Date: 1
Page No.:

Course Code → MCS-022
Course Title → Operating system & Networking Management
Assignment Number → MCA(6)/022/Assignment/2019-20

Name → Mohd Sahil
Enroll. no. → 176485996
Programme → BCA
Study Center → TSL Institute 38016(P)

---

Ans1 Advanced Operating Systems

1. Architecture Operating Systems
   - → Network Operating systems
   - → Distributed Operating systems
   - → Multiprocessor Operating systems
2. Application Driven System
   - → Database Operating System
   - → Real-time Operating system
   - → Multimedia Operating system

Network Operating System → A network operating system is a specialized operating system for a network device such as a router, switch or firewall. Historically operating systems with ~~not~~ networking capabilities where described as network operating system. Because they allow to connect multiple PCs

translate the name into the corresponding IP address. For example, the domain name www.google.com

A domain name is divided into three part -

* Top Level Domain - A top-level domain recognizes a certain element regarding the associated website, such as its objective (business, government, education), its owner, or the geographical area from which it originated.

Generic Top Level Domains

| TDL | Description |
|---|---|
| .com | Commercial |
| .edu | Education |
| .gov | U.S. national and state government agencies |
| .int | International Organizations |
| .mil | U.S. military |
| .net | Network |
| .org | Organization |

Country-Code Top Level Domains

| TDL | Description |
|---|---|
| .in | India |
| .ru | Russia |
| .de | Germany |
| .au | Australia |
| .uk | United Kingdom |
| .cn | China |

etc.

Sponsored Top Level Domains

| TDL | Description |
|---|---|
| .aero | Members of the air-transport industry |
| .coop | Cooperative associations |
| .jobs | Human resource managers |
| .museum | Museums |
| .post | Postal services |
| .tel | For individuals and businesses to publish contact data |
| .travel | Travel agents, airlines, tourism bureaus, etc. |
| .mobi | Providers and consumers of mobile products and services |
| .cat | Catalan linguistic and cultural community |
| .xxx | Pornographic sites |

Infrastructure Top Level Domains - There is only one TLD in this category, which is ".arpa", used for the Internet Engineering Task Force.

* Second Level Domain - In the Domain Name System (DNS) hierarchy, a second-level domain (SLD or 2LD) is a domain that is directly below a top-level domain (TLD).

* Sub Domain - In the Domain Name System (DNS) hierarchy, a sub domain is a domain that is directly below a second-level domain (TLD).

iii) NFS Server ⇒ A network file system (NFS) is a byte type of file system mechanism that enables the storage and retrieval of data from multiple disks and directories across a shared network. It enables local users to access remote data and files in the same way they are accessed locally. NFS was initially developed by Sun Microsystems.

Ans 8. A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

A VPN extends a corporate network through encrypted connections made over the Internet. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Even smartphones and tablets can connect through a VPN.

## Types of VPNs

* Remote access - A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting. think of remote access as computer to network.
* Site-to-Site - A Site-to Site VPN connects the corporate office to branch offices over the Internet. Site-to-Site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to established and maintain a connection. Think of Site-to-Site access as network to network.

## Virtual Private Network Protocols

* PPTP - Point to Point Tunneling Protocol (PPTP) is one of the oldest protocol by Microsoft. It is the fastest of all VPN protocols. It is ideal for applications where speed is important such as streaming and gaming. But PPTP is not as secure because of its weak encryption. PPTP uses the TCP port 1723 for communication.

* L2TP/IPsec - L2TP over IPsec is more secure than PPTP and offers more features. L2TP/IPsec is a way of implementing two protocols together in order to gain the best features of each.

Ans 9. An Intrusion Detection System (IDS) is a type of security software designed to automatically alert administrators when someone or something is typing to compromise information system through malicious activities or through security policy violations. IDS basically classified into two types:

* Network Intrusion Detection System (NIDS) → Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.
* Host Intrusion Detection System (HIDS) → It run on independent hosts or devices on the network.

A HIDS monitors the incoming and outgoing packets from the devices only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or ~~deted~~ deleted, an alert is sent to the administrator to investigate.

