requests and determines whether they are safe for the system.
Resource Request	All the resources in deadlock prevention are requested together.	Resource requests in deadlock avoidance are executed according to the safe path.
Resource Allocation Strategy	It is conservative in deadlock prevention.	It is not conservative in deadlock avoidance.
Information	It doesn't need information about existing resources, resource requests, and available resources.	It needs information about existing resources, resource requests, and available resources.
Pre-emption	In deadlock prevention, it occurs more frequently.	There is no pre-emption in deadlock avoidance.

Q-Banker's Algorithm

Ans-

The banker's algorithm is a resource allocation and deadlock avoidance algorithm that tests for safety by simulating the allocation for predetermined maximum possible amounts of all resources, then makes an "s-state" check to test for possible activities, before deciding whether allocation should be allowed to continue.

Why Banker's algorithm is named so?

Banker's algorithm is named so because it is used in banking system to check whether loan can be sanctioned to a person or not. Suppose there are n number of account holders in a bank and the total sum of their money is S. If a person applies for a loan then the bank first subtracts the loan amount from the total money that bank has and if the remaining amount is greater than S then only the loan is sanctioned. It is done because if all the account holders comes to withdraw their money then the bank can easily do it.

In other words, the bank would never allocate its money in such a way that it can no longer satisfy the needs of all its customers. The bank would try to be in safe state always.

Following **Data structures** are used to implement the Banker's Algorithm:

Let **'n'** be the number of processes in the system and **'m'** be the number of resources types.

- It is a 1-d array of size **'m'** indicating the number of available resources of each type.
- Available[j] = k means there are **'k'** instances of resource type $\mathbf{R_j}$

Max :

- It is a 2-d array of size **'n*m'** that defines the maximum demand of each process in a system.
- Max[i, j] = k means process $\mathbf{P_i}$ may request at most **'k'** instances of resource type $\mathbf{R_j}$.

Allocation :

- It is a 2-d array of size **'n*m'** that defines the number of resources of each type currently allocated to each process.
- Allocation[i, j] = k means process $\mathbf{P_i}$ is currently allocated **'k'** instances of resource type $\mathbf{R_j}$

Q-Paging Numerical

Ans-

Paging with Example

← Prev Next →

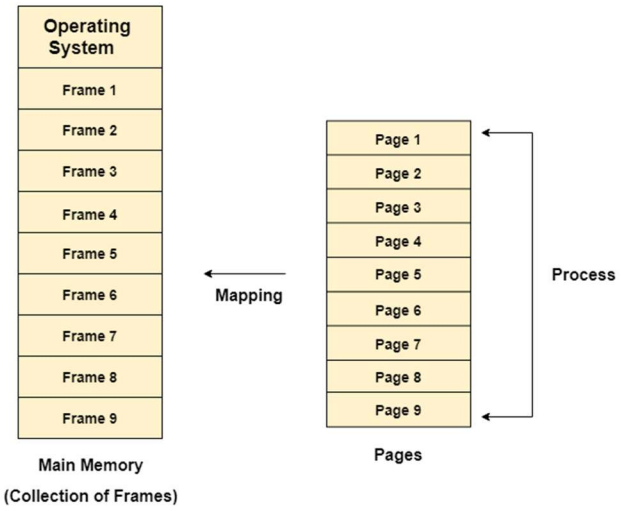
In Operating Systems, Paging is a storage mechanism used to retrieve processes from the secondary storage into the main memory in the form of pages.

The main idea behind the paging is to divide each process in the form of pages. The main memory will also be divided in the form of frames.

One page of the process is to be stored in one of the frames of the memory. The pages can be stored at the different locations of the memory but the priority is always to find the contiguous frames or holes.

Pages of the process are brought into the main memory only when they are required otherwise they reside in the secondary storage.

Different operating system defines different frame sizes. The sizes of each frame must be equal. Considering the fact that the pages are mapped to the frames in Paging, page size needs to be as same as frame size.

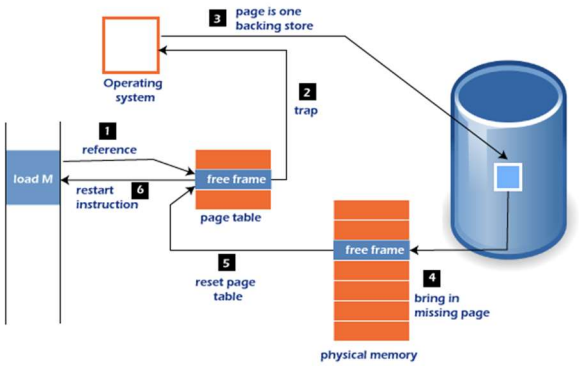


Q-Page Fault

Ans-

What is Page Fault in Operating System?

Page faults dominate more like an **error**. A page fault will happen if a program tries to access a piece of memory that does not exist in physical memory (main memory). The fault specifies the operating system to trace all data into virtual memory management and then relocate it from secondary memory to its primary memory, such as a hard disk.

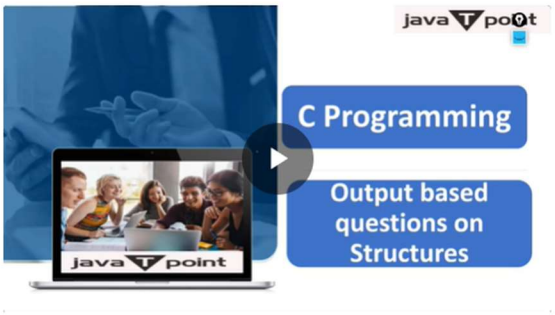


A page fault trap occurs if the requested page is not loaded into memory. The page fault primarily causes an exception, which is used to notify the operating system to retrieve the **"pages"** from virtual memory to continue operation. Once all of the data has been placed into physical memory, the program resumes normal operation. The Page fault process occurs in the background, and thus the user is unaware of it.

