CHAPTER 2

NETWORK OPERATING SYSTEM ADMINISTRATION (CONFIGURATION AND MAINTENANCE)

2.1 Network Operating System (NOS)

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN). Artisoft's LANtastic, Banyan VINES, Novell's NetWare, and Microsoft's LAN Manager are examples of network operating systems. In addition, some multi-purpose operating systems, such as Windows Server RedHat Linux, Debian, Ubuntu Server etc are some example of Network Operating system. Installation and maintenance is the important when you have your own network.

2.1.1 Network Maintenance

Network maintenance basically means you have to do what it takes in order to keep a network up and running and it includes a number of tasks :

- Troubleshooting network problems.
- Hardware and software installation/configuration.
- Monitoring and improving network performance.
- Planning for future network growth.
- Creating network documentation and keeping it up-to-date.
- Ensuring compliance with company policies.
- Ensuring compliance with legal regulations.
- Securing the network against all kind of threats.

Of course this list could be different for each network you work on and perhaps you are only responsible for a number of these tasks. All these tasks can be performed in the following way :

1. **Structured tasks.**
2. **Interrupt-driven tasks.**

Structured means you have a pre-defined plan for network maintenance that will make sure that problems are solved before they occur. As a network engineer this will also make your life a whole lot easier.

Interrupt-driven means you just wait for trouble to occur and then fix it as fast as you can. Interrupt-driven is more like the "fireman" approach...you wait for trouble to happen and then you try to fix the problem as fast as you can. A structured approach where you have a network maintenance strategy and plan reduces downtime and it's more cost effective.

Of course you can never completely get rid of interrupt-driven tasks because sometimes things "just go wrong" but with a good plan we can reduce the number of interrupt-driven tasks for sure.

There are five major elements to the maintenance and management of a network. They include :

- **Fault management** : We will configure our network devices (routers, switches, firewalls, servers, etc.) to capture logging messages and send them to an external server. Whenever an interface goes down or the CPU goes above 80% we want to receive an e-mail so we can see what is going on.
- **Configuration management** : Any changes made to the network have to be logged. We will use a change management so relevant personnel will be notified of planned network changes. Changes to network devices have to be reported and acknowledged before they are implemented.
- **Accounting management** : We will charge (guest) users for usage of the wireless network so they'll pay for each 100MB of data or something. It's also commonly used to charge people for long distance VoIP calls.

- **Performance management** : Network performance will be monitored on all LAN and WAN links so we know when things go wrong. QoS (Quality of Service) will be configured on the appropriate interfaces.
- **Security management** : We will create a security policy and implement it by using firewalls, VPNs, intrusion prevention systems and use AAA (Authorization, Authentication and Accounting) servers to validate user credentials. Network breaches have to be logged and a appropriate response has to be made.

Whatever network maintenance model you decide to use, there are always a number of routine maintenance tasks that should have listed procedures, here are a couple of examples :

- **Configuration changes** : Business are never static but they change all the time. Sometimes you need to make changes to the network to allow access for guest users, normal users might move from one office to another so you'll have to make changes to the network to facilitate this.
- **Replacement of hardware** : Older hardware has to be replaced with more modern equipment and it's also possible that production hardware fails so we'll have to replace it immediately.
- **Backups** : If we want to recover from network problems such as failing switches or routers then we need to make sure we have recent backups of configurations. Normally you will use scheduled backups so you will save the running-configuration each day, week, month or whatever you like.
- **Software updates** : We need to keep our network devices and operating systems up-to-date. Bugs are fixed but also to make sure we don't have devices that are running older software that has security vulnerabilities.
- **Monitoring** : We need to collect and understand traffic statistics and bandwidth utilization so we can spot (future) network problems but also so we can plan for future network growth.

2.2 Network security and IT Career Opportunities

Network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.

Network security involves the authorization of access to data in a network, which is controlled by the network security administrator/ specialist.Security Specialist to implement and maintain our security systems.Security Specialist responsible for preventing unauthorized access to our data and responding to privacy breaches.Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. The responsibilities for network Security Specialist are as follows.

- Analyze IT specifications to assess security risks
- Design and implement safety measures and data recovery plans
- Install, configure and upgrade security software (e.g. antivirus programs)
- Secure networks through firewalls, password protection and other systems
- Inspect hardware for vulnerable points of access
- Monitor network activity to identify issues early and communicate them to IT teams
- Act on privacy breaches and malware threats
- Serve as a security expert and conduct trainings when needed
- Draft policies and guidelines

The various career opportunities for network specialist are as follows :

- Network Technician
- System Engineer
- System Architect
- Network engineer
- Network Architect
- Field Engineer
- Network security Manager
- Network Analyst

2.3 Windows NT

Windows NT is a 32 bit network computer operating system designed for users and businesses needing advanced capability. The first version was released in 1993 as Windows NT 3.1, which was produced for servers and workstations.Windows NT's technology is the base for the Microsoft successor operating system, Windows 2000. Windows NT ("New Technology") is actually two products: Microsoft NT Workstation and Microsoft NT Server. The Workstation is designed for users, especially business users, who need faster performance and a system a little more fail-safe than Windows 95 and Windows 98. The Server is designed for business machines that need to provide services for network-attached computers. The Server is required, together with an Internet server such as Microsoft's Internet Information Server (IIS), for a Windows system that plans to serve Web pages.

FEATURES OF WINDOWS NT

- Windows NT family introduced default file system NTFS which is capable of recovering from disk errors automatically, support large sized hard disk, provide security like permission and encryption.

- Windows NT supports preemptive multitasking feature so that all computer programs share operating system and hardware resources.
- Windows NT 4.0 Terminal Server Edition was designed to provide the feature to log on the system remotely.
- Window NT supports numerous network features.

Windows NT Workstation 4.0 system requirements

- Pentium based system
- 12MB memory (RAM); 16MB recommended
- 110MB available hard disk space
- CD-ROM drive or access to a CD-ROM over a network
- VGA or higher resolution display adapter
- Microsoft mouse or compatible pointing device

Advantages of Windows NT

The advantages of Windows NT are as follows :

- ❑ More pleasing to the eye
- ❑ Low system requirements
- ❑ Runs well on old machines if all patches are installed
- ❑ Faster to operate
- ❑ Easier to Install
- ❑ Security implemented on

Disadvantages of Windows NT

The disadvantages of Windows NT are as follows :

- ❑ More easy to catch viruses and malware
- ❑ Way unstable and crashes so often if you do not have patches installed

Difference between Linux and Windows :

The difference between linux and windows are as follows :

Sr.No.	Linux	Windows
1.	Linux is free and open source operating system	Windows is a commercial operating system whose source code is inaccessible.
2.	Linux is customizable and a user can modify the code and can change its the look and feel.	Windows is not customizable.
3.	No licensing is required to use linux software	Windows operating system is a proprietary/copyrighted software i.e., the user should have license touse this software.
4.	Linux is reliable software and can often run for months and years without needing to be rebooted.	Windows has improved reliability over the last version of Windows, it still cannot match the reliability of Linux.
5.	Linux provides high security	Windows continues to be the most vulnerable to viruses, malware, and other attacks and is less secure.
6.	Users can install an application without using internet support	Internet connection is needed to install an application in windows.
7.	In Linux, file names are case sensitive	Windows file name are case-insensitive.
8.	Linux, variants have improveddramatically in ease of use	Windows is user friendly and easy to use operating system.