Detection Method of IDS-

* Signature-based Method → Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.
Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

* Anomaly-based Method → Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and

anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Ans 10. A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private network connected to the internet, especially intranets. All messages entering or living the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificate and logins.

Firewall Filtering Techniques

Firewalls are used to protect both home and

A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

* Packet Filter - Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transport to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
* Application Gateway - Applies security mechanism to specific applications, such as FTP and Telnet services. This is very effective, but can impose a performance degradation.
* Circuit-level Gateway - Applies security mechanism when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
* Proxy Server - Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is

considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Limitations of Firewall:

* Firewalls cannot protect against what has been authorized
* It cannot stop attacks if the traffic does not pass through them
* They are only as effective as the rules they are configured to enforce.
* The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.
* The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

Ans 11. Fault-tolerance is the ability to survive of one or several disk failure. RAID is a technology that is used to increase the performance and/or reliability of data storage. RAID stands for

Redundant Array of Independent Disks. A RAID system consists of two or more drives working in parallel. There are different RAID levels, each optimized for a specific situation.

* RAID 0 - striping

In a RAID 0 system data are split up into blocks that get written across all the drives in the array. By using multiple disks (at least 2) at the same time, this offers superior I/O performance. This performance can be enhanced further by using multiple controllers, ideally one controller per disk.

* RAID 1 - mirroring

Data are stored twice by writing them to both the data drive (or set of data drives) and a mirror drive (or set of mirror drives). If a drive fails, the controller uses either the data drive or the mirror drive for data recovery and continues operation. You need at least 2 drives for a RAID 1 array.

* RAID 5 - striping with parity

RAID 5 is the most common secure RAID level. It requires at least 3 drives but can work with up to 16 drives. Data blocks are striped across the drives and on one drive a parity checksum of all the block data is written. The parity data are not

written to a fixed drive. They are spread across all drives. Using the parity data, the Computer can recalculate the data of one of the other data blocks, should those data no longer be available. That means a RAID 5 array can withstand a single drive failure without losing data or access to data.

* **RAID 6 - striping with double parity**

RAID 6 is like RAID 5, but the parity data are written to two drives. That means it requires at least 4 drives and can withstand 2 drives dying simultaneously. The chances that two drives break down at exactly the same moment are of course very small. However, if a drive in a RAID 5 systems dies and is replaced by a new drive, it takes hours ~~and~~ or even more than a day to rebuild the swapped drive. If another drive dies during that time, you still lose all of your data. With RAID 6, the RAID array will even survive that second failure.

* **RAID 10 - combining mirroring and striping**

It is possible to combine the advantages of RAID 0 and RAID 1 in one single system. This is a nested or hybrid RAID configuration. It provides security by mirroring all data on secondary drives while using striping across each set of drives to speed up data transfers.

Ans 12. Malicious software is any software that the user did not authorize to be loaded or software that collects data about a user without their permission.

Different Types of Malicious Software

Spyware - Spyware is any technology that aids in gathering information about a person or organization without their knowledge. They can monitor and log the activity performed on a target system, like log key strokes, or gather credit card and other information.

Virus - A computer virus is a piece of software that can 'infect' a computer, install itself and copy itself to other computers, without the users knowledge or permission. It usually attaches itself to other computer programs, data files, or the boot sector of a Hard drive.

Worm - Unlike a virus, a worm, is a standalone piece of malicious software that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security flaws on the target systems to allow access.

Trojan (Trojan Horse) - A type of malware that uses malicious code to install software that seems ok, but is hidden to create back door doors into a system typically causing loss or

theft of data from an external source.

**Adware** - Adware is software that can automatically causes pop-up and banner adverts to be displayed in order to generate revenue for its author $ or publisher. A lot of freeware will use Adware but not always in a malicious way, if it was malicious, it would then be classed as spyware or malware.

**Rootkit** - Rootkit virus assists a hacker in remotely accessing or controlling a computing device or network without being exposed. They are hard to detect due to the reason that they become active even before the system's OS is booted up.

