

Q.11 How does open source becomes famous? write the advantages of Linux over other operating system.

→ Open source software is software with source code that anyone can inspect, modify and enhance. Open source software is generally a team effort where dedicated programmers improve upon the source code and share the changes within the community.

- 1) Open source software can be used freely without having to pay license fees to its developers. Contrasts with the commercial model of software distribution in which the source code remains the developer's closely guarded private property.
- 2) Availability of the source code means that you can modify and enhance software to more closely fit our own needs and there is no restriction on how the software is used and no invoices for each user licence.
- 3) With open source, users keep-up innovating, improving which means often much faster development cycle when compared to proprietary software.
- 4) In open source software, there are number of developers and supporters who collaborate and work on improving the software and meet the needs of its user. Vibrant local, national and global user groups collaborate in creativity, development and trouble shooting.
- 5) OSS relies on stable code bases developed and supported by many providers worldwide. As a result libraries using OSS have more support options than those using proprietary software.
- 6) As the codes of open source are publically available, developers of the community can easily figure out the vulnerabilities and address them in short period of time. Whereas proprietary software, with 'closed' source code, support and future development rely solely on the resource of the single vendor. If vendor goes down, so does your product support.

Hence with all these features base on innovating, sharing, collaborative community involvement, freedom and winning together, decentralized, customizable and faster development, Open source software has become famous:

## # Advantages of linux over other Operating system

### (a) full access vs no access

Having access to the source code is probably the single most significant difference between open source and other operating system. The fact that Linux belongs to the GNU public license ensures that users of all sorts can access (and alter) the code to the very kernel that serves as the foundation of the Linux OS. Whereas in other OS, unless you are a member of a very select group, you will never lay eyes on code making up the OS.

### (b) Licensing freedom vs licensing restrictions:

Along with access comes the difference between the license. I'm sure that every IT professional could go on and on about licensing of PC software. But let's just look at the key aspect of the license. With Linux GPL-licensed operating system, you are free to modify the software and use, and even republish or sell it (so long as you make the code available). Also with the GPL, you can download a single copy of a Linux distribution (or application) and install it on as many machines as you like. With the Microsoft license, you can do none of above. You are bound to the number of license you purchase, so if you purchase 10 license, you can legally install that operating system on only 10 machines.

(c) Online peer support vs paid help-desk support

→ This is one issue where most companies turn their backs on linux. But it's really not necessary. With linux, you have the support of huge community via forums, online search, and plenty of dedicated web sites. And of course if you feel the need, you can purchase support contracts from some of the bigger linux companies.

On the other side of the coin is support for windows. Yes, you can go the same route with microsoft and depend upon your peers for solutions. There are just as many help sites/lists/forums for windows as there are for linux. And you can purchase support from Microsoft itself. Most corporate higher-ups easily fall victim to the safety net that having a support contract brings. But most higher-ups haven't had to depend upon paid support contract. Of the various people I know who have used either a linux paid support contract or a Microsoft paid support contract, I can't say one was more pleased than the other. This of course begs the question "Why do so many say that Microsoft support is superior to linux paid support?"

(d) Centralized vs non centralized application installation.

→ The heading for this point might have thrown you for a loop. But let's think about this for a second. With linux you have a centralized location where you can search for, add or remove software. I'm talking about package management systems, such as Synaptic. With Synaptic, you can open up one tool, search for an application and install that application without having to do any web searching (or purchasing!).

Windows has nothing like this. With windows, you must know where to find the software you want to install, download software and run setup.exe or install.exe with simple double click. For many years, it was thought that installing application on windows was far easier than linux.

### e) Flexibility vs rigidity.

I always compare linux (especially the desktop) and windows to a room where the floor and ceiling are either movable or not. With linux, you have a room where the floor and ceiling can be raised or lowered, at will, as high or low as you want to make them. With windows that floor and ceiling are immovable. You can't go further than Microsoft has deemed it necessary to go.

Take, for instance, the desktop. Unless you are willing to pay for and install a third-party application that can alter the desktop appearance, with windows you can stuck with what microsoft has declared is the ideal desktop for you. With linux, you can pretty much make your desktop look and feel exactly how you want. You can have as much or as little on your desktop as you want. From simple flatbox to a full-blown 3D compiz experience, the linux desktop is as flexible an environment as there is on a computer.

N2. What do you understand by culture of free software? example & its advantage  
Ans. Free and open source software is released with licenses that allow it to be redistributed freely for others to use, copy, and/or modify within certain restrictions and conditions. Free culture refers to developing software and creative materials released with rights for reuse and/or redistribution that are more flexible than those of the traditional marketplace.

Software available freely with source code under GPL license to use, change, improve and redistribute it modified or unmodified. Open source software can be used freely without having to pay license fees to its developers. Contrast with the commercial model of software distribution in which the source code remains the developer's closely guarded private property.

The open source movement is a worldwide effort to promote an open style of software development more aligned with the accepted intellectual style of science than the proprietary models of invention that have been characteristic of modern business. Both open source software and open access to research represent innovative responses to the particular restrictions placed on the sharing and exchange of software code & research publications, respectively, imposed by current intellectual property economics.

