MCA

Systems Analysis and Design

Qualifications of a Systems Analyst

A systems analyst must fulfil the following requirements.

- Working knowledge of information technology
- Computer programming experience and expertise
- General business knowledge
- Problem solving kills
- Communication skills
- Interpersonal skills
- Flexibility and adaptability
- Thorough knowledge of analysis and design methodologies

In summary, the skills that are required may be classified into the following.

- Analytical skills
- Technical skills
- Management skills
- Interpersonal skills

Analytical Skills:

It is the ability to see things as systems, identify, analyze and solve problem in an optional way for a specific organization.

Technical Skills:

It is the ability to understand how computers, data networks, databases, operating systems etc. work together as well as their potentials and limitations.

Management Skills:

It include organization's recourse management, project management (people and money), risk management and change management.

Communication Skills:

It include effective interpersonal communication (written, verbal visual, electronic, face-to-face conversations, presentations in front of groups), listening, group facilitation skills.

Process of implementation of MIS

The choice of the system or the sub-system depends on its position in the total MIS plan, the size of the system, the user understands of the system and the complexity and its interface with other systems. The designer first develops systems independently and starts integrating them with other systems, enlarging the system scope and meeting the varying information needs. MIS is generally used by medium and larger scale organizations. However, small organizations are yet to understand its application. There is dire need to build up computer culture by properly disseminating information about computer application and its
Implementation of MIS can be achieved by using any of the methods such as direct, parallel, modular or phase in. • **Direct Approach** Direct installation of the new system with immediate discontinuance of the old existing system is referred as "cold turnkey" approach. This approach becomes useful when these factors are considered. 1. The new system does no replace the existing system. 2. Old system is regarded absolutely of no value 3. New system is compact and simple. 4. The design of the new system is inexpensive with more advantages and less risk involved. • **Parallel Approach** The selected new system is installed and operated with current system. This method is expensive because of duplicating facilities and personal to maintain both the systems. In this approach a target date must be fixed when the operations of old system cease and new one will operate on its own. • **Modular Approach** This is generally recognized as "Pilot approach", means the implementation of a system in the Organization on a piece-meal basis. This has few advantages / merits 1. The risk of systems failure is localized 2. The major problem can be easily identified and corrected before further implementation. 3. Operating personal can be trained before system is installed in a location. • **Phase-in-Implementation** This approach is similar to modular method but it differs because of segmentation of system, however, not the organization. It has advantages that the rate of changes in a given Organization can be totally minimized and the data processing resource can be acquired gradually over a period of time. System exhibits certain disadvantages such as

limited applicability, more costs incurred to develop interface with old system and a feeling in the Organization that system is never completed.

Implementation Procedures • Planning the Implementation After designing the MIS it is essential that the organization should plan carefully for implementation. The planning stage should invariably include the following: 1. Identification of tasks of Implementation 2. Relationship establishment among the activity 3. Establishing of MIS 4. Acquisition of Facilities 5. Procedure Development 6. Generating Files and Forms 7. Testing of the System

• **Evaluation and maintenance of system** The performance should e evaluated in order to find out cost effectiveness and efficacy of the system with minimum errors due to designs environmental changes or services.

Software Maintenances The proper maintenance is the enigma of the system development and it holds software industry captive lying up programming resources. There are some problems in maintenance such as regarding it as non rewarding non availability of technicians and tools no cognizance of users about maintenance problem and cost lack of standard procedures and guidelines. Most programmers feel maintenance as low level drudgery. If proper attentions is paid over a period of time eventually less maintenance is required.

Types of Maintenance The maintenance of system are classified into corrective/adaptive/perfective. Corrective maintenance means repairing process or performance failures. Adaptive maintenance means changing the programming function whereas perfective maintenance deals with enhancing the performance or modifying the program.

Primary Activities of a Maintenance Procedure Documentation is major part of maintenance in system development. Maintenance staff receives requests from the authorized user. Programming library should be maintained.