Ans 13. Kerberos is a ticketing-based authentication system, based on the use of symmetric keys. Kerberos uses tickets to provide authentication to resources instead of passwords. This eliminates the threat of password stealing via network sniffing. One of the biggest benefits of Kerberos ~~environment~~, is its ability to provide single sign-on (SSO). Once you log into your Kerberos environment, you will be automatically logged into other applications in the environment.

To help provide a secure environment, Kerberos makes

use of mutual authentication. In Mutual Authentication, both the server and the client must be authenticated. The client knows that the server can be trusted, and the server knows that the client can be trusted. This authentication helps prevent man-in-the-middle attacks and spoofing. Kerberos is also time sensitive. The tickets in Kerberos environment must be renewed periodically or they will expire.

When a user needs to access a service protected by Kerberos, the Kerberos protocol process can be divided into two phases - User Identify Authentication and Service access.

User Identify Authentication - User authentication is a process of checking validity of identify information provided by users in the Kerberos authentication service. Identify information can be user names and passwords or information that can provide real identities in other forms. If user information passes the validity check, the Kerberos authentication service returns a valid Ticket-to-Granting Ticket (TGT) Token, proving that the user has passed identity authentication. The user uses the TGT in the subsequent Service Access process.

Service Access - When the user needs to access a service, the user requests the Ticket-Granting

Service (TGS) from the Kerberos server based on the TGT obtained in the first phase, providing the name of the service to be accessed. TGS checks the TGT and information about the service to be accessed. After the information passes the check, TGS returns a Service-Granting Ticket (SGT) token to the user.

## Kerberos in Windows Systems

Kerberos is very prevalent in the windows environment. In fact windows 2000 and later use Kerberos as the default method of authentication. When you install your Active Directory domain, the domain controller is also the key Distribution Center. In order to use Kerberos in a windows environment, your client system must be a part of the Windows domain. Kerberos is used when accessing file servers, web servers, and other network resources. When you attempt to access a web server, Windows will try to sign you in using Kerberos. If Kerberos authentication does not work, then the system will fall back to NTLM authentication.

Ans. 14. Exchanging sensitive information across a network, especially a public network, requires a security

method that will protect the data in transit. That is where Internet Protocol Security (IPSec) comes in. IPSec is a set of protocols that allows you to sign and encrypt data to be sent across an IP network, and authenticate and decrypt the protected packets on the receiving end. Windows 2000 Professional and Server include IPSec.

IPSec → IPSec is a set of protocols and cryptography based services that work together to protect data from unauthorised access or tampering when it is sent across an IP network. IPSec provides three basic services:

* **Authentication** - Confirmation of the origin of the IP packet; verification that the purported sender actually sent it.
* **Integrity** - "Signing" of the packet to ensure that the data has not been changed in any way between the time it left the sender and the time it was received at the authorized destination.
* **Confidentiality** - Encryption of the data to render is unreadable without the correct key.

**Implementation of IPSec in Windows 2000**

Windows 2000's implementation of IPSec provides a high level of security, using a combination of algorithms and keys to encrypt the data so

that it will be unreadable if intercepted along its route. IPSec uses two protocols to accomplish these tasks:

* Authentication Header (AH)- This protocol provides authentication services for IPSec. It allows the recipient of a message to verify the identity of the sender. It also allows the recipient to verify that intermediate devices haven't changed any of the data in the datagram. It also provides protection against so-called replay attacks, whereby a message is captured by an unauthorized user and resent.
* Encapsulating Security payload (ESP)- AH provides integrity authentication services to IPSec-capable devices so that they can verify that messages are received intact from other devices. For many applications, however, this is only one piece of the puzzle. We want to not only protect against intermediate devices changing the datagrams, but also to protect against them examining their contents as well. For this level of private communication, AH is not enough; we need to use the ESP protocol.