Idea is to keep the software advance openly available for everyone to use, understand and improve as in 1960-70 engineers did. Based on innovating, sharing, collaborating, involvement, freedom and winning together.

## Advantages

- ① Ability to fit local need  $\Rightarrow$  availability of the source code mean that you can modify and enhance the software to more closely fit your own needs.
- ② No restrictions on use  $\Rightarrow$  no restrictions on how the software is used and no invoices for each user license.
- ③ low cost  $\Rightarrow$  no charge for the software itself. If other libraries share their efforts, each user's cost is reduced. Pay only for needed support or any additional product or services if required. Even then huge saving than commercial software.
- ④ Innovation  $\Rightarrow$  With open source code, users keep-up innovating, improving which means often much faster development cycle when compared to proprietary software.
- ⑤ collaboration  $\Rightarrow$  vibrant local, national, and global user group collaborate in creativity, development and trouble shooting
- ⑥ Transfer of technical know-how  $\Rightarrow$  Being active member and part of oss community, your licence term members will learn the minimum required know-how of software and technologies in use.
- ⑦ Security  $\Rightarrow$  Proprietary software, with 'closed' source code, support and future development rely solely on the resource of a single vendor. If the vendor goes down, so does your product support?

1.3. What is linux operating system? How does it different from other os.

→ linux is open source operating system or linux OS is a freely distributed cross-platform operating system based on unix that can be used on the computer. linux is the free OS that was developed by linus Torvalds when he was a student at the university of Helsinki in 1991. Torvalds started linux by writing kernel of an OS partly from scratch and partly from publically available software. It is open source operating system that is, the source code for the software is freely available, and anyone can work on it, change it or enhance it.

### linux operating system

(1) linux is free and open source Os.

(2) linux is customizable and a user can modify the code.

(3) linux provide the higher security than other os.

(4) linux can be booted from either primary or logical partition.

(5) directory are separated using forward slash.

(6) file names are case sensitive.

(7) linux uses the monolithic kernel which consumes more running space.

(8) linux is complex for those who having

no programming background.

### other operating system

(1) commercial os's source is inaccessible.

(2) other os is not customizable as linux.

(3) commercial os has less security than linux os.

(4) windows must boot from the primary partitions.

(5) directory are separated using back slash.

(6) file names are case insensitive.

(7) It uses the micro kernel which takes less space but system running efficiency is lower than linux.

(8) windows is simpler to user.

O.N.Q. What is shell? How does the kernel contrast with shell? Explain with figure

↗ Shell is a unix term for the interactive user interface with an OS.

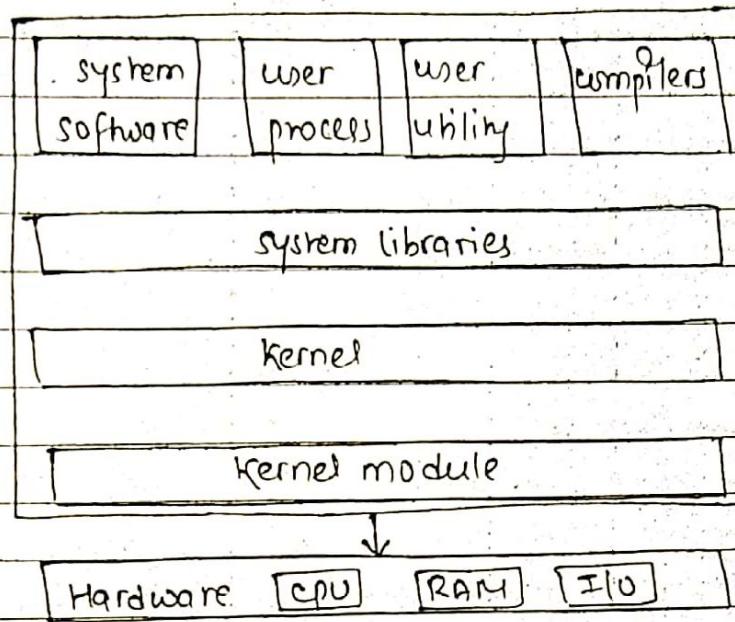
The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called command syntax.

↗ The kernel is the essential center of a computer operating system the core that provides basic services for all other parts of the OS. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in unix operating system than in IBM or microsoft OS. A shell usually implies an interface with command syntax.

Kernel

shell

- |  |   |
|--|---|
| (1) A computer program which acts as the core of the computer's system (OS) and has the control over everything in the system. | (1) A computer program which works as the interface to access the services provided by the operating system |
| (2) Core of the system that controls all the tasks of the system.  | (2) Interface between the kernel and user.  |
| (3) Doesn't have type;   | (3) Type: Bourne shell, Ksh, csh, cshell etc  |
| (4) responsible for task, disk & memory management   | (4) layer of programming that understand and executes the commands a user enters.                           |
| (5) It is lower level program interfacing with hardware on the top of which application are running                            | (5) The shell is a command line interpreter. (CLI)  |



[ Fig: linux operating system ]

**QNS** What is shell script? Explain different types of shell in linux.

→ A shell script is a text file that contains a sequence of command for a UNIX based operating system. A commands in the shell script can contain parameters and subcommands that tell shell what to do.