1. The computer's hardware track to the kernel and the program counter is often saved on the stack. The CPU registers hold information about the current state of instruction.
2. An assembly program is started, which saves the general registers and other volatile data to prevent the Operating system from destroying it.

Page Fault Handling

A Page Fault happens when you access a page that has been marked as invalid. The paging hardware would notice that the invalid bit is set while translating the address across the page table, which will cause an operating system trap. The trap is caused primarily by the OS's failure to load the needed page into memory.



Now, let's understand the procedure of page fault handling in the OS:

1. Firstly, an internal table for this process to assess whether the reference was valid or invalid memory access.
2. If the reference becomes invalid, the system process would be terminated. Otherwise, the page will be paged in.
3. After that, the free-frame list finds the free frame in the system.
4. Now, the disk operation would be scheduled to get the required page from the disk.
5. When the I/O operation is completed, the process's page table will be updated with a new frame number, and the invalid bit will be changed. Now, it is a valid page reference.
6. If any page fault is found, restart these steps from starting.

Page Fault Terminology

There are various page fault terminologies in the operating system. Some terminologies of page fault are as follows:

1. Page Hit

When the CPU attempts to obtain a needed page from main memory and the page exists in **main memory (RAM)**, it is referred to as a **"PAGE HIT"**.

2. Page Miss

If the needed page has not existed in the **main memory (RAM)**, it is known as **"PAGE MISS"**.

3. Page Fault Time

The time it takes to get a page from secondary memory and recover it from the main memory after loading the required page is known as **"PAGE FAULT TIME"**.

4. Page Fault Delay

The rate at which threads locate page faults in memory is referred to as the **"PAGE FAULT RATE"**. The page fault rate is measured per second.

5. Hard Page Fault

If a required page exists in the hard disk's page file, it is referred to as a **"HARD PAGE FAULT"**.

Q-External and internal fragmentation

Ans-

What is Fragmentation?

"Fragmentation is a process of data storage in which memory space is used inadequately, decreasing ability or efficiency and sometimes both." The precise implications of fragmentation depend on the specific storage space allocation scheme in operation and the particular fragmentation type. In certain instances, fragmentation contributes to "unused" storage capacity, and the concept also applies to the unusable space generated in that situation. The memory used to preserve the data set (- for example file format) is similar for other systems (- for example, the FAT file system), regardless of the amount of fragmentation (from null to the extreme).

There are three distinct fragmentation kinds: internal fragmentation, external fragmentation, and data fragmentation that can exist beside or a combination. In preference for enhancements, inefficiency, or usability, fragmentation is often acknowledged. For other tools, such as processors, similar things happen.

Internal Fragmentation

Most memory space is often reserved than is required to adhere to the restrictions regulating storage space. For instance, memory can only be supplied in blocks (multiple of 4) to systems, and as an outcome, if a program demands maybe 29 bytes, it will get a coalition of 32 bytes. The surplus storage goes to waste when this occurs. The useless space is found inside an assigned area in this case. This structure, called fixed segments, struggles from excessive memory-any process consumes an enormous chunk, no matter how insignificant. Internal fragmentation is what this garbage is termed. Unlike many other forms of fragmentation, it is impossible to restore inner fragmentation, typically, the only way to eliminate it is with a new design.

External Fragmentation

When used storage is differentiated into smaller lots and is punctuated by assigned memory space, external fragmentation occurs. It is a weak point of many storage allocation methodologies when they cannot effectively schedule memory used by systems. The consequence is that, while unused storage is available, it is essentially inaccessible since it is separately split into fragments that are too limited to meet the software's requirements. The word "external" derives from the fact that the inaccessible space is stored outside the assigned regions.

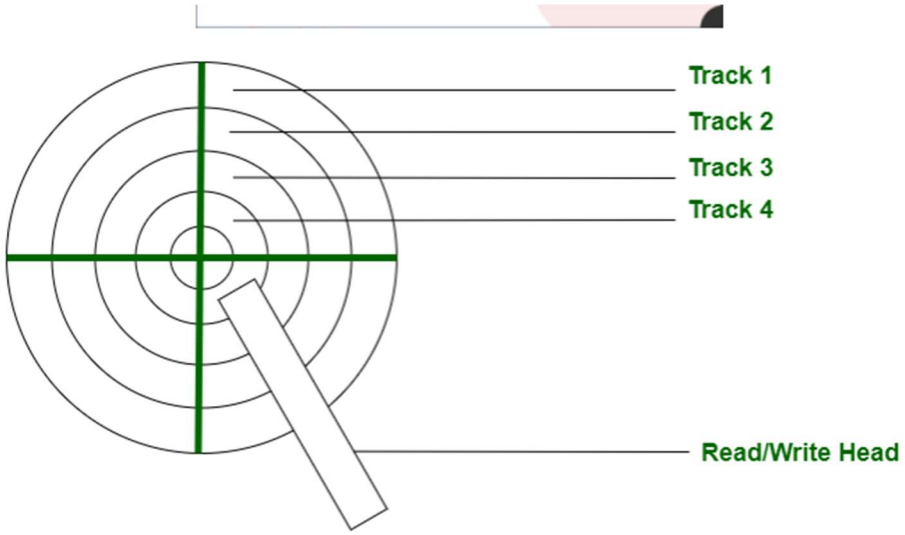
Consider, for instance, a scenario in which a system assigns three consecutive memory blocks and then relieves the middle block. The memory allocator can use this unused allocation of the storage for future assignments. Fortunately, if the storage to be reserved is more generous in size than this available region, it will not use this component.