—x—

Course Code → MCS-022
Course Title → Operating Sys. Concepts & Networking Manggemt
Assignment Number → MCA(6)/022/Assignment/2019-20

Name → Rahul Kumar
Roll no → 176415413
Programme → BCA
Study Center → TSL Institute 38016(P)

Ans 1. a) Advanced Operating Systems

1. Architecture Operating Systems
   ⇒ Network Operative System
   ⇒ Distributed Operating System
   ⇒ Multiprocessor Operating System
2. Application Driven System
   ⇒ Database Operating System
   ⇒ Real-Time Operating System
   ⇒ Mutimedia Operating System

Network Operating System ⇒ A network operating system is a specialized operating system for a network device such as a router, switch or firewall. Historically operating systems with networking capabilities were described as network operating system, because they allowed personal computers (PCs) to participate in computer networks and shared file and printer

access within a local area network (LAN). Network operating systems can be embedded in a router or hardware firewall that operates the functions in the network layer (layer 3).

Some important Network OS are listed below :-

* Cisco IOS ⇒ Cisco Internetwork Operating System is a family of network operating systems used on many Cisco Systems routers and current Cisco network switches. Earlier, Cisco switches ran CatOS. IOS is a package of routing, switching, internetworking and telecommunications functions integrated into a multitasking operating system.
* Cisco NX-OS ⇒ NX-OS is a network operating system for the Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches made by Cisco Systems.
* AppleShare ⇒ AppleShare was a product from Apple Computer which implemented various network services. Its main purpose was to act as a file server, using the AFP protocol.

Real-Time Operating System ⇒ Real-time system means that the system is subjected to real time, i.e., response should be guaranteed within a specified timing constraint or system should

meet the specified deadline. For Example: missile systems, air traffic control systems, robots etc.
There are two types of Real-Time Operating System:-
* Hard Real-Time Systems ⇒ Hard Real-Time Systems are require for the applications where time constraints are very strict and even the shortest possible delay is not acceptable. These systems are built for saving life like automatic parachutes or air bags which are required to be readily available in case of any accident.
* Soft Real-Time Systems ⇒ Soft real-time systems are less restrictive. A critical real-time task gets priority over other tasks and retains the priority until it completes. Soft real-time systems have limited utility than hard real-time systems. For example, multimedia, virtual reality, Advanced Scientific Projects like undersea exploration and planetary rovers, etc.

Ans 1. b) Key characteristics of modern operating systems.
Multi-threading ⇒ Multithreading is the ability of a program or an operating system process to manage its use by more than one user at a time and to even manage multiple requests by the same user without

having to have multiple copies of the programming running in the computer. The process is divided into threads that can run simultaneously.

Symetric Multi-processing ⇒ In Symmetric Multi-processing system a computer has more than one processor. These processors can share the same memory, data path, I/O facilities and also the same job for execution.

Distributed Operating System ⇒ A Distributed Operating system is an operating system that runs on a network of computers. The operating system, memory files shared by the number of users in the network from the server. In a Distributed Operating System, each users thinks that running on a single large system with one operating system. The users don't need to know where the files in the network.

Micro-Kernel Architecture ⇒ Kernel is the core part of an operating system which manages system resources. It also acts like a bridge between application and hardware of the computer. It is one of the first programs loaded on start-up (after the Bootloader).

Object-Oriented Design ⇒ It is used for adding modular extensions to a small kernel. It also enables programmers to customize an operating system without disrupting system integrity.