#### (a) The Bourne shell

→ The Bourne shell (sh), written by Steve Bourne at AT&T Bell labs is the original unix shell. It is the preferred shell for shell program because of its compactness and speed. Its drawbacks is that it lacks feature for interactive use and also logical expression handling.

command full path name is (/bin/sh and /sbin/sh)

#### (b) C shell (csh)

→ It was written by Bill Joy at Berkeley University Incorporated features for interactive use, such as aliases and command history. Includes convenient programming features, such as built-in arithmetic and a c-like expression syntax. full path name is /bin/csh.

#### (c) The Korn shell (ksh)

→ It was written by David Korn at AT and T Bell labs. It supports everything in the Bourne shell. It also has interactive features comparable to those in the C shell. Includes convenient programming feature like built-in arithmetic and c-like arrays, functions and strings manipulation facilities. Is faster than C shell. Runs script written for the Bourne shell. full path name is bin/ksh.

#### (d) The Bourne Again shell

→ 'bash' is compatible to Bourne shell. Incorporates useful features from the Korn and C shells. Has arrow key that automatically mapped for command recall and editing. Command full-path name is /bin/bash.

Q. What are the main required while installing linux? Write with their purpose:

→ Main required while installing linux os are as follows:

- (1) Insert the bootable cd/dvd and configure BIOS restart
- (2) Hit enter to install GUI mode and [linux next] command in GUI mode.

(3) choose the language and select ok

(4) choose keyboard type and select ok.

(5) select the monitor configuration.

(6) choose the installation method (either install or upgrade)

(7) skip the installation number:

(8) choose your partitioning strategy:

    (a) automatic partition:

    (b) Manual partition with disk drived

(9) choose partitioning:

    (a) remove all linux partitions on this system

    (b) Remove all partitions on this system

    (c) keep all partitions and use existing free space.

(10) choose the new option

    (a) mount point : /boot (about 50 MB)

    (b) file system type: ext3.

    (c) size : 512 MB and press ok.

(11) choose new option:

    (a) mount point

    (b) file system type: SWAP

    (c) size (MB) : 2 \* size of RAM

    (d) press ok.

(12) choose new option

    (a) mount point : /

    (b) file system type : ext3

    (c) size : remaining free space size. press ok.

- 13) Choose boot loader configuration, select GRUB boot loader & ok .
- 14) choose Master boot loader
- 15) configure the networking
- 16) choose the time zone
- 17) Enter root username & password
- 18) In package selection window select the packages such as web server, software development etc. and press ok.
- 19) After that press ok in the installation to begin process.

Q Data  
Page 2  
1.7. What is general partitioning scheme while installing linux OS and what do you prefer or recommend?

→ General partitioning scheme is the creation of one or more regions on a hardware or other secondary storage, so that an operating system can manage information in each region separately. These regions are called partitions.

→ partitions are really handy because they act as a sandbox. If you have a 1TB harddrive partitioned into a 250 GB partition and 250GB partition, what you have on the later will not affect the other and viceversa. A common configuration for Linux desktop system is to use two partition. One holding a file system mounted on root "/" and swap partition.

→ There are only three kinds of partitions: primary, extended and logical. Any given harddisk can only have a maximum of four primary partitions. This limitation is due to Master Boot Record (MBR) which tells the computer which partitions it can boot from, so primary partitions are usually reserved for OS.

→ preference of partition scheme is dependent on the strategy.

(A) Choose your partitioning :- we have two choices related to how your disk is partitioned for Red Hat Linux

(a) automatic partition → with this selection, all Linux partitions on all hard disks are erased and used for the installation. The installation process automatically handles the partitioning

(b) Manually partitioning with disk druid → with this selection, the disk druid utility is run to let you partition your harddisk.

④ Choose partitioning : If you selected to have the installer automatically partition for us, we can choose from the following options:

- (A) Remove all linux partition on this system
- (B) Remove all partition on the system
- (C) Keep all partition and use existing free space

→ If you have multiple hard disk, you can select which of those disks should be used for your Red HAT linux installation. Turn the review check box on to see how linux is choosing to partition your hard disk. Click next to continue.

After reviewing the partitions screen, you can change any of the partitions you choose. providing you have at least one root ( / ) partition that can hold the entire installation and one swap partition. A small 1gb partition (about 100mb) is recommended. The swap partition usually double size of RAM on your computer (for ex. 128 MB RAM you could use 256 MB of swap) Having less than doubled your physical memory for swap can cause performance problems:

P. Write the function of following command with example:

→

chmod 777 → The chmod command is used to change file permission mode, where 'chmod 777' means making file readable, writeable and executable by everyone for eg. \$chmod 777 sample.txt

touch BCA8 → The touch command can be used to modify the access modification timestamps of files. It is more often used to actually just create an empty file quickly. Touch BCA8 will create blank file named BCA8.

fdisk → It is used to create hard disk partition. Harddisk is divided into one or more logical disks called partition. For eg:

↳ to list all existing disk partitioning ⇒ fdisk -l

↳ to view all partitions of specific hard disk ⇒ fdisk -l /dev/sda

ps tree → It is used to display a tree of processes. The tree is rooted at either pid or init. If username is specified, all process trees are rooted owned by that user are shown.

passwd ⇒ It is used to change user password.