2.4 Linux Firewall

Firewall is a network security system that filters and controls the traffic on a predetermined set of rules. This is an intermediary system between the device and the internet.A properly configure firewall can increase the security of computer. All network traffic among the affected networks is routed through the firewall.

There are two types of firewalls: software and hardware. Software firewalls tend to be cheap (or free) and easily available while hardware firewalls are more expensive. A software firewall is an application that is installed on a server which controls and restricts network access to the machine. It's generally setup on a specific server where other applications are located. Both Linux and Windows generally come with their own software firewall, while several other third-party options exist as well.

The five types of firewall are :

1. Packet filtering firewall
2. Circuit-level gateway
3. Stateful inspection firewall
4. Application-level gateway
5. Next-generation firewall (NGFW)

1. Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets, but rather they compare each packet received to a set of established criteria — such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers.

2. Circuit-level gateway

Circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate — whether the remote system is considered trusted.

3. Stateful inspection firewall

State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

4. Application-level gateway

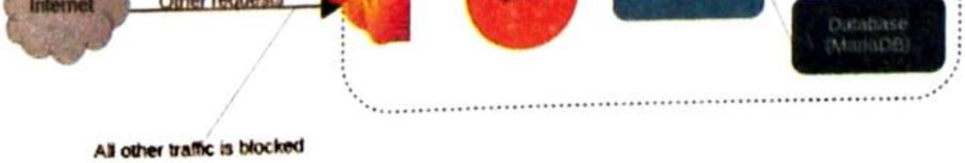
This kind of device - technically a proxy and sometimes referred to as a proxy firewall — combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended - as specified by the destination port - but also by certain other characteristics, such as the HTTP request string.

5. Next-generation firewall (NGFW)

A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection, as well as other network security systems, such as intrusion detection/prevention, malware filtering and antivirus.A deep packet inspection firewall tracks the progress of a web browsing session.

How the Firewall of Linux works :

Most of the Linux distro's ship with default firewall tools that can be used to configure them. We will be using "IPTables" the default tool provided in Linux to establish a firewall. Iptables is used to set up, maintain and inspect the tables of the IPv4 and IPv6 packet filter rules in the Linux Kernel.

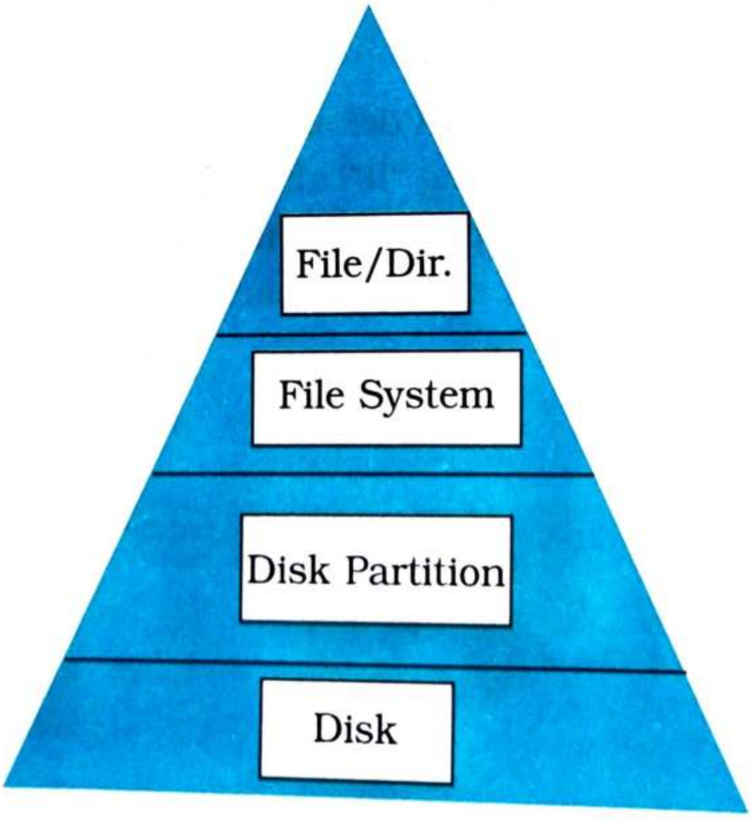

Only authenticated admins will be allowed SSH access
All HTTP users are allowed web site access
Firewall
SSH
File system
PHP
HTTP
Internet
Other requests
Apache
Application
Database (MariaDB)
All other traffic is blocked

A firewall can filter requests based on protocol or target-based rules.

2.5 Understanding Basic Disk Concept

All the data and information is stored in storage media this storage media can be a Hard disk (HDD), USB Disk (pen drive), CD, DVD etc. Big Storage media can be divided and each division is known as partition. We usually partition our Hard Disk. Partitioning is also required to be done during installation. We could have selected other options as well. Other options are used to manage the disk manually.

Disk partitioning or **disk slicing** is the creation of one or more regions on a hard disk or other secondary storage, so that an operating system can manage information in each region separately. Partitioning is typically the first step of preparing a newly manufactured disk, before any files or directories have been created. The disk stores the information about the partitions' locations and sizes in an area known as the partition table that the operating system reads before any other part of the disk. Each partition then appears in the operating system as a distinct "logical" disk that uses part of the actual disk. System administrators use a program called a partition editor to create, resize, delete, and manipulate the partitions.



Layers in a typical system

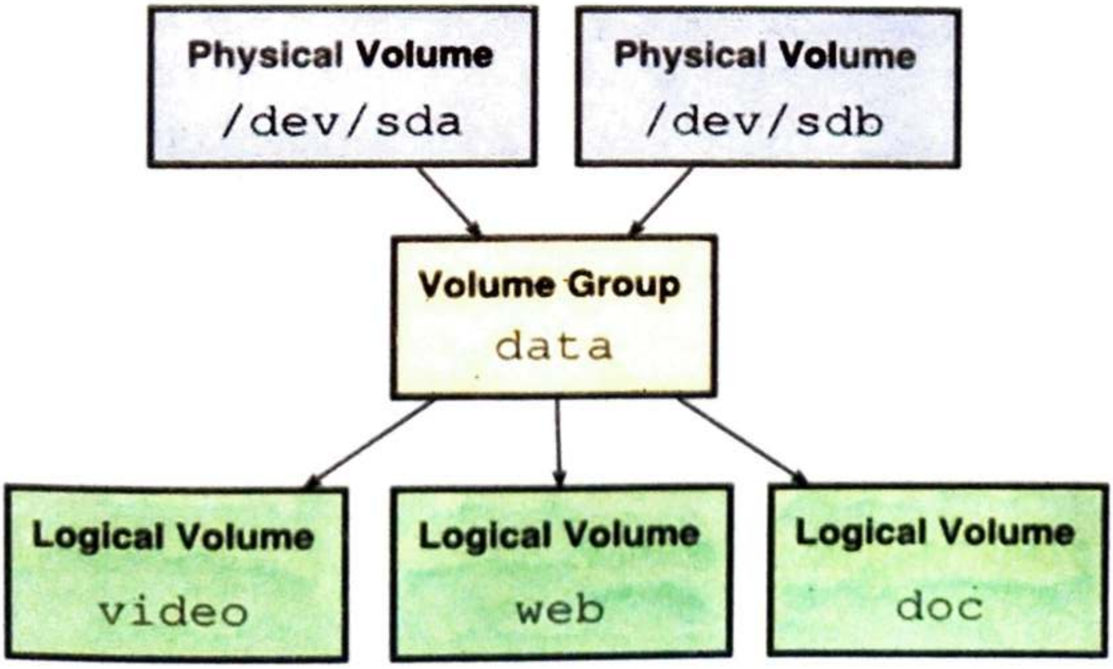
2.6 Logical Volume Manager (LVM)

LVM stands for *Logical Volume Management*. LVM, is a storage management solution that allows administrators to divide hard drive space into physical volumes (PV), which can then be combined into volume groups (VG), which are then divided into logical volumes (LV) on which the filesystem and mount point are created.

