message. When communicating using a computer, we can use asynchronous methods so that both parties do not have to be present simultaneously.

2) Try

cat /dev/tty04

where /dev/tty04 is the device file corresponding to the desired terminal.

One can also try

cp msgfile > /dev/tty04

3) You get an error message like

write: Input/output error

4) Prepare the message and store it in a file such as msgfile. For this you can use vi or any other editor. Then say

write khanz < msgfile

because write reads the standard input. You will have to see that khanz is logged in. If he is logged in from more than one terminal you will need to specify the terminal as well.

Check Your Progress 2

1) You can login but others who have you in your friend list will not be able to see that you are online. This is called logging in invisible mode.

2) Try Yourself

3) When she has not responded to your message for quite some time and you want to draw her attention.

4) Try Yourself

5) One way is to select the transcript and copy it to a file in your favourite word processor.

Check Your Progress 3

1) Try Yourself

2) The mail command has a rudimentary, hard to use interface. It does not have the features one would expect to have in a good e-mail client.

3) It allows one to organise one's mail better. Related messages can be stored in different folders rather than all messages being in one folder with hundreds of messages. This makes it easier to look for a message.

4) This saves us from the trouble of having to remember a large number of e-mail addresses. One can save the contact details of a person and then just use a short name or his nickname to send mail to him.

4.8 FURTHER READINGS

There are a host of resources available for further reading on the subject of Red Hat Linux version 9.0.

1. http://www.redhat.com/docs/manuals/linux
2. http://www.linux.org gives among other information, a list of good books on Red Hat Linux.
3. Consider joining a good linux mailing list.

UNIT 5 UNIX SYSTEM ADMINISTRATION

Structure **Page Nos.**

5.0 INTRODUCTION

In the previous units you have been introduced to Linux and have got an idea of its features and the facilities available in it. In this unit we will look at how to administer a Linux system and take care of it so that you can make use of its power. This would mean being able to install Linux on a machine and configuring and setting it up so that you could start working on it. It also requires maintaining the machine subsequently, such as by adding user accounts and keeping your data safe by backing it up.

The activities described in this unit are mostly performed as the superuser. So you have to be very careful and understand the commands you issue thoroughly, because Linux does not conduct many checks on what the superuser asks it to do. As an ordinary user you could not modify a file if you did not have permission, but the superuser can change any file irrespective of its permission settings. This might seem like a convenience, and it is indeed so. But it also means that you have the potential to cause severe damage to the installation through one mistakenly issued command.

5.1 OBJECTIVES

After completing this unit, you should be able to have an understanding of basic system administration tasks and be able to perform basic installation, configuration and maintenance of a Linux system. Some of the abilities you should have acquired are:

- understand what is meant by system administration;
- understand the responsibilities of the system administrator;

- install Linux on a personal computer;
- understand how to boot a Linux system and what goes on while starting it up;
- how to add and maintain user accounts;
- understand character and block special files, and
- know how you can back up data from the system and restore it when required.

5.2 SYSTEM ADMINISTRATION

You have started working on a Linux system and have learnt some of the basic facilities provided by the operating system. When you began your exploration of Linux, you were given a user account on a machine. For this to have happened, what are the actions that somebody would have performed for you? Let us try to work backwards and figure this out.

First of all, somebody would have had to load Linux on the machine that you are working on. This would mean having to know how the operating system is to be loaded on to your machine. Secondly, having got the machine working under Linux, somebody would have to set up user accounts and give them permission to log in to the machine and work on it. There are several other such activities that one can think of.

Configuring the system to connect to the local area network (LAN)

Adding new hardware devices to the system, such as hard disks, a printer or a CD-ROM drive. Taking backups of the important system and configuration files.

Booting up and shutting down the system as needed. Restoring the system to normal working in case of a crash, by using the backups.

Fixing software problems that might arise, such as a corrupted system file. Addressing issues such as performance tuning if the system is slow. Making sure that the system is secure from the assault of unscrupulous persons. Installing operating system upgrades and patches as required. Installing and configuring any new software that has been acquired by the organisation. Providing required network services such as e-mail, Internet connectivity and other services as appropriate. Helping ordinary users in trouble, such as those who might have forgotten their password.

Being able to do the above requires much more knowledge of the working of Linux than you have obtained so far. It also requires experience with various commands, tools and utilities. The tasks listed above are not the only ones that need to be performed for ordinary users to make use of the system and are only indicative.