Eg. to change your own password ⇒ \$ passwd -

↳ change password for specified username

⇒ ~~username~~ \$ sudo passwd username.

top. → It is used to display linux tasks and list processes running on the system.

### ⑨ sudo

→ execute a command as another user. sudo determines who is an authorized user by consulting the file /etc/sudoers. for eg.

↳ to get a listing of an unreadable directory.

\$ sudo ls /usr/local/protected.

### ⑩ ls

→ list directory content. ls list information about the files (the current directory by default). Eg \$ls

↳ to display all info about file → \$ls -l

(↳ to display hidden file → \$ls -a)

### ⑪ grep

→ search files for lines that match a given pattern. Eg. To search for given string in a single file test.sh.

\$ cat test.sh

#!/bin/bash

fun()

echo "this is a test"

# terminate our shell script with success message exit.

fun()

from above file grep exit

\$ grep "exit" demo-file

output

exit)

① rpm (red hat package manager)

→ It is used to handle redhat linux installation process or other packages.

② cat

→ concatenate and print the content of files

Eg. \$ cat sample1.txt sample1.txt > sample2.txt  
\$ cat sample2.txt

→ This is a sample text file

Q.N.9. Write the role of following command with example:

(a) gpasswd  $\Rightarrow$  It is used to administer the /etc/group file. System administrator can use -A option to define group admin and -M option to define members.  
Eg. \$ gpasswd -A bca managers.

(b) useradd  $\Rightarrow$  create a new user or update default new user information  
Eg. # useradd bca2

(c) groupmod  $\Rightarrow$  modify the group definition on the system. The group command modify the definition of the specified group by modifying the appropriate entry in the group database.  
Eg. # groupmod -n oldgroup newgroup.

(d) userdel  $\Rightarrow$  delete a user account and related files. The userdel command modifies the system account file, detecting all entries that refers to login-name. The named user must exist. Eg. # userdel many.

(e) usermod  $\Rightarrow$  modify a user account. The usermod command modifies the system account files to reflect the changes that are specified on the command file.

(f) groupadd  $\Rightarrow$  industry standard method of adding new group

(10) Define and explain vi text editor. What do you know about linux file hierarchy system and the important directories?

→ Vi-editor is the very powerful application which is installed in almost every linux and unix platform. Linux by default install the improved version of vi text editors known as vim editor. It is a text editor which is used in editing all text document. It basically operates on the command mode. To type in the document we need to move from command mode to insert mode. To switch from command mode to insert mode 'I' key is pressed. After typing in the insert mode, we need to save the document. It is done by pressing esc (escape key) which brings back the text editor from insert mode to command mode and then pressing :wq and then enter key.

# To switch from command mode to insert mode certain key are used

a → start typing after the current character

A → start typing at the end of the current line

i → start typing before the current character

I → start typing at start of the current line.

o → start typing on a new line after the current line.

O → start typing on a new line before the current line.

Note: Instead of 'I' key, other keys as mentioned above can be used to switch from command mode to insert mode.

# To save and exit vi

:w → save (write)

:w fname → save as fname

:q → quit

:wq → save and quit

:Z → save and quit

:q! → quit (discarding your changes)

:w! → save (and write to non-writable file)



Date \_\_\_\_\_  
Page \_\_\_\_\_

linux file hierarchy system is the structure in which all the information on your computer is stored. files are organized within a hierarchy of directories. Each directory can contain files, as well as other directories, which is represented by a forward slash (/). Everything in your system can be found under this root directory even your system can be found under different virtual or physical devices.

Some of important file directory are:

- /bin → contain common linux user commands, such as ls, sort, date and chmod.
- /boot → Has the bootable linux kernel and boot loader configuration file (GRUB)
- /dev → Contain files representing access points to devices on your sys These include terminal devices (pty\*), floppy disk (fd\*), hard disk (hd\*), RAM (ram\*) and CD-ROM (cd\*). Users normally access these devices directly through the device files.
- /etc → contain administrative configuration file.
- /home → Contains directories assigned to each user with a login account.
- /mnt → Provides a location for mounting devices, such as remote file systems and removable media (with directory name of cdrom for floppy and so on)
- /root → represent the root user's home directory.
- /sbin → contains administrative commands and daemon processes.
- /tmp → contains temporary file used by applications.
- /usr → contain user documentation, games, graphical file (x11), libraries (lib) and a variety of other user and administrative common and file.
- /var → contains directories of data used by various application.

11. What are the main responsibility of system administrator in linux system different between root login and normal user login.

⇒ main responsibility of system administration are:

(a) Installing the server system

(b) Configuration updating, operating and maintaining the system hardware as well as software;

(c) Managing the failures in system;

(d) Managing disk space as well as backup;

(e) accountable for changing the content of file.

(f) Reset new passwords and security constantly monitors the security of the server.

(g) Monitoring CPU usages and system performance.