There are 3 concepts that LVM manages :

- Volume Groups
- Physical Volumes
- Logical Volumes

A *Volume Group* is a named collection of physical and logical volumes. Typical systems only need one *Volume Group* to contain all of the physical and logical volumes on the system, and I like to name mine after the name of the machine. *Physical Volumes* correspond to disks; they are block devices that provide the space to store logical volumes. Logical volumes correspond to partitions: they hold a file system. Unlike partitions though, logical volumes get names rather than numbers, they can span across multiple disks, and do not have to be physically contiguous.



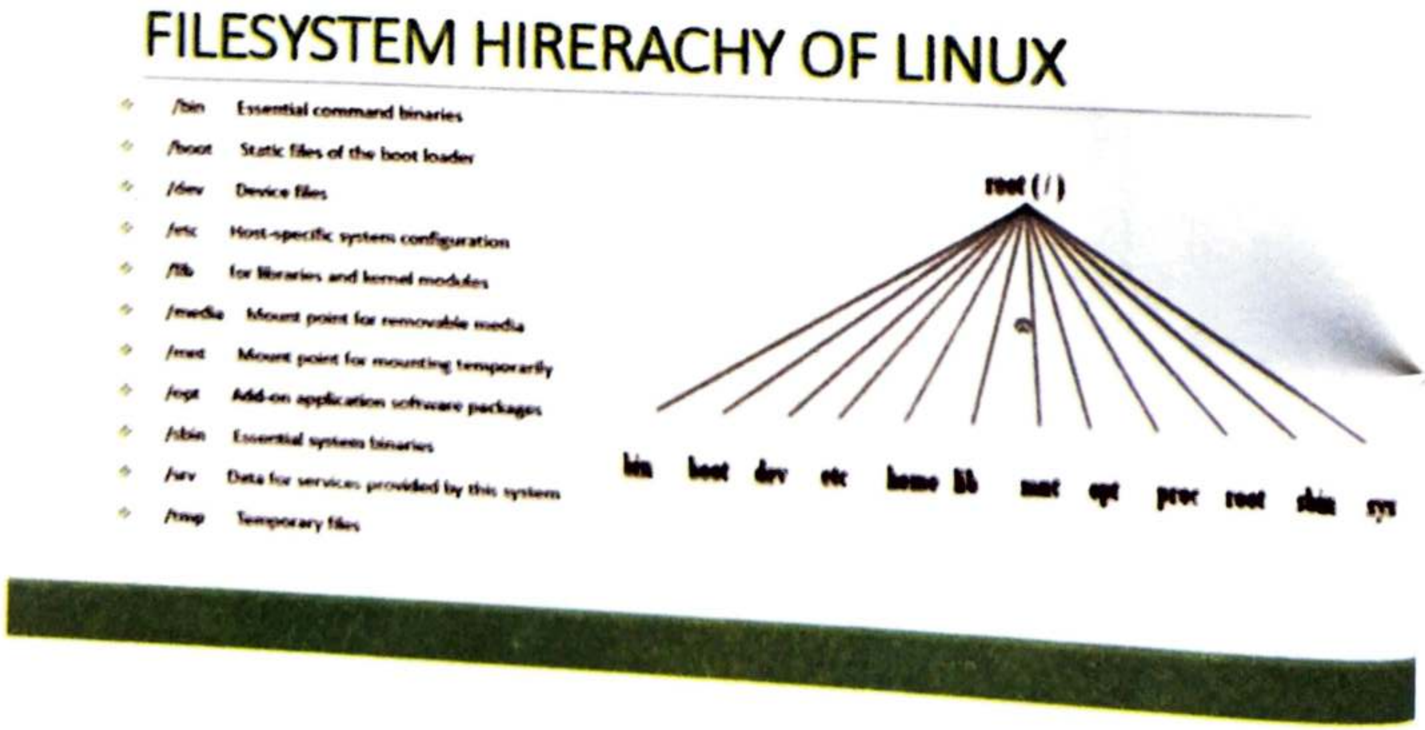
Logical Volume Management

2.7 File systems

The files on Linux are arranged in a tree-based hierarchy, with / (forward slash) denoting the root directory of the filesystem. Everything in Linux is a file - it can be a text-based regular file as well as a special device file (for example, /dev/dsp). These files can exist on different hard disk drives, external devices, and media. Hard disk drives (indicated as hda, sda) can have multiple partitions with different types of filesystem formats, such as ext, ext2, ext3, ext4, and so on. The filesystem controls how users and programs can access and manage the files. You need to use the mount command to attach each partition/device to the filesystem before accessing the partition/device.

The organization of your file system begins when you install Linux. Part of the installation process is to divide your hard disk (or disks) into partitions. Those partitions can then be assigned to:

- A part of the Linux file system,
- Swap space for Linux,
- Other file system types (perhaps containing other bootable operating systems)



FILESYSTEM HIRERACHY OF LINUX

- /bin Essential command binaries
- /boot Static files of the boot loader
- /dev Device files
- /etc Host-specific system configuration
- /lib for libraries and kernel modules
- /media Mount point for removable media
- /mnt Mount point for mounting temporarily
- /opt Add-on application software packages
- /sbin Essential system binaries
- /srv Data for services provided by this system
- /tmp Temporary files

Basic File Permissions

Permission Groups

Each file and directory has three user based permission groups :

- **owner** - The Owner permissions apply only the owner of the file or directory, they will not impact the actions of other users.
- **group** - The Group permissions apply only to the group that has been assigned to the file or directory, they will not effect the actions of other users.
- **all users** - The All Users permissions apply to all other users on the system, this is the permission group that you want to watch the most.

Permission Types

Each file or directory has three basic permission types:

- **read** - The Read permission refers to a user's capability to read the contents of the file.
- **write** - The Write permissions refer to a user's capability to write or modify a file or directory.
- **execute** - The Execute permission affects a user's capability to execute a file or view the contents of a directory.

Viewing the Permissions

You can view the permissions by checking the file or directory permissions in your favorite GUI File Manager (which I will not cover here) or by reviewing the output of the **\"ls -l\"** command while in the terminal and while working in the directory which contains the file or folder.

The permission in the command line is displayed as: **_rwxrwxrwx 1 owner:group**

1. **User rights/Permissions**
   1. The first character that I marked with an underscore is the special permission flag that can vary.
   2. The following set of three characters (rwx) is for the owner permissions.
   3. The second set of three characters (rwx) is for the Group permissions.

4. The third set of three characters (rwx) is for the All Users permissions.

2. Following that grouping since the integer/number displays the number of hardlinks to the file.

3. The last piece is the Owner and Group assignment formatted as Owner:Group.

Modifying the Permissions

When in the command line, the permissions are edited by using the command ***chmod***. You can assign the permissions explicitly or by using a binary reference as described below.

Explicitly Defining Permissions

To explicitly define permissions you will need to reference the Permission Group and Permission Types.

The Permission Groups used are:

- **u** - Owner
- **g** - Group
- **o** or **a** - All Users

The potential Assignment Operators are + (plus) and - (minus); these are used to tell the system whether to add or remove the specific permissions.