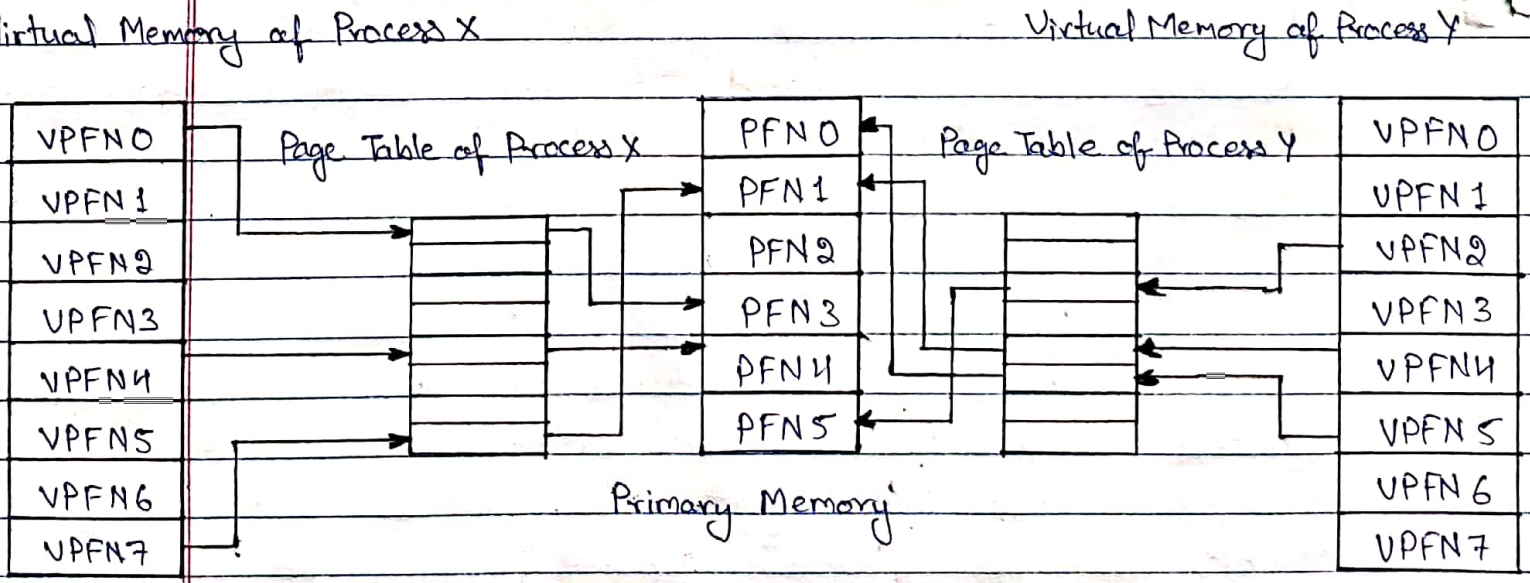
Ans 2. i) Hubs ⇒ If multiple incoming connections need to be connected with multiple outgoing connections, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. Hubs are multi-port repeaters, and as such they obey the same rules as repeaters. They operate at the OSI Model Physical Layer. Hubs are used to provide a physical Star Topology.

ii) Routers ⇒ In an environment consisting of several network segments with different protocols and architecture, a bridge may not be adequate for ensuring fast communication among all of the segments. A complex network needs to device which not only knows the address of each segment, but also can determine the best part for sending data and filtering broadcast traffic to the local segment. Such a device is called a Router. Routers are both hardware and software devices. Routers operates at the Network Layer of the OSI Model.

Ans 3. Your computers has two types of memory, Random Access Memory (RAM) and Virtual Memory. All programs use RAM, but when there isn't enough RAM for the program you're trying to run,

Windows temporarily moves information that would normally be stored in RAM to a file on your hard disk called a Paging File. The amount of information temporarily stored in a paging file is also referred to as virtual memory. Using virtual memory, in other words, moving information to and from the paging file, frees up enough RAM for programs to run correctly.

A virtual address does not represent the actual physical location of an object in memory; instead the system maintains a page table for each process, which is an internal data structured used to translate virtual addresses into their corresponding physical addresses. Each time a thread references an address the system translates the virtual address to a physical address.



In this model, both virtual and physical memory are divided up into handy sized chunks called pages. These pages are all the same size. Each of these pages is given a unique number; the page frame number (PFN). For every instruction in a program, for example to load a register with the contents of a location in memory, the CPU performs a mapping from a virtual address to a physical one. Also if the instruction itself references memory then a translation is performed for that reference. The address translation between virtual and physical memory is done by the CPU using page tables which contain all the information that the CPU needs. Typically there is a page table for every process in the system. Above figure shows a simple mapping between virtual addresses and physical addresses using page tables for Process x and Process y. Each entry in the theoretical page table contains the following information:

* The virtual PFN.
* The physical PFN that it maps to.
* Access control information for that page.