(h) accountable for configuration of module.

⇒ root login is the username or account that by default has access to all commands and files. It is also referred to as the root account, root user and the super user.

⇒ The su command is used to switch to another user, in other words change user ID during a normal login session. If executed without a username for example su-1, it will login as root user by default.

⇒ Super user or root in linux is a user who has all the rights and permissions including the administrative right to the system. More often than not the root is the superuser on the linux system. Because of this it is usually advisable not to use root as the everyday user.

Q.N.12. What is grub?

- GRUB stands for Grand Unified Bootloader is the bootloader package that supports multiple operating systems on a computer. During bootup the user can select the operating system to run. GRUB can run from any device, including harddrives, floppy disk, DVD, CD-ROM and USB drives.
- The GRUB is bootable bootloader available from the GNU project. A bootloader is very important as it is impossible to start an operating system without it. It is the first program which starts when the program is switched on. The bootloader transfer the control to the operating system kernel.

GRUB feature:

- ↳ GRUB support LBA (logical block addressing) mode which puts the addressing conversion used to find files into the firmware of the hardware drive.
- ↳ GRUB provide maximum flexibility in loading OS which requires options using a command based, pre-operating system environment.
- ↳ The booting option such as kernel parameters can be modified using the GRUB command line.
- ↳ There is no need to specify the physical location of linux kernel for GRUB. It only required the hard disk number, the partition number and file name of the kernel.
- ↳ GRUB can boot almost any operating system using the direct or chain loading boot methods.

GRUB functions:

- ↳ GRUB loads the default kernel image as specified in GRUB configuration file.
- ↳ GRUB configuration file is /boot/grub/grub.conf (let's grub.conf)
- ↳ GRUB just loads and executes kernel and initrd images.



13 What do you mean by system start up script? write the function of these scripts.

During system start-up, a series of scripts are run to the start the services that we need. These include scripts to start network interfaces, mount directories and monitor our system.

A runlevel is a software configuration of the system which allows only a selected group of processes to exist. When the linux system is booting up, you might see various services getting started. For example: "it might starting sendmail... ok" Those are the run level programs executed from the run level directory as defined by your run level.

Most of the startup scripts are run from subdirectories of /etc/rc.d. The program that starts most of these services up when you boot and stops them when you shut down is the /etc/rc.d/rc script.

The /etc/rc.d/rc. script is a script that is integral to the concept of run levels. Any change of run level causes the script to be executed with the new run level as an argument. The /etc/rc.d/rc script performs following tasks:

- (a) checks that run level scripts are correct
- ↳ The rc script checks to find each run level script that exists and excludes those that represent backup scripts left by rpm updates
- (b) Determine current and previous run levels:
  - ↳ Determines the current and previous run level to know which run level script to stop (previous level) and start (current level)
- (c) Decides whether to enter interactive startup.
- ↳ If the confirm option is passed to the boot loader at boot time, all services must be confirmed at the system console before starting.

(d) kill and start run-level scripts.

→ stop runlevel scripts from the previous level, then starts runlevel script from the current level.

The scripts (letcrlc.d | rc) are actually symbolic links to system service scripts under the /etc/rc.d/init.d directory, so /etc/rc.d is linked to /etc/rc.d/rc0.d. Under the /etc/rc.d/rc directories, you would see programs that start with s and k. Program start with s are used during startup and k are used during shutdown. There are sequence number associated with s and k in which programs should be started or killed.

Example:

- ↳ k12 mysql
- ↳ s12 syslog
- ↳ s10 network
- ↳ s80 sendmail.erc

14. show the process how linux system supports the user and user login account in computer.

#### → creating a technical support mailbox

Email is a wonderful communication tools, especially for overworked system administrator. Through email, an important details can be cut and pasted from other sources.

linux supports mailbox for technical and personal issues which has advantages like:

- support mail message will not be confused with personal, non-support related messages
- Multiple people can check mailbox without needing to read each other's personal email.

Suppose you wish to create a support alias that redirects message to the user accounts. for support staff members. you should login as root, edit the /etc/aliases file and add lines:

```
# technical support mailing list  
support: Joe, Mary, bob
```

After saving the file, you need to run the new aliases command to recompile the /etc/aliases file into a database format.

#### → Resetting a user's password

Red Hat Linux stores password in an encrypted format one common problem that users will encounter is the inability to login because they have the capslock key on, they have forgotten the password or the password has expired.

If you must reset a user's password, do so with the `passwd` command while logged in as root, type `passwd` followed by the login name you are resetting. You are prompted to enter the password twice for example to change the password for mary type:

```
# passwd mary.
```

After resetting the password, set it to expire so that the user is forced to change it the next time she logs in. You can use the `chage` command to set an expiration period for the password and to trick the system into thinking that the password is long overdue to be changed.

```
# chage -M 30 -d 0 mary
```

The `-M 30` option tells the system to expire mary's password every 30 days:

U.15 Write default configuration in /boot/grub/grub.conf file.

- ⇒ The configuration file which is used to execute the in GRUB's menu. Interface of operating system to boot essentially allows the user to select a package group of commands to execute.