Reduction in Maintenance Costs Several organizations having MIS generally go in for reducing maintenance costs and it consists of three major phases. 1. Maintenance management audit through questionnaires and interviews. 2. Software system audit. 3. Software modification.

Evaluation Methods Evaluation of the MIS in an organization is integral part of the control processes. There are several evaluation approaches such as quality assurance review compliance of audits budget performance review computer personal productivity assessment computer performance evaluation service level monitoring user audit survey post installation review and cost benefit analysis. Evaluation performance measurement can be classified into two classes as effectiveness and efficiency. The relationship between effectiveness and efficiency is that the format is a measure of goodness of out put and the latter is a measure of the resources required to achieve the output.

Operating System Concepts and Networking Management

How is microkernel architecture different from kernel architecture? Explain.

Early operating system kernels were rather small, partly because computer memory was limited. As the capability of computers grew, the number of devices the kernel had to control also grew. Through the early history of Unix, kernels were generally small, even though those kernels contained device drivers and file system managers. When address spaces increased from 16 to 32 bits, kernel design was no longer cramped by the hardware architecture, and kernels began to grow.
Berkeley UNIX (BSD) began the era of big kernels. In addition to operating a basic system consisting of the CPU, disks and printers, BSD started adding additional file systems, a complete TCP/IP networking system, and a number of "virtual" devices that allowed the existing programs to work invisibly over the network. This growth continued for many years, resulting in kernels with millions of lines of source code. As a result of this growth, kernels were more prone to bugs and became increasingly difficult to maintain.
The microkernel was designed to address the increasing growth of kernels and the difficulties that came with them. In theory, the microkernel design allows for easier management of code due to its division into user space services. This also allows for increased security and stability resulting from the reduced amount of code running in kernel mode. For example, if a networking service crashed due to buffer overflow, only the networking service's memory would be corrupted, leaving the rest of the system still functional.

How is multithreading useful in uniprocessor as well as symmetric multiprocessing? Explain.

symmetric multiprocessing or SMP involves a multiprocessor computer hardware architecture where two or more identical processors are connected to a single shared main memory and are controlled by a single OS instance. Most common multiprocessor systems today use an SMP architecture. In the case of multi-core processors, the SMP architecture applies to the cores, treating them as separate processors. Processors may be interconnected using buses, crossbar switches or on-chip mesh networks. The bottleneck in the scalability of SMP using buses or crossbar switches is the bandwidth and power consumption of the interconnect among the various processors, the memory, and the disk arrays. Mesh architectures avoid these bottlenecks, and provide nearly linear scalability to much higher processor counts.
SMP systems allow any processor to work on any task no matter where the data for that task are located in memory, provided that each task in the system is not in execution on two or more processors at the same time; with proper operating system support, SMP systems can easily move tasks between processors to balance the workload efficiently.

What is the purpose of caching in DNS?

Ans. All Internet hosts, including your computer when it is connected to the Internet, use a DNS server. Every time you go to a website, you need to look up the site's IP address using the domain name of the website. Your request for this lookup is eventually passed to a DNS server somewhere.

But your request is one of thousands, even millions of requests being made at any one time across the Internet. The DNS lookup process requires that if your local DNS server is not Authoritative for the domain that contains the domain name you are trying to reach, it should ask other servers to get an answer. Your local server could get quite busy performing these lookup requests, and this could slow down its performance if it is Authoritative for a domain name. To combat this the answers that a DNS server gets from another DNS server can be added to their own internal database and retained for a period of time equal to the time to live (ttl) value set on the record stored on the Authoritative DNS server. Storing these responses is called caching, and allows a DNS server to respond more quickly to multiple queries for the same domain or host. If you are on a website, and want to retrieve the next page on the site, the local DNS server does not have to look up the host again, provided the time to live (ttl) value has not expired and caused the local DNS server to delete the information. This is why it takes so long to contact a website at first, but subsequent requests for pages on the same site are somewhat faster. Caching DNS servers are configured for recursive lookup as well. This creates a server that will respond to lookup requests by delivering answers from its cache, or looking them up on other servers. It is the job of a caching DNS server to handle general lookups of Internet domains. A caching DNS server reduces the load placed on an Authoritative DNS server by handling the requests that don not pertain to the local domain. Almost all Internet Service Providers (ISPs) operate some kind of caching DNS server.