The Permission Types that are used are :

- **r** - Read
- **w** - Write
- **x** - Execute

So for an example, lets say I have a file named file1 that currently has the permissions set to**_rw_rw_rw,** which means that the owner, group and all users have read and write permission. Now we want to remove the read and write permissions from the all users group.

To make this modification you would invoke the command: ***chmod a-rw file1***

To add the permissions above you would invoke the command: **chmoda+rw file1**

As you can see, if you want to grant those permissions you would change the minus character to a plus to add those permissions.

Creating a Filesystem in Linux

You would want to create a filesystem in Linux for various reasons –

- keep your audio and video files, project file separately.
- hold your backup files separately.

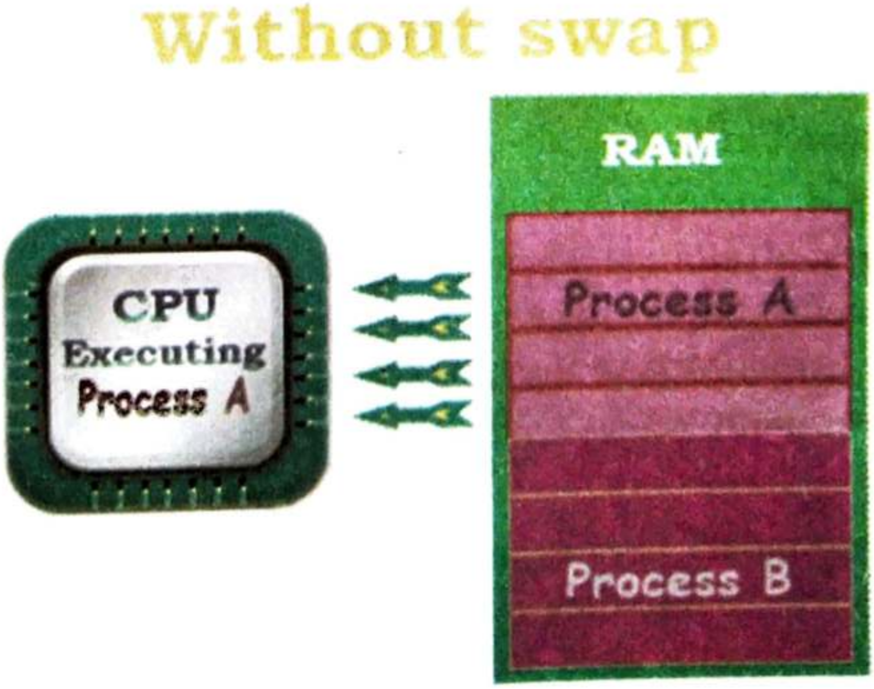
To create a filesystem, you need to create a partition and format it.

2.8 Swap Space

Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space. While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM. Swap space is located on hard drives, which have a slower access time than physical memory.

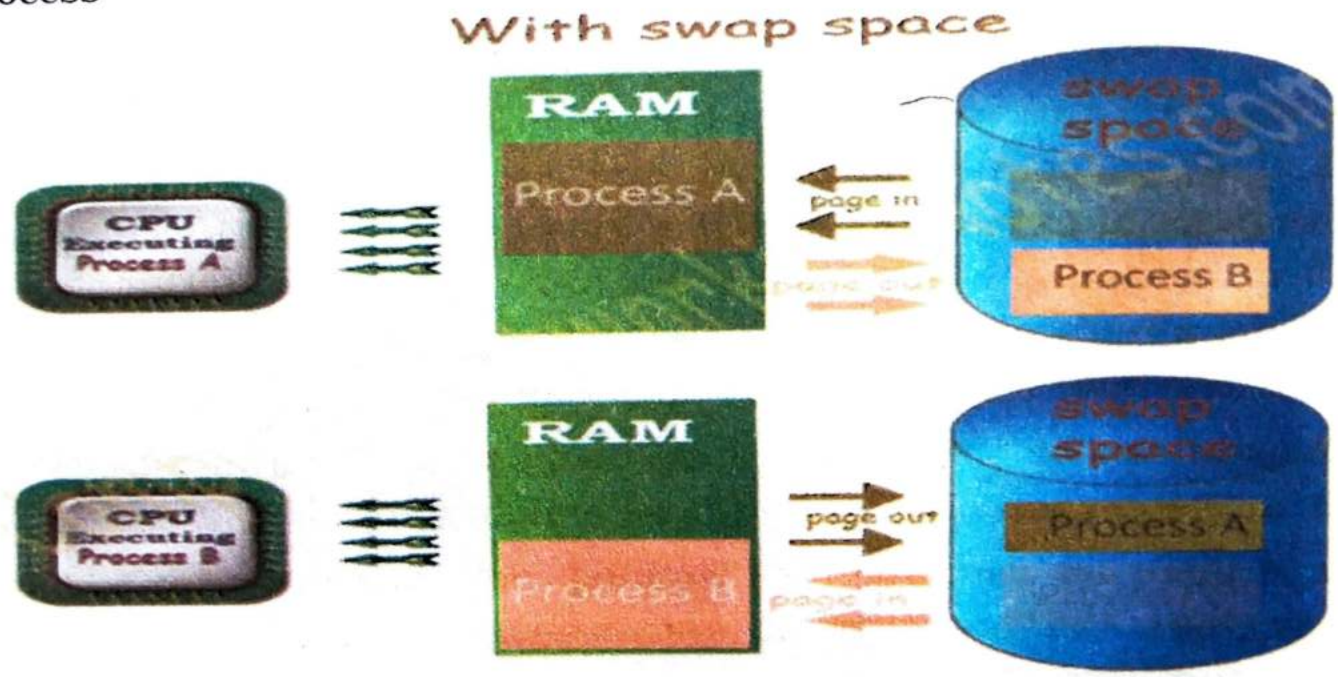
Swap space can be a dedicated swap partition (recommended), a swap file, or a combination of swap partitions and swap files.

Suppose there are two processes running. Both processes are assigned memory pages. CPU is processing process one. Following figure illustrates this scenario.



As we can see in above figure, no memory pages available for another process. System will not start new process until any existing process is finished. Swap space can improve this situation a little bit. If swap space is configured and RAM is filled, idle pages will be moved in swap space.

The process of moving idle memory pages from RAM to swap is known as **page out.** The process of moving required memory pages back from swap to RAM in known as **page in**.Following figure illustrates this process



2.9 Mount Point :

Mount is to access a filesystem in Linux. You can mount a filesystem on any directory and access content by entering to that directory. In Linux terms, these directories are called mount points.

The Linux mount command is used to mount USBs, DVDs, SD cards, and other types of storage devices on a computer running the Linux operating system. Linux uses a directory tree structure. Unless the storage device is mounted to the tree structure, the user can't open any of the files on the computer.

How to Use the Mount and Umount Commands in Linux

External storage media devices are usually mounted in subdirectories of the "/mnt" directory, but they can be mounted by default in any other directory created by the user. In this example, a CD has been inserted into the computer's CD drive. To see the files on the CD, open a terminal window in Linux and enter:

```
Mount/dec/cdrom/mnt/cdrom
```

This command connects the device **/dev/cdrom** (the CD ROM drive) to the directory **/mnt/cdrom** so you can access the files and directories on the CD ROM disk under the **/mnt/cdrom** directory, which is called the mount point. It must already exist when the command is executed. The mount point becomes the root directory of the device's file system.

To unmount the same CD ROM drive, enter this command:

```
umount/mnt/cdrom
```

After the unmount command is executed, the files and directories on the CD ROM are longer accessible from the directory tree of the Linux system.