The GRUB's menu interface configuration file is /boot/grub/grub.conf. The command to set the global performance for the menu interface are passed at the top of the program followed by stanzas for each operating kernel in the menu.

GRUB allows a number of useful commands in the command line interface:

↳ boot - Boots the operating system or chain loader that was last loaded

↳ chainloader </path/to/file> ; loads the specified file as a chain loader that was last loaded.

↳ display mem → displays the current use of memory, based on information from BIOS.

↳ initrd → enables users to specify and initial each disk to use when loading booting.

The etc/default/grub file is short and should be easy to edit.

Choose the default os:

⇒ change the GRUB\_DEFAULT = line. By default, GRUB\_DEFAULT = 0 uses the first entry as default change the number to 1 to use the second entry. 2 to use the third entry, or so on. You should also use GRUB\_DEFAULT = saved and GRUB would automatically boot the last os. you chose each time you boot.

for ex. If you had an operating system named windows7 (loader) in your os list you would use GRUB\_DEFAULT = "windows7 (loader)"

Q.N 16 What is backup? How can you make system backup in linux explain. (F)

→ Backup refers to the process of making copy of data or datatype file to use in the event the original data or data file are lost or destroyed. There are several ways of system backup:

(a) Full backup:

→ A full backup is one that stores every file on a particular disk or partition. If that disk should ever crash, you can rebuild your system by restoring the entire backup to a new disk.

(b) Incremental backup:

→ An incremental backup is one that contains only those files that have been added or modified since the last time a more complete backup was made.

(c) Disk mirroring

→ It is usually common for the system to continuously update the duplicate drive with the most current information. In fact, with a type of mirror called RAID, the duplicate drive is written to at the same time as the original.

(d) Network backup

→ You can share a single backup drive with many computers on a network. A web server may store a duplicate copy of its data on another server. If the first server crashes, a simple TCP/IP host name change can redirect the web traffic to the second server.

(e) Getting and installing mirrordir to clone directories:

→ The mirrordir package is a way of doing hard-drive mirroring. Mirror is a powerful tool that enables you to make and maintain an exact copy of a hierarchy of directory.

1. rpm -Uvh mirrordir.rpm

## (F) closing a directory with mirrordir

→ You have a second hard drive with a partition large enough to hold a copy of your /home directory. Your first step is to create a directory to mount the partition on and then mount it. Log in as root and type the following:

```
# mkdir -p /mirror/home
```

```
# mount /dev/hdb5 /mirror/home.
```

## (G) Restoring backup file:

→ The restore command is used to retrieve the file from a backup tape or other medium that was created by dump. You can use restore to recover an entire file system or to interactively select individual files:

O.N.17. What are the different techniques for maintaining security in Linux?

As operating system, Linux puts the user's privacy and safety above all. The following points covers a range of security measures to protect your Linux.

(1) Add users and passwords

→ Creating separate user accounts with a good password is your first line of defense in keeping your data secure.

(2) Read, write and execute permissions.

→ Every item in a Linux file system can be restricted by read, write and execute permission for that item's owner and group as well as by all others.

(3) Protect root:

→ The root user has special abilities to use and change your Linux system. Protect the root account's password and don't use the root account when you don't need it.

(4) Get software updated

→ As vulnerabilities and bugs are discovered in software packages, every Linux distribution offers tools for getting and installing those updates, especially if you are using Linux on a server.

(5) Use restrictive firewall

→ A primary job of a firewall is to accept requests for services from a network that you want and turn away that you don't. A server system should allow requests for a controlled set of ports.

(f) enable only services you need.

→ Don't enable service you don't need. In fact you shouldn't even install server software you don't need.

(g) limit access to services

→ You can restrict access for a service you want to have on to a particular host computer, domain or network interface. Service may limit access in their own configuration file using TCP/IP wrappers.

(h) check your system

→ After you install Linux, you can check access to its port using major watch network traffic using Wireshark or Nessus to get a more complete view of your system security.

Q418. What do you mean by run level? Explain different levels.

Ans: Run level is a software configuration of the system which allows only a selected group of processes to exist. Depending on your default init level setting, the system will execute the programs from one of the following directories:

\* Run level 0

halt (etcrc.d|rc0.d), shut down the system

\* Run level 1

single user mode (etcrc.d|rc1.d), mode for administrative task.

\* Run level 2 (etcrc.d|rc2.d)

multiuser mode without NFS, doesn't configure network interface

\* Run level 3 (etcrc.d|rc3.d)

full multiuser mode start the system normally.

\* Run level 4

unused, for special purposes.

\* Run level 5

multi-user mode, with ~~Xorg~~ display manager as well as console logins

\* Run level 6

reboot the system.

Q. 19 What is kudzu, How can you configure module in linux system.

→ Kudzu is a hardware probing program which relies on a library of hardware device information when the computer boots. Kudzu detects change in the running system's hardware configuration, if any and activates the newly detected hardware.

→ When you add or remove hardware from your computer and reboot Red Hat Linux, a window appears during the reboot process advising that hardware has either been added or removed and asking if you want to reconfigure it. The program that detect and reconfigure your hardware is called kudzu.