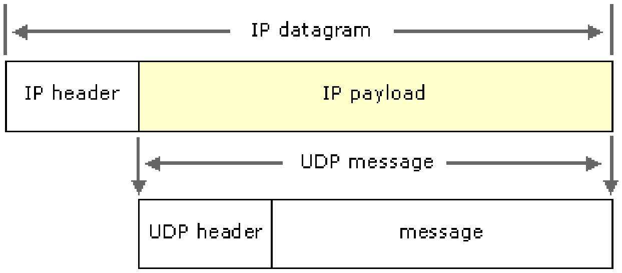
Unfortunately DNS caching is a double-edged sword. It speeds up resolution by storing recent answers, and short-circuiting the normal resolution process. However there is a down side. Because DNS servers cache answers, and don't delete these answers until the time to live (ttl) expires, it can take hours or days for the entire Internet to recognize changes to DNS information for your domain name

Question 1. D) Why UDP instead of TCP/IP is used in network management protocol?

User Datagram Protocol (UDP) is a TCP/IP standard defined in RFC 768, "User Datagram Protocol (UDP)." UDP is used by some programs instead of TCP for fast, lightweight, unreliable transportation of data between TCP/IP hosts.

UDP provides a connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. A source host that needs reliable communication must use either TCP or a program that provides its own sequencing and acknowledgment services.

UDP messages are encapsulated and sent within IP datagrams, as shown in the following illustration.



How is Linux different from Unix operating sysem? Explain.

UNIX is copyrighted name only big companies are allowed to use the UNIX copyright and name, so IBM AIX and Sun Solaris and HP-UX all are UNIX operating systems. The Open Group holds the UNIX trademark in trust for the industry, and manages the UNIX trademark licensing program.Most UNIX systems are commercial in nature.

Linux is a UNIX Clone

But if you consider Portable Operating System Interface (POSIX) standards then Linux can be considered as UNIX. To quote from Official Linux kernel README file:

Linux is a Unix clone written from scratch by Linus Torvalds with assistance from a loosely-knit team of hackers across the Net. It aims towards POSIX compliance.

However, "Open Group" do not approve of the construction "Unix-like", and consider it misuse of their UNIX trademark.

Linux Is Just a Kernel

Linux is just a kernel. All Linux distributions includes GUI system + GNU utilities (such as cp, mv, ls,date, bash etc) + installation & management tools + GNU c/c++ Compilers + Editors (vi) + and various applications (such as OpenOffice, Firefox). However, most UNIX operating systems are considered as a complete operating system as everything come from a single source or vendor.

As I said earlier Linux is just a kernel and Linux distribution makes it complete usable operating systems by adding various applications. Most UNIX operating systems comes with A-Z programs such as editor, compilers etc. For example HP-UX or Solaris comes with A-Z programs.

License and cost

Linux is Free (as in beer [freedom]). You can download it from the Internet or redistribute it under GNU licenses. You will see the best community support for Linux. Most UNIX like operating systems are not free (but this is changing fast, for example OpenSolaris UNIX). However, some Linux distributions such as Redhat / Novell provides additional Linux support, consultancy, bug fixing, and training for additional fees.

User-Friendly

Linux is considered as most user friendly UNIX like operating systems. It makes it easy to install sound card, flash players, and other desktop goodies. However, Apple OS X is most popular UNIX operating system for desktop usage.

Security Firewall Software

Linux comes with open source netfilter/iptables based firewall tool to protect your server and desktop from the crackers and hackers. UNIX operating systems comes with its own firewall product (for example Solaris UNIX comes with ipfilter based firewall) or you need to purchase a 3rd party software such as Checkpoint UNIX firewall.