This command has the same effect :

```
umount/mnt/cdrom
```

It unmounts the CD ROM.

2.10 Shell Scripting

If you are using any major operating system you are indirectly interacting to shell. If you are running Ubuntu, Linux Mint or any other Linux distribution, you are interacting to shell every time you use terminal. So before understanding shell scripting we have to get familiar with following terminologies –

- Kernel
- Shell
- Kernel

The kernel is a computer program that is the core of a computer's operating system, with complete control over everything in the system. It manages following resources of the Linux system –

- File management
- Process management
- I/O management

- Memory management
- Device management etc.
- Shell

A shell is special user program which provide an interface to user to use operating system services. Shell accept human readable commands from user and convert them into something which kernel can understand. It is a command language interpreter that execute commands read from input devices such as keyboards or from files. The shell gets started when the user logs in or start the terminal.

Shell Scripting

Usually shells are interactive that mean, they accept command as input from users and execute them. However some time we want to execute a bunch of commands routinely, so we have type in all commands each time in terminal.

As shell can also take commands as input from file we can write these commands in a file and can execute them in shell to avoid this repetitive work. These files are called **Shell Scripts** or **Shell Programs**. Shell scripts are similar to the batch file in MS-DOS. Each shell script is saved with **.sh** file extension eg. **myscript.sh**

A shell script have syntax just like any other programming language. If you have any prior experience with any programming language like Python, C/C++ etc. it would be very easy to get started with it.

A shell script comprises following elements –

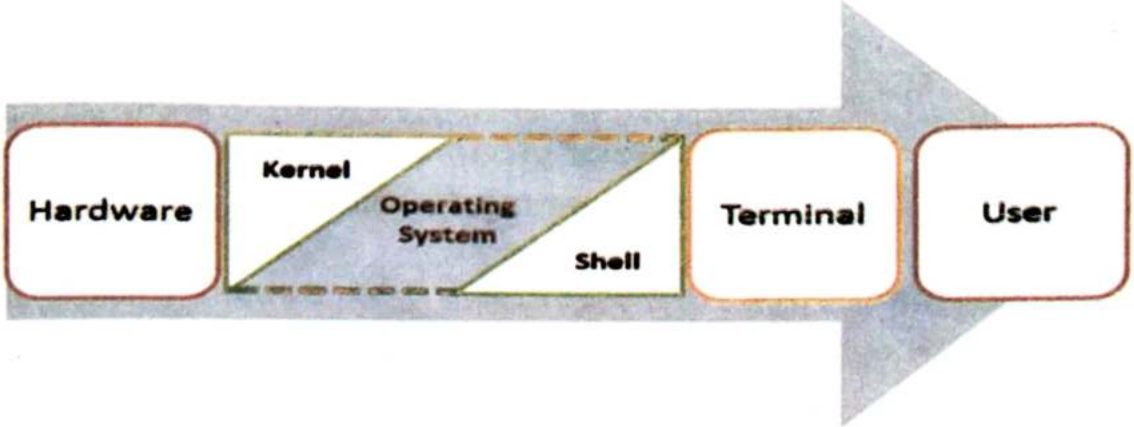
- Shell Keywords – if, else, break etc.
- Shell commands – cd, ls, echo, pwd, touch etc.
- Functions
- Control flow – if..then..else, case and shell loops etc.

Why do we need shell scripts

There are many reasons to write shell scripts –

- To avoid repetitive work and automation.
- System admins use shell scripting for routine backups.

- System monitoring.
- Adding new functionality to the shell etc.



Advantages of shell scripts

- The command and syntax are exactly the same as those directly entered in command line, so programmer do not need to switch to entirely different syntax
- Writing shell scripts are much quicker
- Quick start
- Interactive debugging etc.

Disadvantages of shell scripts

- Prone to costly errors, a single mistake can change the command which might be harmful
- Slow execution speed
- Design flaws within the language syntax or implementation
- Not well suited for large and complex task

2.11 Creating Groups Using The Command Line in Linux

As Linux is a multi-user operating system, there is a high need of an administrator, who can manage user accounts, their rights, and the overall system security.

In Linux, every user is assigned an individual account which contains all the files, information, and data of the user. You can create multiple users in a Linux operating system.

Managing users is done for the purpose of security by limiting access in certain specific ways. The superuser (root) has complete access to the operating system and its configuration; it is intended for administrative use only.

The steps to creating a user are :

For example, to create a new custom group called "Accounting" from the command line in Ubuntu, run the commands below.

```
sudogroupadd Accounting
```

Command To View All Groups

To view all groups currently created on your machine, run the commands below. A list of groups will show starting with the group name on the first column.

```
cat /etc/group
```

Adding Users To Groups

To add a user to a group called 'Accounting' run the commands below. It can also be used to add users to the sudo and admin groups and make them root or administrator.

```
sudousermod -a -G Accounting username
```

Removing Users From Groups

To remove a user from the Accounting group, run the commands below.

```
sudodeluser username Accounting
```

List Groups Users Belong To

To view the groups a user belongs to, run the commands below.

```
sudo groups username
```

Deleting Groups In Ubuntu

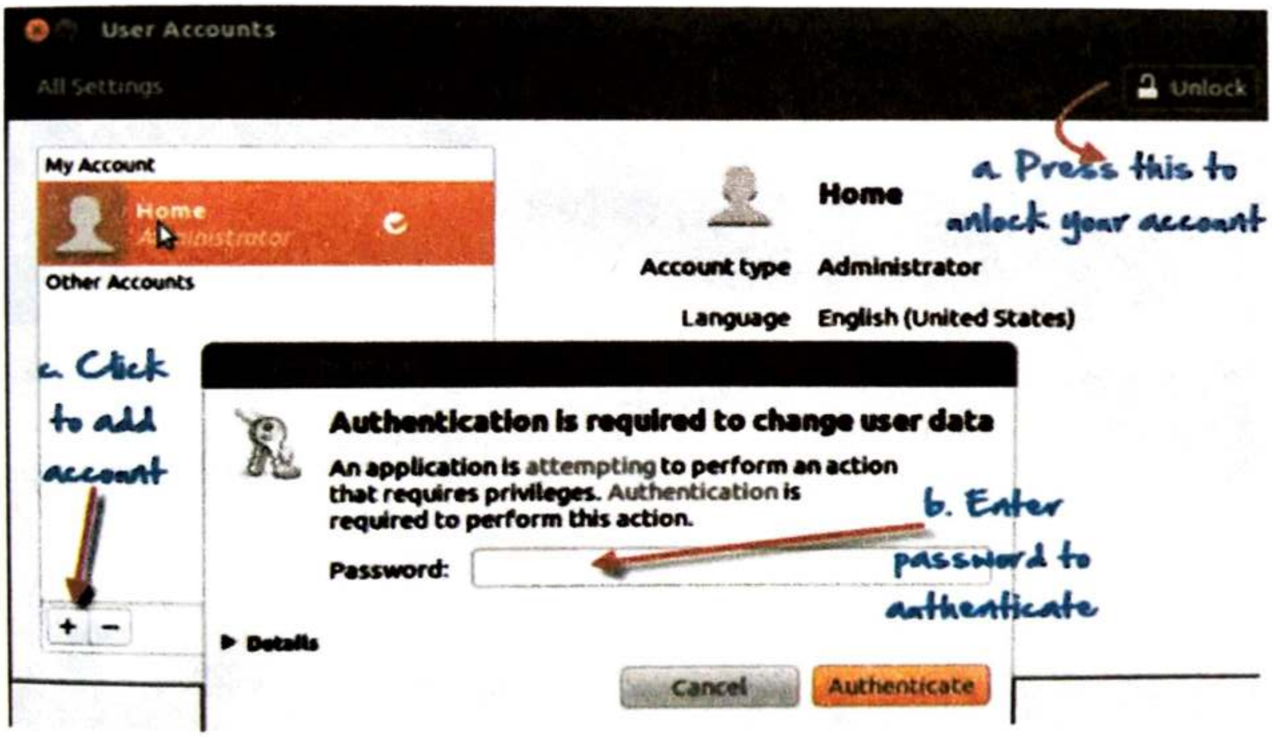
For example, to delete the Accounting Group, run the commands below

```
sudodelgroup Accounting
```

2.12 Administering Groups and users using GUI Tools

Step 1) Go to the system settings look for an icon which says 'User Accounts'.