Moreover, most of these responsibilities can be performed only by persons having superuser or root access to the system. Ordinary users, without root permission, cannot run many of the required commands. Because of this, these tasks have to be performed by experienced individuals, and with great care. A moment of carelessness could result in a wrong command being issued or an incorrect option being used, with the potential of catastrophic damage to the installation and to the work of several users who use that machine.

The activities we have described above are the domain of a role called the system administrator. The person who performs these tasks is called the system administrator. Depending on the size of the organisation, the responsibilities of a system administrator can be discharged by one person or by a group dedicated to this work. These people need to have adequate experience and training or knowledge about the working of

Linux, and need to keep themselves updated with the latest happenings to keep their knowledge current.

In a larger organisation, the work of a system administrator can be divided into various specialities, with a different person or group looking after each such speciality. These can be:

- A Network Administrator to look after the LAN, Internet connectivity and network services such as e-mail.
- A Security group to ensure that the system is secure from hackers and other disreputable individuals.
- A Hardware support group to keep hardware in fine fettle and to ensure it works well with your Linux system.

Sometimes you can have a Systems Group with different individuals or sub-groups looking at these functions. The exact structure and division of responsibility will depend heavily on the kind of organisation, the number of users there and the nature of work performed. In some companies, all installations might be performed by a different group or might be part of the computer supplier's work itself. A software development group in a financial services company might have much more need for security and so that aspect might receive more emphasis in such an establishment.

Any installation will tend to find the need for performing certain tasks again and again, or there might be a need to do certain things for which there are no specific commands or utilities in Linux. The system administrator therefore has occasion to create and use shell scripts that will help her do all this easily. She should therefore be skilled at shell programming. Such locally developed programs are often kept in a directory such as /user/local/bin for general use.

So we see that the system administrator is responsible for installing and maintaining the Linux installation. The specific nature of duties will depend on the organisation, but there are a few tasks that are common. The system administrator will therefore need to have adequate skill and experience in those tasks. In addition, he will often be faced with problems that have not occurred before. He should therefore be good at problem solving and innovation. Some of the qualities and training that he needs to have are:

- Knowledge of the structure of Linux and its usage
- Tools and utilities with their various options
- Shell programming
- Diagnosing the causes of problems.

These are therefore the qualities you have to imbibe as you take on the task of system administration. We will now look at how to perform some of the tasks of the system administrator.

5.3 INSTALLING LINUX

One of the basic tasks that you need to perform first of all, before you can do anything else, is to install Linux on your system. There are many ways in which you can do this and we will look at the main methods here. As always, because of the limited amount of space that we have here, we will concentrate on the main points. For more details, you should refer to the documentation that Red Hat Linux makes available to you. The installation process can be broken down into the following steps:

- Choosing an installation method
- Choosing an installation class
- Pre-installation checks
- Actual installation
- Configuration and set up

In some cases you might find it expedient to perform an upgrade instead of a full blown installation. This is something you could decide while choosing the installation method. There are also different things to be taken care of when installing Linux on different kinds of computers. For large machines that are more powerful than the typical microcomputer, the vendor of the machine would provide the Linux installation and support mechanism. Here we are looking at installing Linux on an IBM compatible personal computer. If your PC is of another type, such as an Apple Macintosh or a laptop or an older IBM compatible, there could be additional intricacies involved that we will not be able to cover here. You would need to make sure that Red Hat Linux will work on that system.

So now let us assume that we have a computer on which Linux will work and begin the steps for performing the installation.

5.3.1 Choosing an Installation Method

You have to first decide how you are going to be performing the Linux installation, as there are many methods available. One straightforward way is to do a local installation using a Linux distribution purchased from Red Hat. In that case you get a CD-ROM that you can used to boot your machine with. The rest of the installation can then be continued using the Linux CD-ROMs provided. For simplicity, we are assuming here that your computer has an IDE CD-ROM drive and that there is no other operating system installed on it. This means that your computer is blank, with nothing else on it and your Linux installation is going to be the first time anything has been put on it. If you have some other hardware, then there will be an additional driver diskette that you will need to have and that you will have to insert at the appropriate time. You can boot the Linux installation program from a floppy also.

Some other ways of installing Linux are:

- Using an FTP server that has the Linux images on it
- Using an HTTP server that has the Linux images on it
- Using an NFS server that has the Linux images on it.

In all the above cases, you will need a network driver floppy diskette or a PCMCIA driver diskette.