The kudzu program is a hardware auto detection and configuration tools that runs automatically at boot time. If you like, you can also start kudzu while Redhatlinux is running. In either case, here is what kudzu does:

- ① It checks the hardware connected to your computer
- ② It compare the hardware it finds to the database of hardware information stored in the /etc/sysconfig/hwconfig file.
- ③ It prompt you to change your system configuration, based on new or removed hardware that was detected.

→ There are few command that allow you to manipulate the kernel. Each is quickly described below, for more information say man [command]

- depmod → handle dependency descriptions for loadable kernel module
- insmod → install loadable kernel module
- lsmod → list loaded module
- modinfo → display information about a kernel module
- modprobe → high level handling of loadable modules
- rmmod → unload loadable module

QN21 How can you set an default as "Ramesh" username, comment as "pokhara university" default shell as bash.

# set a user default

First, create a n user

# user add Ramesh

To view the user default

# user add -D

Go to /etc/default and open file

useradd with vi editors

Now create default home directory and default bash

# useradd -d /home' -s /bin/bash

At last for mentioning comment

# useradd -c "pokhara university" Ramesh.

N-22. What is web server? what are the file and steps required to configure to use machine as web server?

A web server is a system that delivers content or services to end users over the internet. A web server consists of a physical server, server operating system and software used to facilitate HTTP communication.

The webserver usually has a simpler job to accept HTTP request and send a response to the client. To configure your web server in any computer you need to follow following steps:

(1) make sure that apache is installed by typing the following form a terminal window.

```
$ rpm -qal | grep httpd
```

(2) A valid host name is recommended for your apache server. If you don't have any then edit the `/etc/httpd/conf/httpd.conf` file and define `servername` as your computer's IP address.

(3) Open the `httpd.conf` file in any text editor, search your IP address (for example `servername 10.0.0.1`)

(4) Add an administrative email address. In the `/etc/httpd/conf/httpd.conf` file the default administrative address would be.

`serverAdmin root@localhost`

change `root@localhost` to the email address of your apache administrator.

(5) start the httpd server. As root user, type the following

```
# /etc/init.d/httpd start
```

(6) To have httpd start every time you boot your system, run the command as root user

```
# chkconfig httpd on
```

(7) To make sure webserver is working, open mozilla and type following.

- Q Date \_\_\_\_\_  
Page \_\_\_\_\_
- (8) You should see the test page for apache web server
  - (9) The test page is actually indicating that you haven't added any content to your website yet
  - (10) To get started you should add an `index.html` file that contains your own home page content to `/var/www/html` directory.

QN 23 What is DHCP server? Define package and configuration setting for both client and server site.

→ A DHCP server is a network server that automatically provides and assign IP addresses and other network parameters to client devices. It relies on the standard protocol known as dynamic host configuration protocol to respond queries by clients.

Setting up the DHCP server

→ The minimum tools you need to get the DHCP server working are:

- (i) A firewall that allows DHCP access
- (ii) A configured `/etc/dhcpd.conf` file
- (iii) A running `dhcpd` server daemon.

↳ Opening your firewall for DHCP

The firewall on your DHCP server must be configured to allow access to UDP port 67 and 68. If you are using iptables use following as root

```
#iprables -I input -I eth0 -p udp --sport 67:68 --dport 67:68
```

If the rule was accepted you can use entire firewall so that the new rule is included permanently.

.. `iptables -S > /etc/sysconfig/iptables`

↳ Configuring the dhcpcd.conf file.

There may be a need to set static IP addresses to particular host on the network such as printer, webserver and etc.

```
default-lease-time 600;
```

```
max-lease-time 7200;
```

```
subnet 10.1.1.0 netmask 255.0.0.0 {
```

```
range 10.1.1.3 10.1.1.254;
```

```
option domain-name-servers 10.1.1.1;
```

```
option routers 10.1.1.1;
```

```
}
```

```
subnet 192.168.0.0 netmask 255.0.0.0 {
```

```
{
```

```
host printer {
```

```
hardware ethernet 00:16:d3:b7:8f:86;
```

```
fixed-address 10.1.1.100;
```

```
2
```

```
host web-server {
```

```
hardware ethernet 00:17:a4:c2:44:22;
```

```
fixed-address 10.1.1.200;
```

```
2p
```

Starting DHCP server

After the etc/dhcpcd.conf file is configured, you can start the DHCP server automatically as a root user from a terminal window, type:

```
# service dhcpcd start
```

- setting DHCP client
- (1) while you are initially installing Redhat linux, click configure using DHCP on the network configuration screen.
  - (2) To set up DHCP after installation, open the network configuration window.
  - (3) from the network configuration window:
    - @ click the device tab
    - (b) click your Ethernet device (eth0)
    - (c) click edit
    - (d) click the general tab
    - (e) click "Automatically obtain IP address settings with and select dhcp".
    - (f) select ok
    - (g) select apply.
  - (4) Then, from a terminal window type
  - (5) # /etc/init.d/network restart

N.24. Define DNS with necessary configuration

ing ↳ The DNS server software that comes with the current Red hat linux  
↳ Berkeley Internet Name Daemon (BIND) To configure, you work with following components.