Step 2) Click on the unlock icon and enter a password when prompted, then click the plus sign.



Home
Administrator

Account type Administrator

Language English (United States)

Authentication is required to change user data

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

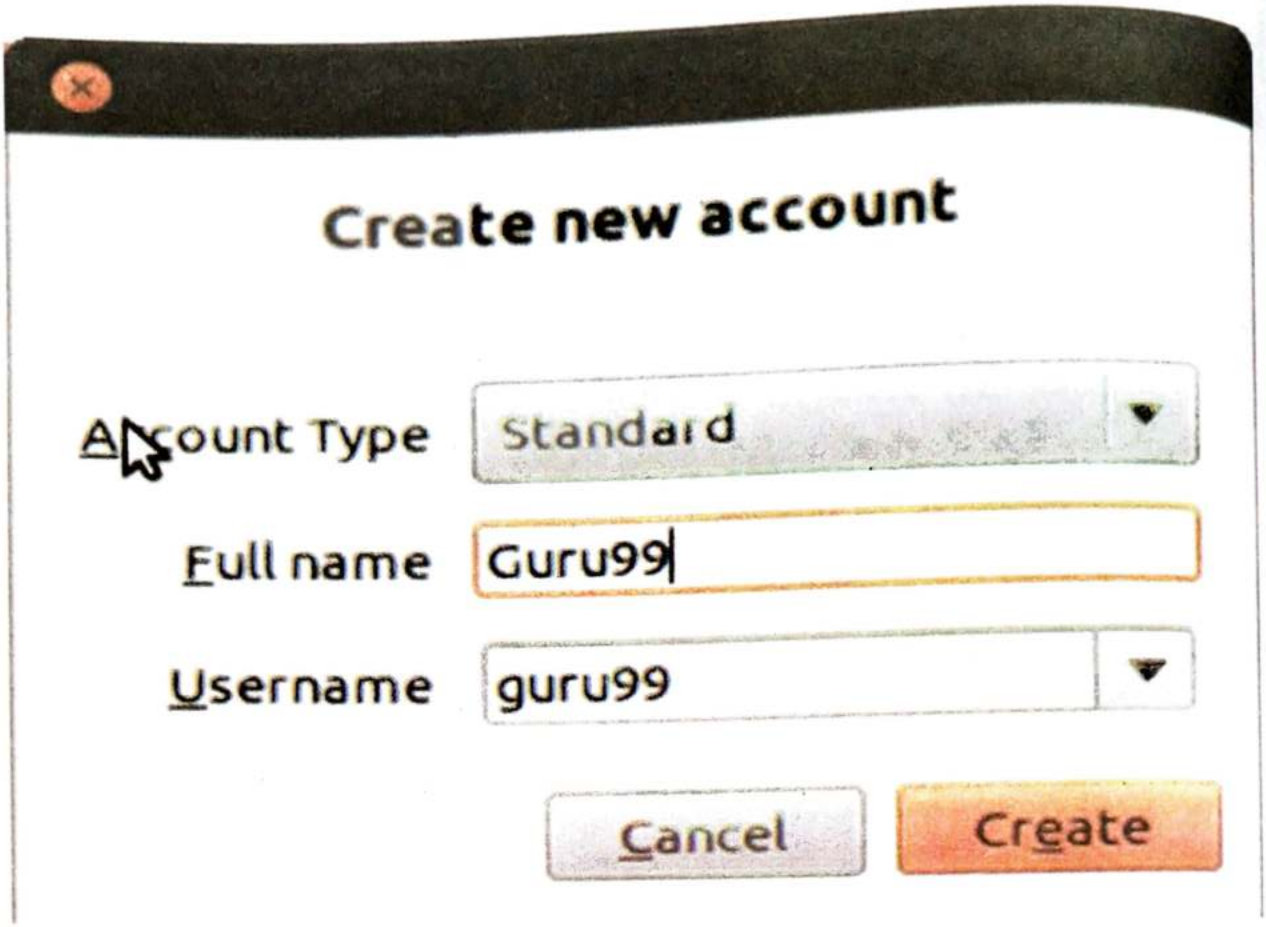
Password:

a. Press this to unlock your account

b. Enter password to authenticate

c. Click to add account

Step 3) A new window would pop up, asking you for adding information to the new user account.The account type offers two choices - standard and administration(Ubuntu Limitation). If you want the new user to have administrative access to the computer, select Administrator as the account type. Administrators can do things like add and delete users, install software and drivers, and change the date and time. Otherwise, choose standard.Fill in the full name, username and click on create.



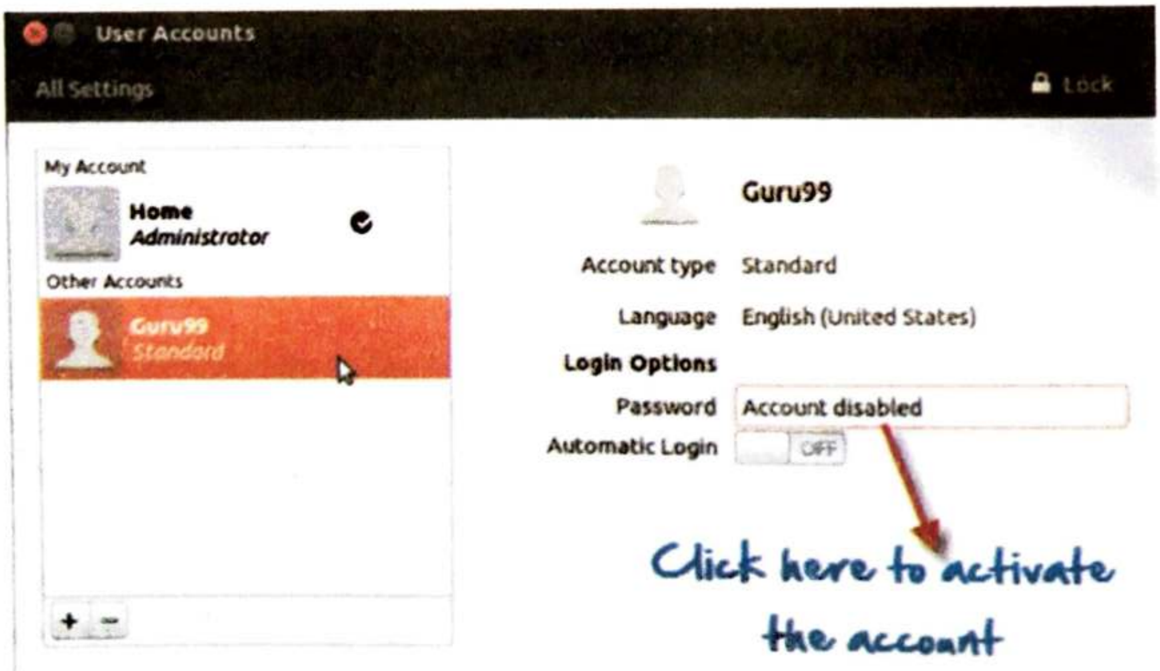
Create new account

Account Type: Standard

Full name: Guru99

Username: guru99

Step 4) The new account would show, but would **be disabled by default.**



User Accounts

Guru99

Account type: Standard

Language: English (United States)