Q-Seek Time and Latency

Ans-

Seek Time:

A disk is divided into many circular tracks. Seek Time is defined as the time required by the read/write head to move from one track to another.



Rotational Latency:

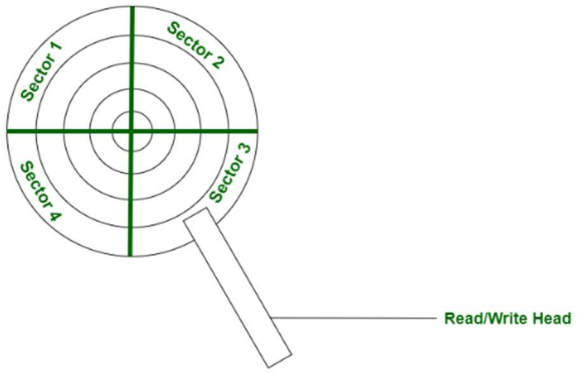
The disk is divided into many circular tracks, and these tracks are further divided into blocks knows as sectors. The time required by the read/write head to rotate to the requested sector from the current position is called Rotational Latency.

Example,

Consider the following diagram, We have divided each track into 4 sectors.

The systems get a request to read a sector from track 1, thus the read/write head will move to track 1 and this time will be seek time.

The read/write head is currently in sector 3.



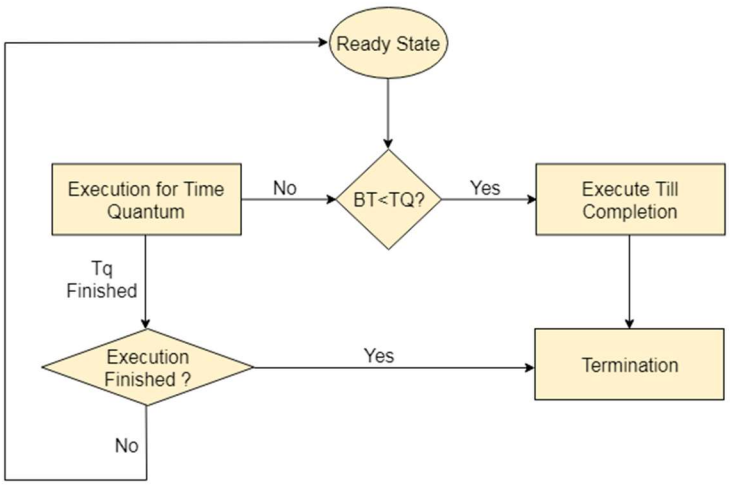
Q- Round Robin

Ans-

Round Robin Scheduling Algorithm

← Prev Next →

Round Robin scheduling algorithm is one of the most popular scheduling algorithm which can actually be implemented in most of the operating systems. This is the **preemptive version** of first come first serve scheduling. The Algorithm focuses on Time Sharing. In this algorithm, every process gets executed in a **cyclic way**. A certain time slice is defined in the system which is called time **quantum**. Each process present in the ready queue is assigned the CPU for that time quantum, if the execution of the process is completed during that time then the process will **terminate** else the process will go back to the **ready queue** and waits for the next turn to complete the execution.



Advantages

1. It can be actually implementable in the system because it is not depending on the burst time.
2. It doesn't suffer from the problem of starvation or convoy effect.
3. All the jobs get a fare allocation of CPU.

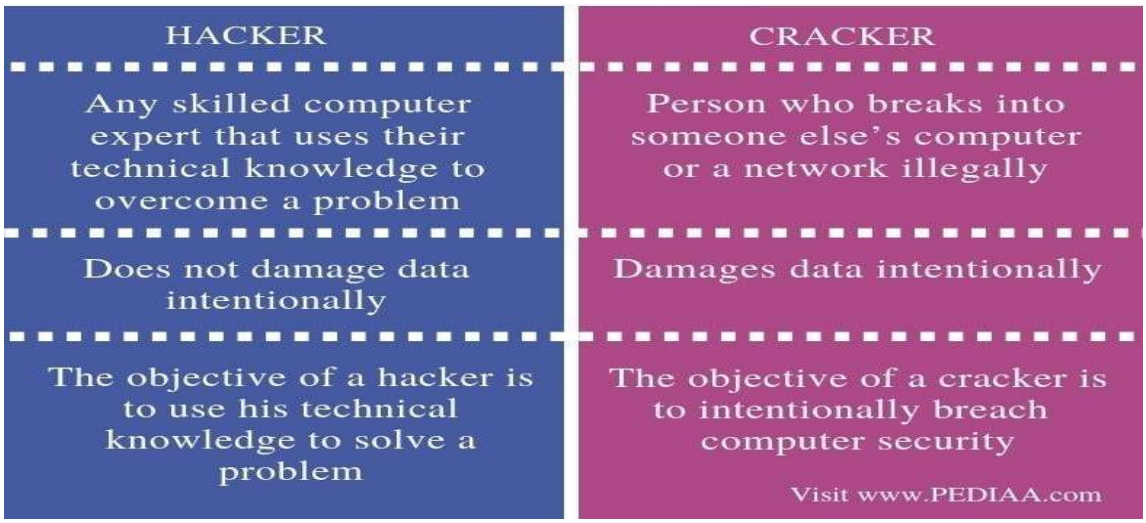
Disadvantages

1. The higher the time quantum, the higher the response time in the system.
2. The lower the time quantum, the higher the context switching overhead in the system.
3. Deciding a perfect time quantum is really a very difficult task in the system.