Ans 4. Important directories and files of Linux :-

/-Root :-

* Every single file and directory starts from the root directory

* Only root user has write privilege under this directory.
* Please note that / root is root user's home directory. which is not same as /.

## /bin - User Binaries

* Contains binary executables.
* Common linux commands you need to use in single-user modes are located under this directory.
* Commands used by all the users of the system are located here. For example: ls, ping, grep, cp, etc.

## /boot - Boot Loader Files

* Contains boot loader related files.
* Kernel initrd, vmlinux, grub files are located under /boot. For example: initrd.img-2.6.32-24-generic.

## /dev - Device Files

* Contain device files.
* These include terminal devices, usb, or any device attached to the system. For example: /dev/tty1.

## /etc - Configuration Files

* Contains configuration files required by all programs.
* This also contains startup and shutdown shell scripts used to start/stop individual programs. For example: /etc/resolv.conf.

/home - Home Directories

* Home directories for all users to store their personal files. For example: /home/debabrata.

/lib - System Libraries

* Contains library files that supports the binaries located under /bin and /sbin.
* Library filenames are either ld* or lib*.so.*. For example: ld-2.11.1.so, libncurses.so.5.7, etc.

/media - Removable Media Devices

* Temporary mount directory for removable devices. For examples: /media/cdrom for CD-ROM.

/mnt - Mount Directory

* Temporary mount directory where sysadmins can mount filesystems.

/opt - Optional add-on Applications

* opt stands for optional.
* Contains add-on applications from individual vendors.
* add-on applications should be installed under either /opt/ or /opt/sub-directory.

/proc

* Contains information about system process.
* This is a pseudo filesystem contains information about

running process. For example: /proc/$pid$ directory contains information about the process with that particular pid.
* This is a virtual filesystem with text information about system resources. For example: /proc/uptime.

/sbin - System Binaries
* Just like /bin, /sbin also contains binary executables.
* Linux commands located under this directory are used typically by system administrator. For example: reboot.

/srv - Service Data
* srv stands for service.
* Contains server specific services related data. For example: /srv/cvs contains cvs related data.

/temp - Temporary Files
* Directory that contains temporary files created by system and users.
* Files under this directory are deleted when system is rebooted.

/usr - User Programs
* Contains binaries, libraries, documentation, and sourcecode for second level programs.
* /usr/bin contains binary files for user programs. If you can't find a user binary under /bin, look under /usr/bin.

/var - Variable Files
* Content of the files that are expected to grow can be found under this directory.
* This includes - system log files (/var/log); packages and database files (/var/lib), emails (/var/mail), etc.

Ans 5. a) Consider that the "myfile.text" contains the following lines

Motherboard
Processor
RAM
Monitor
Hard Disk
DVD Writer
Graphic Card
RAM
Motherboard
Hard Disk
mohan play football

$ cat my file.text | head -7 | tail -5
Print the last 5 lines from the first 7 lines of the "myfile.text" file.
root@UBUNTU-PC:/MyDirectory # cat myfile.text | head -7 | tail -5
RAM
Monitor
Hard Disk

DVD Writer
Graphic Card
root@UBUNTU-PC:/My Director#

$ sort my file.text | unique.
Wrong Command
Right Command is:- sort myfile.text | uniq
First sort the file contents alphabetically, then remove the duplicate lines.
root@UBNTU-PC:/MyDirectory # sort myfile.text | uniq
DVD Writer
Graphic Card
Hard Disk
mohan play football
Moniter
Motherboard
Processor
RAM
root@UBUNTU-PC:/MyDrirectory #

$ cat my file.txt | grep "mohan" | wc-l
Count the number of lines present in the "myfiles.text" file which contains the particular pattern "mohan".
root@UBUNTU-PC:/MyDirectory # cat myfile.text | grep "mohan" | wc-1
root@UBUNTU-PC:/MyDirectory #