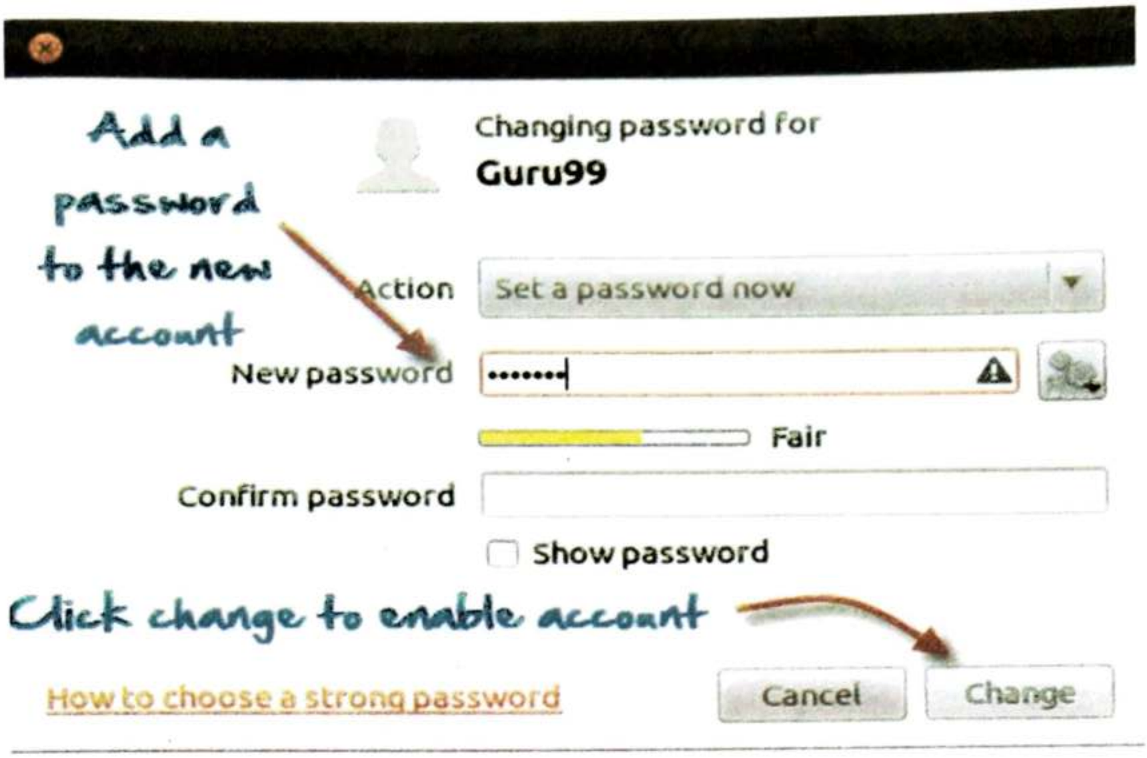
Login Options

Password: Account disabled

Automatic Login: OFF

Click here to activate the account

To activate it, click the password option and add a new password. Click change to enable the account.


Add a password to the new account

Changing password for
Guru99

Action: Set a password now

New password: •••••••

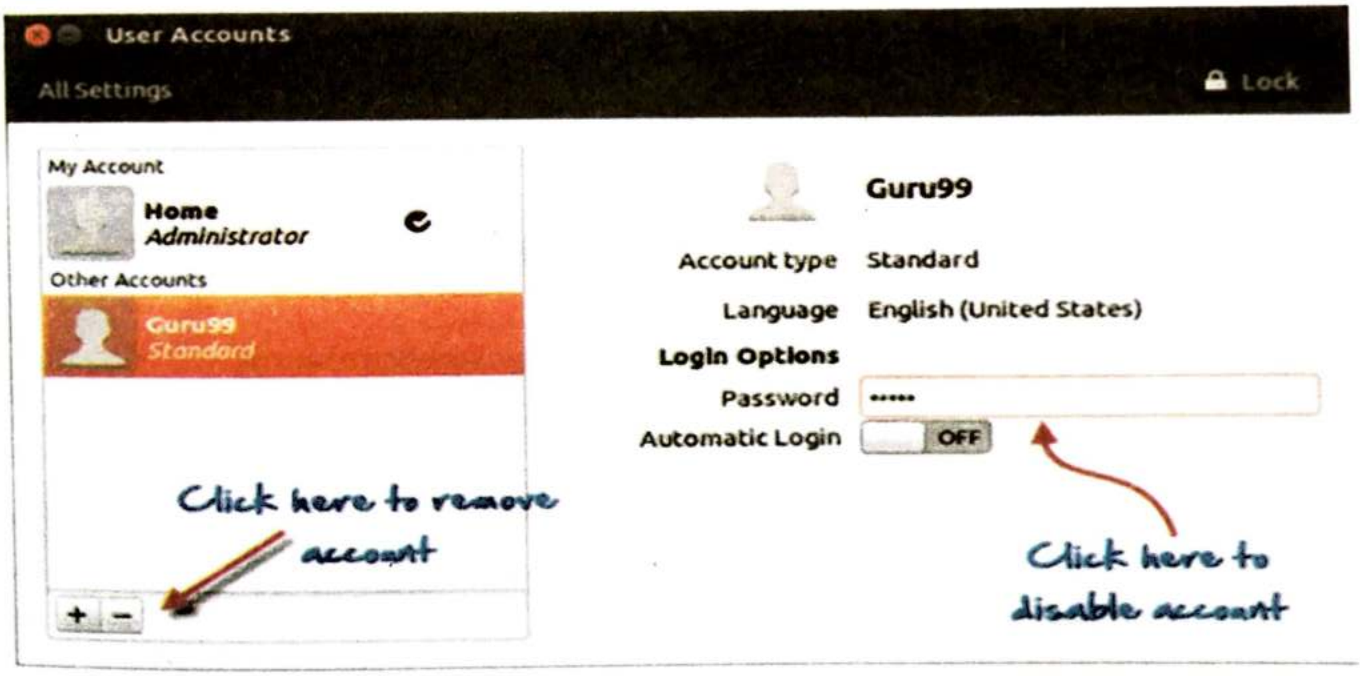
Fair

Confirm password:

□ Show password

Click change to enable account

Step 1) Highlight the user account and click the minus sign to delete.