Q1. What is Fork system call?
Ans. Fork system call is used for creating a new process, which is called child process, which runs concurrently with the process that makes the fork() call (parent process). After a new child process is created, both processes will execute the next instruction following the fork() system call.

Q2. What is a semaphore?
Ans. Semaphores refer to the integer variables that are primarily used to solve the critical section problem via combining two of the atomic procedures, wait and signal, for the process synchronization.

Q3. Distinguish between hacker and cracker?
Ans.



Q4. What is cypher text?
Ans. Cipher text is encrypted text transformed from plain text using an encryption algorithm. Cipher text can't be read until it has been converted

into plain text (decrypted) with a key. The decryption cipher is an algorithm that transforms the cipher text back into plain text.

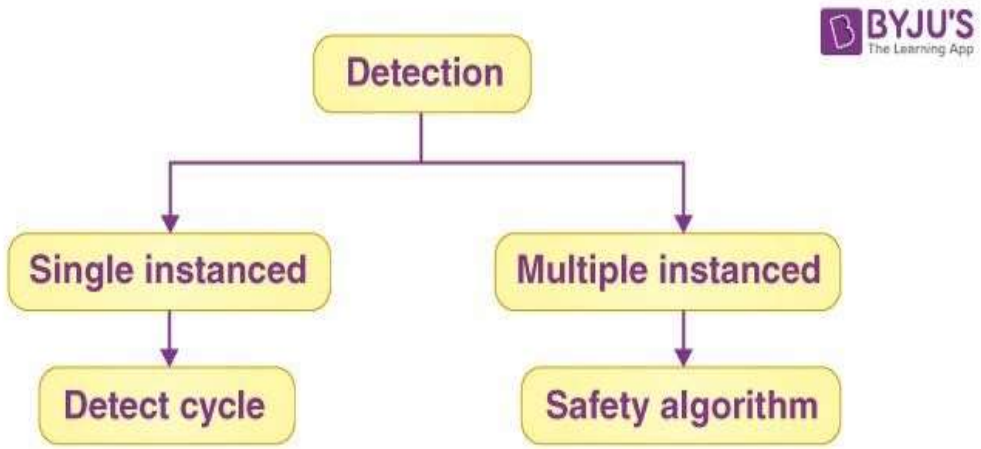
Q5. What is a peer to peer network?

Ans. Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal, they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux, and Windows, can function as peer-to-peer network operating systems.

Q6. When does the deadlock occur? Explain deadlock detection and recovery in detail.

Ans. Deadlock occurs when a set of processes are in a wait state, because each process is waiting for a resource that is held by some other waiting process. Therefore, all deadlocks involve conflicting resource needs by two or more processes.

Deadlock detection:- The OS does not use any mechanisms to avoid or prevent deadlocks in this approach. As a result, the system predicts that the deadlock will occur. The OS periodically scans the system for any deadlocks in order to avoid them. If any deadlocks are discovered, the OS will attempt to restore the system using several ways.



Deadlock Recovery:- OS examines either resources or processes to recover the system from deadlocks.

For Resource

Preempt the resource:- We can take one of the resources from the resource owner (process) and give it to another process in the hopes that it will finish the execution and release the resource sooner. Choosing a resource that will be snatched will be challenging.

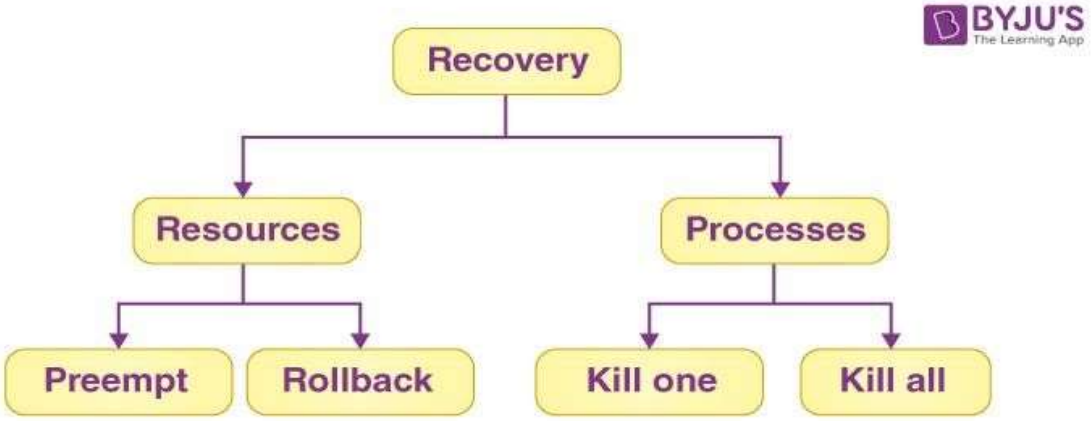
Rollback to a safe state:- To reach the deadlock state, the system happens to go through several states. The operating system has the ability to restore the system to a previous safe state. The OS must implement checkpointing at each state for this to work.

When we reach a deadlock, we must reverse all allocations and return to the prior safe state.

For Process

Kill a process:- Our problem can be solved by killing a process; however, the bigger issue is deciding which process to kill. A process that has done the least amount of work till now is usually killed by the operating system.

Kill all processes:- This is not a persuasive strategy, but it may be used if the problem becomes extremely serious. Killing all processes will result in system inefficiencies because all processes will have to start over.



Q7. What is critical section problem? Explain any one problem with solution.

Ans. The critical section problem is to make sure that only one process should be in a critical section at a time. When a process is in the critical

section, no other processes are allowed to enter the critical section. This solves the race condition.

Progress:- Progress means that if a process is not using the critical section, then it should not stop any other process from accessing it. In other words, any process can enter a critical section if it is free.