Backup and Recovery Software

UNIX and Linux comes with different set of tools for backing up data to tape and other backup media. However, both of them share some common tools such as tar, dump/restore, and cpio etc.

File Systems
Linux by default supports and use ext3 or ext4 file systems.
UNIX comes with various file systems such as jfs, gpfs (AIX), jfs, gpfs (HP-UX), jfs, gpfs (Solaris).
System Administration Tools
UNIX comes with its own tools such as SAM on HP-UX.
Suse Linux comes with Yast
Redhat Linux comes with its own gui tools called redhat-config-*.
However, editing text config file and typing commands are most popular options for sys admin work under UNIX and Linux.
System Startup Scripts
Almost every version of UNIX and Linux comes with system initialization script but they are located in different directories:
HP-UX - /sbin/init.d
AIX - /etc/rc.d/init.d
Linux - /etc/init.d

How is distributed file system implemented in Windows 2000.

In Windows NT 4.0, Microsoft provided an add-on product called Distributed File System (DFS) that allowed physically separate network file resources to be grouped together and accessed as if they were a single logical structure. The product, which was a free download, failed to make a great impact with network administrators and went largely unnoticed. With Windows 2000, DFS is included with the OS and provides a number of new functions. The tool for managing the DFS structure has been improved, and wizards serve to make setup an easy task.
DFS is a service that gives administrators a way to provide users with simple access to increasingly distributed amounts of data. In this article, I will look at some of the features of DFS and how to create a DFS tree in Windows 2000
DFS provides the ability to create a single logical directory tree from different areas of data. The data included in a DFS tree can be in any location accessible from the computer acting as the DFS root. In other words, the data can be on the same partition, disk, or server, or on a completely different server. As far as DFS is concerned, it makes no difference. A DFS tree appears as one contiguous directory structure, regardless of the logical or physical location of the data.
After the DFS root is created, links to directories can be added or removed to construct the single logical directory structure. The DFS tree can be navigated using standard file utilities such as Windows Explorer. Unless users are made aware of the fact that the data is being accessed from different locations, they will not realize that they are using a DFS system at all.

The purpose of VPN and name some VPN protocols supported by windows 2000.

VPN gives extremely secure connections between private networks linked through the Internet. It allows your remote computer(s) to act as though they were on the same secure, local (USU) network.
Allows you to be at home or anywhere Internet access is available and access the USU network and computer systems in the same way as if you were connected directly at USU.
Almost impossible for someone to tap or interfer with data in the VPN tunnel.

For secure VPNs, the technologies that VPNC supports are
IPsec with encryption
L2TP inside of IPsec
SSL with encryption
For trusted VPNs, the technologies that VPNC supports are:
MPLS with constrained distribution of routing information through BGP ("layer 3 VPNs")
Transport of layer 2 frames over MPLS ("layer 2 VPNs")
Question 4. i) Describe backup strategies for your system?

backup or the process of backing up refers to making copies of data so that these additional copies may be used to *restore* the original after a data loss event. The verb is *back up* in two words, whereas the noun is *backup* (often used like an adjective in compound nouns).[1]
Backups are useful primarily for two purposes. The first is to restore a state following a disaster (called disaster recovery). The second is to restore small numbers of files after they have been accidentally deleted or corrupted. Data loss is also very common. 66% of internet users have suffered from serious data loss.[2]
Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. Organizing this storage space and managing the backup process is a complicated undertaking. A data repository model can be used to provide structure to the storage. In the modern era of computing there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.
Before data is sent to its storage location, it is selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and de-duplication, among others. Many organizations and individuals try to have confidence that the process is working as expected and work to define measurements and validation techniques. It is also important to recognize the limitations and human factors involved in any backup scheme.

the features of Intrusion detection system?
An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.
IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection

systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat

List and describe the various security features in Windows 2000 OS?

Windows 2000 OS contain so many features some of features are:

1. Converting NTFS format
2. Disabling TCP/IP and IIS
3. Securing guest and administrator account
4. Creating a local security policy
5. Creating groups
6. Disable sharing