5.3.2 Choosing an Installation Class

There are different classes or types of Linux installations that you can choose from. They are appropriate in different situations and you can decide the one to use based on the intended end use of the system. Remember that these types really determine what kind of software components are installed and there is no fundamental difference between them. They are really a short, predetermined set of components or packages. The classes are briefly described here.

Personal Desktop

This is the simplest installation that brings in the least number of software packages. It is useful if the machine is going to be used by an end user, such as at home, or for

office productivity. It will also install the GUI desktop environment with the X-Window system. This is useful for new users who are just getting familiar with Linux and will not want to perform advanced tasks.

Such an installation needs 1.8 GB of free space. During the installation you can still choose to install additional packages that are not part of the default installation. So what you really put on the machine is still up to you. But it does save you from the tedium of choosing every single package to put in.

This installation will use up to twice your RAM as disk space for your swap partition. The root partition will hold all the system files and user files. The size of the boot partition will be 100 MB.

Workstation

A workstation installation is useful for professional software developers. It puts in a graphical user interface together with basic software development tools and more system administration utilities. It will use up to 2.2 GB of disk space. The other characteristics are the same as the Personal Desktop installation. Both of these can take up any other software packages that you want to install as you go through the process. Remember that if you choose to put in more packages, the disk space required will be correspondingly greater.

Server

If you are going to use your machine as a server then you would perhaps not need much configuration to be done on it. In such a case you can do a server installation without even putting in a graphical user interface. You would then need just 850 MB to 1.5 GB of space depending on how much functionality you plan to put in. Should you decide to put in the GUI, the space required would increase correspondingly. The other characteristics of the default server installation are the same as for the other classes.

Custom

A custom installation is the most flexible option as it does not have any predetermined packages that will be put in. You have to decide which packages you want as you proceed. This therefore requires an understanding of the packages that are available and their dependencies. It is meant for advanced users who know exactly what they want and need the freedom to decide. The disk space required varies from 475 MB to 5.0 GB, depending on what you choose to put in.

All the above classes of installations have the same partitions if you choose automatic partitioning. Also, the disk space requirements mentioned above assume you are installing only the English language version. Should you choose other languages as well, the space requirements will go up in each of the above cases.

Upgrade

It is also possible to install Linux on a system that already has some earlier version of the same operating system. The old Linux version should be 6.2 or later, because that is when the rpm method of package installation was introduced. If that is the case, you do not have to go through all the steps needed in a fresh installation. The advantage is that all the data that you have will be preserved in an upgrade. Your partitions will not be altered and only the appropriate software packages will be upgraded. So you do not have to go through the exercise of backing up your data and restoring it after the installation has been completed.

5.3.3 Pre-installation Checks

Before commencing your installation, it would be politic to garner information about your machine. You first need to see how much hard disk space you have. That could have an impact on the kind of installation you can perform. However, in these days of large hard disks of 80 GB and above, it is unlikely to be a constraint. Yet it is best to make sure.

When we refer to the disk space, it means unpartitioned disk space that is not currently being used by another operating system because every partition on the disk behaves like a separate disk drive. It is quite possible to install Linux on a machine that is currently running some other version of Linux or of an operating system like Microsoft Windows of some flavour, such as Windows 2000 or Windows 98.

You next need to find about more about the type and make of the hardware on your machine, as this is information you will have to provide as you go ahead with the installation process. For this, you will need to refer to the documentation provided by the manufacturer of your machine. If you have an assembled machine, refer to the documentation that came with the computer components that you put together. In many cases, your existing operating system can give you information about your hardware. For example, in Windows 2000 you can look at your Device Manager tab under the System icon in the Settings to find out about the hardware and the specific type and make. While this is no substitute for actually finding out about your hardware physically, it is usually sufficient for you to be able to perform the installation.

Here is a list of some of the hardware that you should get more information about, to be able to carry out your Linux installation without interruption.

- The hard disk – is it an IDE or a SCSI? What is its capacity and is there any volume label? What are the partitions you will want to create and what will be their sizes? For example, do you want to have `/tmp` or `/home` as separate partitions or will everything be in `/root`?
- Similarly you need to know about your CD-ROM drive. Is it an IDE or a SCSI type?
- Which is your hard disk controller? If using a SCSI adapter, who is the manufacturer and what is the model number?
- What kind of mouse do you have? Here you must know the mouse type, such as serial, bus or USB and the protocol, such as generic. Also note the number of buttons, which are commonly 2 or 3. Does it have a vertical or horizontal scroll wheel?
- What kind of monitor do you have? Here note the manufacturer and the model number for reference.
- What are the characteristics of your display adapter? This is especially important if you are going to install the Graphical User Interface. Remember the manufacturer and the model number as well as the amount of video RAM used.
- Find out about your sound card. For this you again need to know the manufacturer and the model number. In addition, note down the chipset used.
- Do not forget the amount of RAM in your computer.