Q8. Explain with the help of diagram functionality of client server network?

Ans. A client-server network is the medium through which clients access resources and services from a central computer, via either a local area network (LAN) or a wide-area network (WAN), such as the Internet.

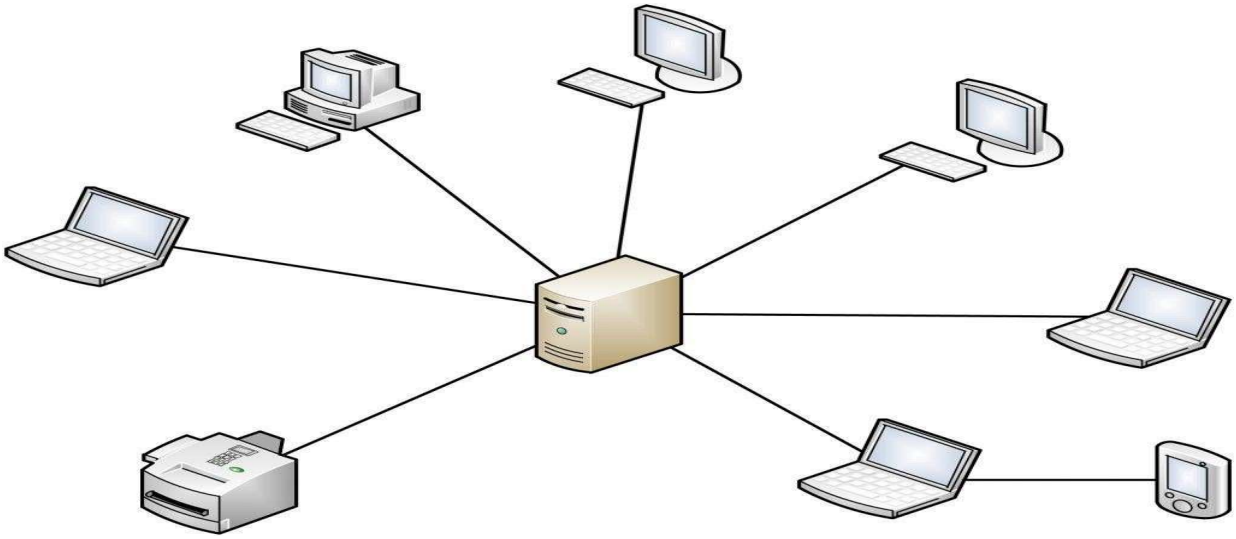


Diagram of Client Server Network

Q9. Elaborate the concept of system threat with the help of example.

Ans. System threat contains viruses, worms, trojan horses, and other dangerous software. These are generally short code snippets that may corrupt files, delete the data, replicate to propagate further, and even crash a system.

Q10. Which of the following scheduling algorithms could result in starvation? Explain in detail:a. First-come, first-served

b. Shortest job first

c. Round robin

d. Priority

Ans. Priority Scheduling:- It is a non pre-emptive Algorithm that works in batch systems and in this each process is given a priority and the process with highest priority is executed first and others are executed according to priorities which can lead to starvation for those processes.

a. **First-come, first-served:-** FCFS is the simplest of CPU Scheduling Algorithm which executes the process that comes first. It is a nonpreemptive algorithm. The process that arrives first in the ready queue gets to be executed by the CPU first, then the second one, then the third one, and so on.

b. **Shortest job first:-** Shortest job first is a scheduling algorithm in which the process with the smallest execution time is selected for execution next. Shortest job first can be either preemptive or nonpreemptive. Owing to its simple nature, shortest job first is considered optimal.

c. **Round robin:-** Round Robin is a CPU scheduling algorithm where each process is assigned a fixed time slot in a cyclic way. It is basically the preemptive version of First come First Serve CPU Scheduling algorithm.

d. **Priority:-** Priority scheduling is a non-preemptive algorithm and one of the most common scheduling algorithms in batch systems. Each process is assigned first arrival time (less arrival time process first) if two processes have same arrival time, then compare to priorities (highest process first).

Q11. Explain the concept of virtual memory along with demand paging?

Ans.Virtual memory:- It is actually the memory of the hard disk and it is then mapped into the physical memory.

Demand Paging:- Demand paging is a type of swapping done in virtual memory systems. In demand paging, the data is not copied from the disk to the RAM until they are needed or being demanded by some program.

Q12. Explain DDOs? Explain the difference between DDOS and DOS attack.

Ans. DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cyber criminals employ in order to make an

online service, network resource or host machine unavailable to its intended users on the Internet.

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single	Victim PC is loaded from the packet of data sent from Multiple
DOS	DDOS
	location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.

Types of DOS Attacks are:	Types of DDOS Attacks are:
1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

Q13. What are the three main uses of OS?

Ans. An operating system has three main uses:-

1. Manage the computer's resources, such as the central processing unit, memory, disk drives, and printers.

2. Establish a user interface.

3. Execute and provide services for applications software.

Q14. What is deadlock?

Ans. A deadlock is a situation in which two computer programs sharing the same resource are effectively preventing each other from accessing the resource, resulting in both programs ceasing to function. The earliest computer operating systems ran only one program at a time.

Q15. What is segmentation?

Ans. In Operating Systems, Segmentation is a memory management technique in which the memory is divided into the variable size parts. Each part is known as a segment which can be allocated to a process.

Q16. What are the different types of networks?