(i) configuration file (/etc/named.conf):

↳ The main DNS server configuration file.

(ii) zone directory (/var/named):

↳ The directory containing files that keep information about Internet root DNS servers (named.ca file) and information about the zones that you create for your DNS server.

(iii) Daemon process (/usr/sbin/named)

↳ The daemon process that means listens for DNS request and responds with information that the named.conf file present.

(iv) Debugging tools (named-checkconf, and named-check-zone);

What you use to determine whether you created your DNS configuration correctly

To create a useful DNS server for your example small-office environment, you have following zones

↳ public dns server zone

↳ private dns server zone.

To begin you configure the /etc/named.conf file on the primary master DNS server representing your example yourdomain.com domain. This example starts from the /etc/named.conf file that with caching nameserver.

The edited version of the /etc/named.conf file is as follows.

options {  
 directory "/var/named";

?;

acl "mylan" {

127.18.10.0.0.0.124;

?;

view "inside" {

match-client "mylan"; ?;

recursion yes;

zone "." IN {

type hint;

file "named.ca";

?;

zone "0.0.10.in-addr.arpa" IN {

type master;

file "yourlan.db";

?;

zone "yourdomain.com" {

type master;

file "db.yourdomain.com.inside";

allow-transfer { 10.0.0.2; } ?;

?;

?;

Page \_\_\_\_\_

view "outside" of  
match-client \$any; &  
recursion no;

zone ". IN {  
 type hint;  
 file "named.ca";  
};

Zone "yourdomain.com"  
type master;  
file "db.yourdomain.com.outside";  
allow-transfer \$123.45.67.2; 4;  
2;  
};

include "/etc/named.key";

⇒ The /var/named directory contains the zone files that the /etc/named.conf file names. For example, you need to create only three zone files from scratch you can leave the named.ca file alone.

\$TTL 86400

@ IN SOA yourdomain.com hostmaster.yourdomain.com \$  
2003040101 ; serial  
28800 ; refresh  
14400 ; retry  
. 8600000 ; expires  
86400 ; minimum

25 : What is MySQL? In what are the package and configuration of mysql?  
 MySQL is a popular Structured Query Language (SQL) database server which provides the means of accessing and managing SQL database.

The following package comes with Red Hat Linux:

- (i) MySQL
- (ii) MySQL-server
- (iii) MySQL-devel
- (iv) php.mysql

configuration of MySQL.

- ① installing MySQL-server
- ② creating the my.conf configuration file

many options which shows how MySQL server and related client programs runs are defined in /etc/my.conf file.  
 The default my.conf file contains only a few settings.

Example

```
[mysqld]
datadir = /var/lib/mysql
socket = /var/lib/mysql.sock
```

```
[mysql.server]
user = mysql
basedir = /var/lib
```

```
[safe mysqld]
err_log = /var/log/mysql.log
pid_file = /var/run/mysql/fd/mysql.pid
```

EDMITNOU  
QUAD

The default data dir value indicates that /var/lib/mysql is directory that stores mysql databases you create. The socket option identifies /var/lib/mysql/mysql.sock as the socket that is used to create the MySQL. The basedir identifies as the base directory in which the MySQL software is installed.

The err-log and pid-file options tells the locations of the error log and the file that stores the process ID of the mysqld daemon when it is running.

Starting the mysql server

To run on MySQL server, the /etc/init.d/mysqld startup script is delivered with the MySQL server package

To start manually

```
# service mysqld start
```

To have MySQL start each time computer boots:

```
# chkconfig mysqld on
```

प्रातःरात्रि

26. What are different Linux supporting files?

⇒ Linux is a very flexible operating system that has a long history of interoperability with other operating systems.

(a) Ext file system

⇒ The Ext file system is the extensible file system. Linux supports the various extensions of Ext i.e. Ext1, Ext2, Ext3, Ext4.

(b) Reiserfs

⇒ The Reiserfs file system is a journalising file system designed for fast server performance especially in directories of thousands of files.

(c) System v:

⇒ Linux currently provides read support for System V partitions, and write support is experimental.

(d) UFS

⇒ UFS is used in Solaris and early BSD operating system. Linux provides read support, and write support is experimental.

(e) NTFS

⇒ NTFS is next generation of HPFS. It comes with all version of Microsoft Corporation system beginning with Windows NT.

(f) IBM JFS

⇒ IBM JFS is an easy to use journalising file system created by IBM. It is designed for high throughput server environments.

(g) SGI XFS

⇒ SGI's extended file systems (XFS) is SGI's newest file system for all Silicon Graphics system, from workstations to its supercomputer line.

Now do you create a  
iosl, comment name Binod  
login shell as tsh shell. Also

11e.

.. user

id Binod

view the user default

A user add -D

Go to in /etc/default and open file user and with  
vis editor

Now create default home directory and default tsh

# useradd -d /home -s /bin/tsh

At last for mentioning comment

# useradd -c "Binod paudel" Binod

Traditionally, the /etc/passwd file is used to keep track of every registered user that has access to a system.

The permission for /etc/passwd are by default set so that it is world readable, that is, so that it can be read by any user on system.