Guru99

Account type: Standard

Language: English (United States)

Login Options

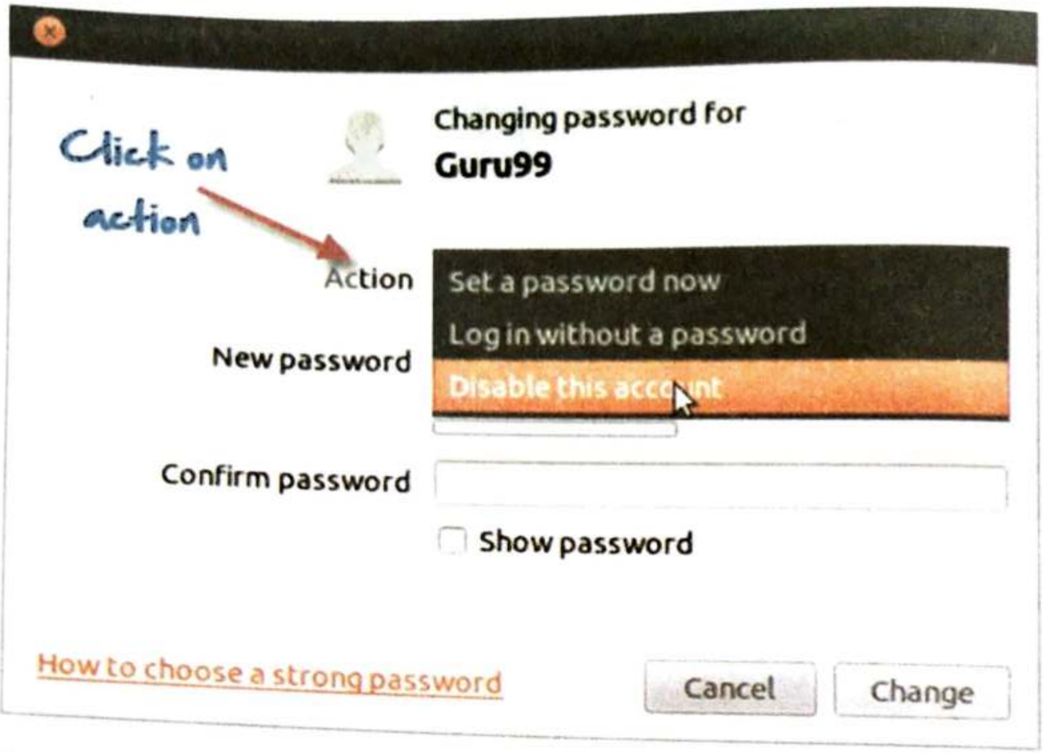
Password: •••••

Automatic Login: OFF

Click here to remove account

Click here to disable account

Step 2) For disabling click on the area where the password is stored, and you would get the following prompt. Select disable this account and click on change.



Adding Users To the User Groups

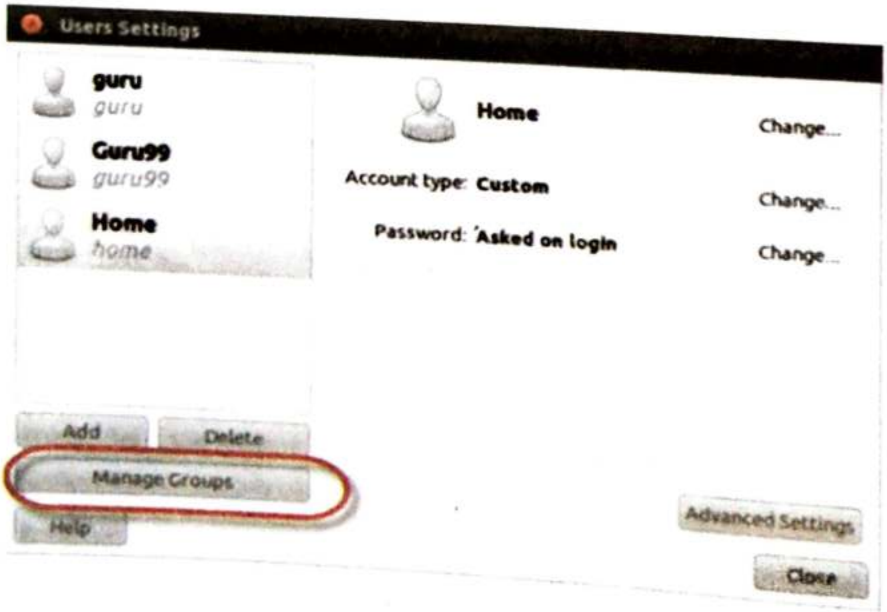
If you do not want to run the commands in terminal to manage users and groups, then you can install a GUI add-on .

```
sudo apt-get install gnome-system-tools
```

Once done, type

```
users-admin
```

Check user settings, and a tab Manage Groups will appear-



Account type: Custom

Password: Asked on login

Linux/Unix user management commands

Here is a list of linux user management commands

Command	Description
sudoadduser username	Adds a user
sudopasswd -l 'username'	Disable a user
sudouserdel -r 'username'	Delete a user
sudousermod -a -G GROUPNAME USERNAME	Add user a to a usergroup
sudodeluser USER GROUPNAME	Remove user from a user group
finger	Gives information on all logged in user
finger username	Gives information of a particular user

SUMMARY

Network Operating System (NOS)

A network operating system (NOS) is a computer operating system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN).

Network Maintenance

Network maintenance basically means you have to do what it takes in order to keep a network up and running and it includes a number of tasks:

Windows NT

Windows NT is a 32 bit network computer operating system designed for users and businesses needing advanced capability. Windows NT ("New Technology") is actually two products: Microsoft NT Workstation and Microsoft NT Server.

Linux Firewall

Firewall is a network security system that filters and controls the traffic on a predetermined set of rules. This is an intermediary system between the device and the internet. A properly configure firewall can increase the security of computer.

Disk partitioning or **disk slicing** is the creation of one or more regions on a hard disk or other secondary storage, so that an operating system can manage information in each region separately.

Logical Volume Manager (LVM)

LVM stands for *Logical Volume Management*. LVM, is a storage management solution that allows administrators to divide hard drive space into physical volumes (PV), which can then be combined into volume groups (VG), which are then divided into logical volumes (LV) on which the filesystem and mount point are created.

File Systems

The files on Linux are arranged in a tree-based hierarchy, with / (forward slash) denoting the root directory of the filesystem. Everything in Linux is a file - it can be a text-based regular file as well as a special device file (for example, /dev/dsp).

Swap Space

Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space.

Mount Point :

Mount is to access a filesystem in Linux. You can mount a filesystem on any directory and access content by entering to that directory.

Shell Scripting

Some time we want to execute a bunch of commands routinely, so we have type in all commands each time in terminal.

As shell can also take commands as input from file we can write these commands in a file and can execute them in shell to avoid this repetitive work.

TRUE/FALSE

Q.1 State whether the following statements are True or False :

1) Window NT is a network operating system.

2) Firewall did not prevent from unauthorized access.

3) The kernel cannot be updated.

4) The root user is allowed to access all files and programs in the system.

5) delgroup command is used to delete a group in linux.

6) Network security specialist do not protect company data.

7) Root users perform system administration work.

8) users enter commands directly to the kernel of the linux operating system.

9) Kernal is known as core of operating system.

10) The root of a directory structure is the topmost directory on the disk.

Answer : (1) True (2)False (3)False (4) True (5) True
(6) False (7) True (8) False (9) True (10) True

EXERCISE

Q.No.1 What do you understand by Network Maintenance ?

Q.No.2 What is Windows NT ? What are its advantages and disadvantages ?

Q.No.3 What are responsibilities of network security specialist ?

Q.No.4 What do you mean by linux firewall ? Explain its types.

Q.No.5 What is the difference between linux and windows ?Expalin.

Q.No.6 What do you mean by LVM ? Explain.

Q.No.7 What is a swap space ? Explain.

Q.No.8 What is mount point in linux ?

Q.No.9 What do you mean by shell scripting ? Explain.

Q.No.10 What do you understand by disk partition ?

—End—