Ans. There are 4 types of network:-

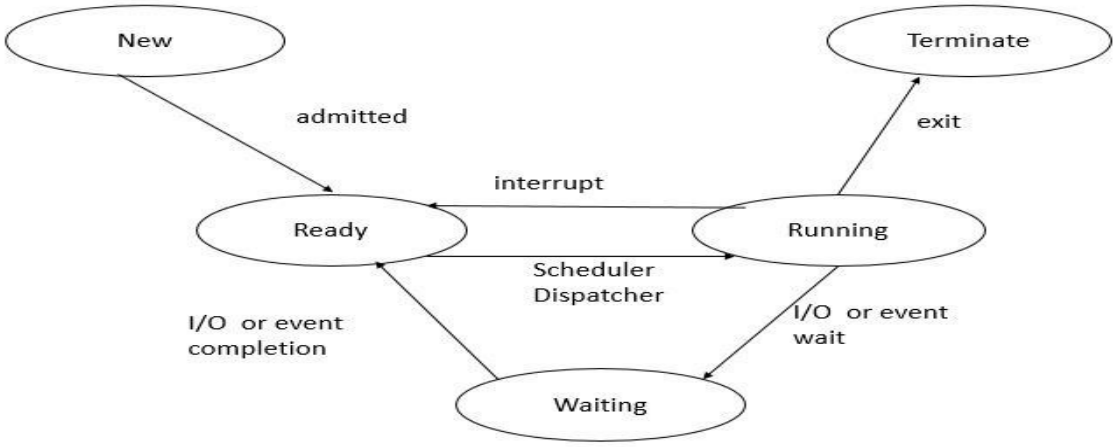
1. PAN
2. WAN
3. LAN
4. Campus Network

Q17. What is session hijacking?

Ans. Session hijacking is a technique used by hackers to gain access to a target's computer or online accounts. In a session hijacking attack, a

hacker takes control of a user's browsing session to gain access to their personal information and passwords.

Q18. a.) With the help of a neat diagram elaborate the concept of process and its states?
b.) Construct the Process Control Block along with its description in detail?
Ans.
a.

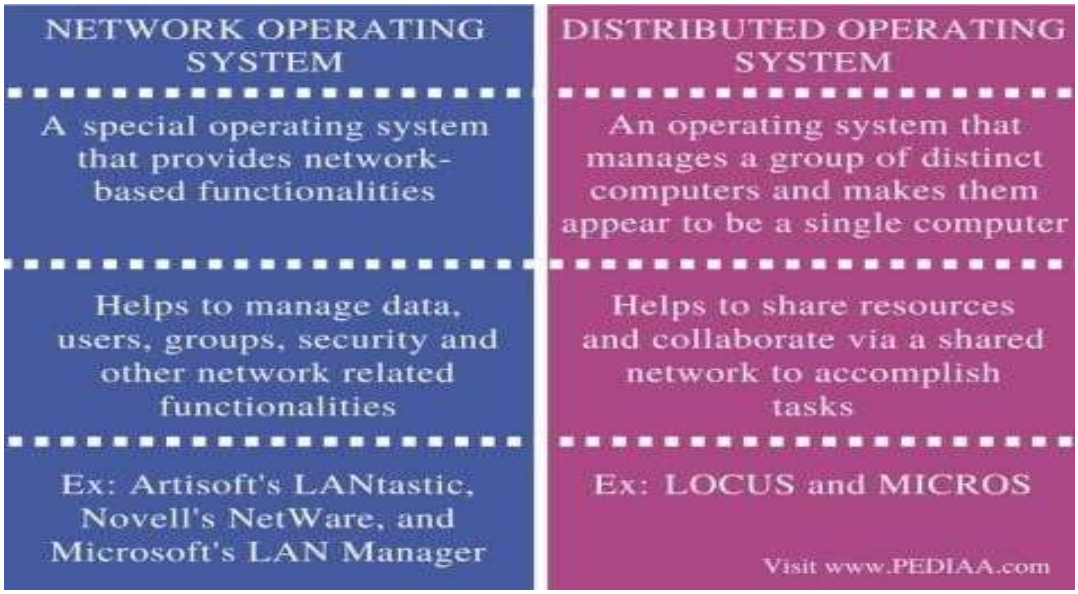


b. A **process control block** (**PCB**) is a data structure used by computer operating systems to store all the information about a process. It is also known as a process descriptor. When a process is created (initialized or installed), the operating system creates a corresponding process control block. This specifies the process state i.e. new, ready, running, waiting or terminated.

Q18. Consider a disk with 200 tracks and the queue has random requests from different processes in the order:
55, 58, 39, 18, 90, 160, 150, 38, 184
Initially arm is at 100. Find the Average Seek length using FIFO, SSTF.

Ans. We assume a disk with 200 tracks and disk request queue has random requests in it. The requested disks in the order are 55,58,39,18,90,160,150,38,184 starting with a track 100. (ques10.com)
Q19. With suitable example differentiate between Network Operating System and Distributed Operating System.

Ans.



Q21. What is access matrix? Explain the implementation of access matrix?

Ans. Access Matrix is a security model of protection state in computer system. It is represented as a matrix. Access matrix is used to define the rights of each process executing in the domain with respect to each object. The rows of matrix represent domains and columns represent objects.

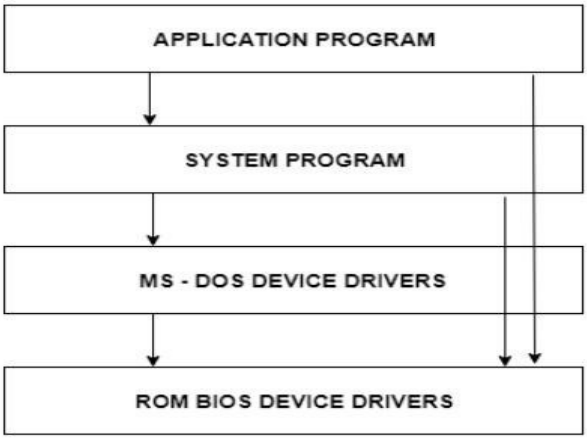
There are various methods of implementing the access matrix in the operating system. These methods are as follows:

- Global Table
- Access Lists for Objects
- Capability Lists for Domains
- Lock-Key Mechanism

Q22. Enumerate the different operating system structure and explain with neat sketch?

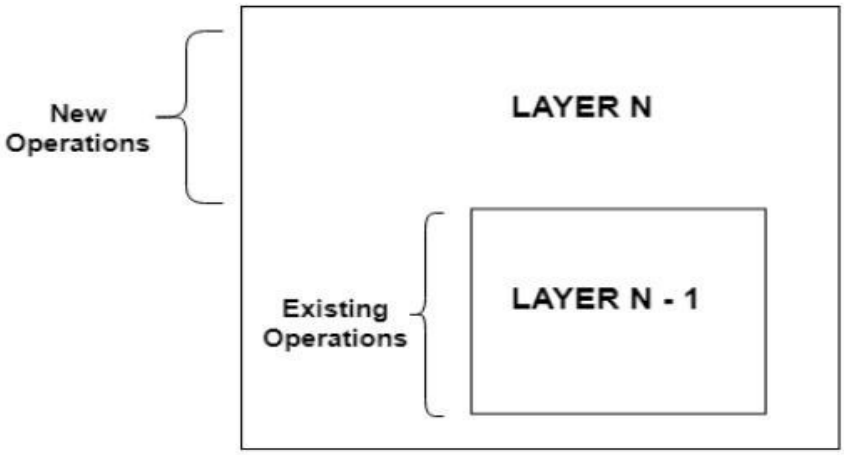
Ans. There are 2 different OS structure:-

1. Simple Structure:-



MS-DOS STRUCTURE

2. Layered Structure:-



Layered Structure of Operating System

Q23.

a. Evaluating the maximum number of pages needed, if a system supports 16 bit address line and 1K page size.

b. What is the difference between user-level instructions and privileged instructions?

Ans.

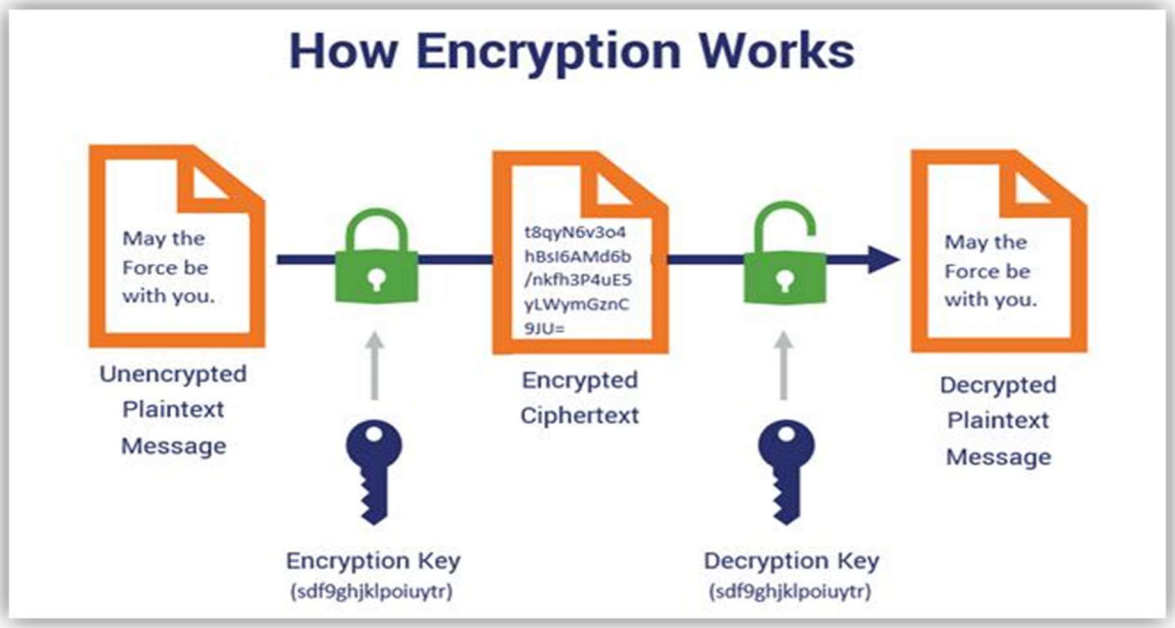
a. A 16 bit address can locate up to 2^16 = 65536 locations (bytes). Given page size is 0.5 KB = 512 Bytes (Ref: 1 KB = 1024 Bytes). Therefore, total pages = 65536/512 = **128 pages**.

b. **i. User-level Instruction:-** The Instructions that can run only in User Mode are called Non-Privileged Instructions or User-level Instruction.

ii. Privileged Instructions:- The Instructions that can run only in Kernel Mode are called Privileged Instructions.

Q24. What is encryption? Explain the working with the help of example?

Ans. Encryption is an important way for individuals and companies to protect sensitive information from hacking. For example, websites that transmit credit card and bank account numbers encrypt this information to prevent identity theft and fraud.



Q25. What is TLB?

Ans. A translation lookaside buffer (TLB) is a memory cache that stores recent translations of virtual memory to physical addresses for faster retrieval. When a virtual memory address is referenced by a program, the search starts in the CPU. First, instruction caches are checked.

Q26. Define access time?

Ans. Access time refers to how fast the disk or memory can locate and begin retrieving (accessing) a specific piece of information or transfer data to the CPU. For a disk drive, the access time includes both the head seek time and the latency.

Q27. What is time sharing OS?
Ans. The Time-Sharing OS provides computer resources to numerous programs simultaneously in a time-dependent manner. As a result, it aids in providing direct access to the main computer to a large number of users.

Q28. What is worm?
Ans. A worm is a type of malware whose primary function is to selfreplicate and infect other computers while remaining active on infected systems. A computer worm duplicates itself to spread to uninfected computers.

Q29. What are the advantages of star topology?
Ans.

- It is very reliable – if one cable or device fails then all the others will still work
- It is high-performing as no data collisions can occur
- Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
- Easier to put in
- Robust in nature
- Easy fault detection because the link are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

Q30. What do you mean by page-fault? When does page-fault occur? Describe the action taken by the O.S when page fault occur? Ans. In computing, a page fault (sometimes called PF or hard fault) is an exception that the memory management unit (MMU) raises when a process accesses a memory page without proper preparations. Accessing the page requires a mapping to be added to the process's virtual address space.
Page fault occurs when a requested page is mapped in virtual address space but not present in memory.
A page fault occurs when an access to a page that has not been brought into main memory takes place. The operating system verifies the memory access, aborting the program if it is invalid.

Q31. Explain CIA in detail?

Ans. Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

Q32. Write a short note on levels of security measures and what is the difference between security and protection

Ans. The most common techniques used to protect operating systems include the use of antivirus software and other endpoint protection measures, regular OS patch updates, a firewall for monitoring network traffic, and enforcement of secure access through least privileges and user controls.

Q33. What are the different type of operating systems in detail. Also describe advantages and disadvantages of each type?

Ans.

- Batch OS
- Time-sharing OS
- Network OS
- Distributed OS ➢ Real-time OS

1. Batch OS:-

Advantages of Batch Operating System:

- It is very difficult to guess or know the time required for any job to complete. Processors of the batch systems know how long the job would be when it is in queue
- Multiple users can share the batch systems
- The idle time for the batch system is very less ➢ It is easy to manage large work repeatedly in batch systems

Disadvantages of Batch Operating System:

- The computer operators should be well known with batch systems
- Batch systems are hard to debug
- It is sometimes costly
- The other jobs will have to wait for an unknown time if any job fails

2. Time-sharing OS:*Advantages of Time-Sharing OS:*

- Each task gets an equal opportunity
- Fewer chances of duplication of software ➢ CPU idle time can be reduced

Disadvantages of Time-Sharing OS:

- Reliability problem
- One must have to take care of the security and integrity of user programs and data
- Data communication problem

3. Network OS:-

Advantages of Network Operating System:

- Highly stable centralized servers
- Security concerns are handled through servers
- New technologies and hardware up-gradation are easily integrated into the system
- Server access is possible remotely from different locations and types of systems

Disadvantages of Network Operating System:

- Servers are costly
- User has to depend on a central location for most operations
- Maintenance and updates are required regularly

4. Distributed OS:-

Advantages of Distributed Operating System:

- Failure of one will not affect the other network communication, as all systems are independent from each other
- Electronic mail increases the data exchange speed
- Since resources are being shared, computation is highly fast and durable
- Load on host computer reduces
- These systems are easily scalable as many systems can be easily added to the network
- Delay in data processing reduces

Disadvantages of Distributed Operating System:

- Failure of the main network will stop the entire communication
- To establish distributed systems the language which is used are not well defined yet
- These types of systems are not readily available as they are very expensive. Not only that the underlying software is highly complex and not understood well yet

5. Real-time OS:*Advantages of RTOS:*

- Maximum Consumption
- Task Shifting
- Focus on Application
- Real-time operating system in the embedded system
- Error Free
- Memory Allocation

Disadvantages of RTOS:

- Limited Tasks
- Use heavy system resources
- Complex Algorithms
- Device driver and interrupt signals ➢ Thread Priority

Q34. Explain the concept of FRAGMENTATION in detail?

Ans. Fragmentation refers to an unwanted problem that occurs in the OS in which a process is unloaded and loaded from memory, and the free memory space gets fragmented. The processes can not be assigned to the memory blocks because of their small size. Thus the memory blocks always stay unused.

Q35.

A. What is the difference between a client and a server?

B. Distinguish between client-server and peer to peer models of distributed system.

Ans. A.

Parameters	**Server OS**	**Client OS**
Basics	We use a Server OS for providing various services to multiple numbers of clients.	We use a Client OS for obtaining various services from any given server.
Number of Users/ Clients	A Server OS is capable of serving multiple clients at any given time.	The Client OS is capable of serving just a single client at any given time.
Complexity	It is a complex type of OS.	It is a fairly simple type of OS.
Medium	A server OS basically runs on a given server.	A client OS basically runs on various client devices, such as computers, laptops, etc.
Operations	This type of OS is designed in a way that it operates on any server.	This type of OS is designed in a way that it operates within a desktop.
Security	It is comparatively more secure.	It is comparatively much less secure.
Processing Power	The processing power is fairly high in Server OS.	The processing power is much lower in Client OS.
Efficiency	The Server OS is highly efficient.	The Client OS is comparatively less efficient.

Stability	Server OS is much more stable.	Client OS is much less stable.
Examples	Linux, Red Hat, etc., are a few examples of the Server OS.	Android, Windows, etc., are a few examples of the Client OS.

B.

Client-Server Architecture	Peer-to-Peer Architecture
A clear separation between clients and servers.	No differentiation between clients and servers.
Data is provided only in response to a request.	Peers have the authority to request as well as provide a service.
Centralized data management.	It has own data and applications.
Purpose is to store and exchange information.	Goal is to maintain connections among peers.
Suitable for small as well as large networks.	Suitable for less number of users or devices.