Besides the above, you will need to have some more information for your computer to be able to access the network. First you have to choose a name for your system. This is a personal choice and has to be unique within a domain. Organisations have their own schemes for this. Some use the names of rivers, mountains, sages or places. Others leave it to the system owner while still others use mundane numbering schemes

such as `marketing001`. You will have to follow the organisation's policy here. Make sure you know the organisation's Internet domain name. This is typically derived from the organisation's name but could be different. For example, for IGNOU, the domain name is `ignou.ac.in`. In larger companies, the Internet domain name is further subdivided and if so, you have to know the domain name for your subdivision in the organization. This could be something like `marketing.mycompany.com`.

Next, make note of your network interface card. Again, here you must know the manufacturer and the model number.

Find out the IP address allotted to your machine. This could be a static IP address decided by the organisation. If it is allocated dynamically by DHCP, you should be aware of the DHCP server address that does this allocation. In many cases, while the address is allocated by a DHCP server, it is permanent in that it does not change from one boot to the next. In addition, you need to know the network mask for your machine.

In case your machine will boot off a machine on the network, you need to supply that machine's IP address.

You also need to know the IP address of the default gateway for your network that connects it to the outside world.

Lastly, you need to note down the IP address of the DNS server that your machine will use to resolve hostnames to IP addresses and vice versa. There could be more than one nameserver, in which case you need to know the IP addresses of those machines as well.

Once you have all of the above information, you can proceed to the actual installation of Linux on your machine. You should see that all of this is noted down on a piece of paper for ready reference as you go ahead with the process.

5.3.4 Installation

We will now see how to install Linux on your machine using the Linux bootable CD-ROM. As we have already observed, there are several ways of installing Linux. Here we are assuming a simple scenario where you are installing Linux from a Red Hat distribution from a CD-ROM on a computer with IDE drives. There is no other operating system running on the computer, so we do not have to take into consideration the issues involved in creating a dual boot system.

As a beginner to installation, you would prefer to use the graphical user interface with a mouse for your work. Of course, the keyboard can also be used for working with the GUI. Later, when you become more experienced, you can look at using a command line interface and performing more intricate installations. These can include using text mode installation, booting from a different source, controlling memory usage, using kernel options and so on.

To begin loading Linux, insert your bootable CD-ROM into the drive and turn on the machine. Here you will need to make sure that your system is configured to boot from the CD-ROM. For this you might have to change your BIOS settings to alter the boot order. If this is taken care of, your machine will display a prompt

```
boot:
```

At this point you can either do nothing and the boot process will start automatically after some time. Alternatively, to begin right away, you can press the ENTER key. If you do this, you would be ignoring the various boot options that you are presented with by the program. That is just what you would probably want to do as you learn about the process of loading Linux.

Once the booting process starts, you should find that your hardware is automatically detected. If this does not happen, you will have to do the installation in expert mode. But here we assume that things go well and you are able to proceed. You will now get the boot loader screen, where you should select the option to install from CD-ROM. The system will first try to determine the type of your CD-ROM drive. If yours is an IDE type drive, the program should detect it. In case you have a SCSI drive, you will be asked to choose a SCSI driver. If your drive is an IDE but the program is not able to detect it, you will need to refer to the Linux installation documentation or seek expert help on the matter.

If all goes well, you will come to a screen that says Language Selection. Here you have to specify the language that you would like to use during the installation process. There is a wide choice here, that includes Chinese, Japanese, French, Italian and many more. Let us assume that you want to work with English, in which case you should select it and then click on the Next button to continue.

The next screen that you get prompts you to select your keyboard layout type that you want to use. Here you would probably want to use the U.S. English layout. This is the QWERTY keyboard that we are familiar with and that has the $ sign over the number 4 in the top row. So select this layout using the mouse. You can also change your keyboard layout after the installation is over by using the keyboard configuration tool.

This brings us to the next screen, which is where we specify the kind of mouse that we have. Here there are many choices, and unlike the previous two cases, it is not at once apparent what type you are likely to have. The research on your hardware that you

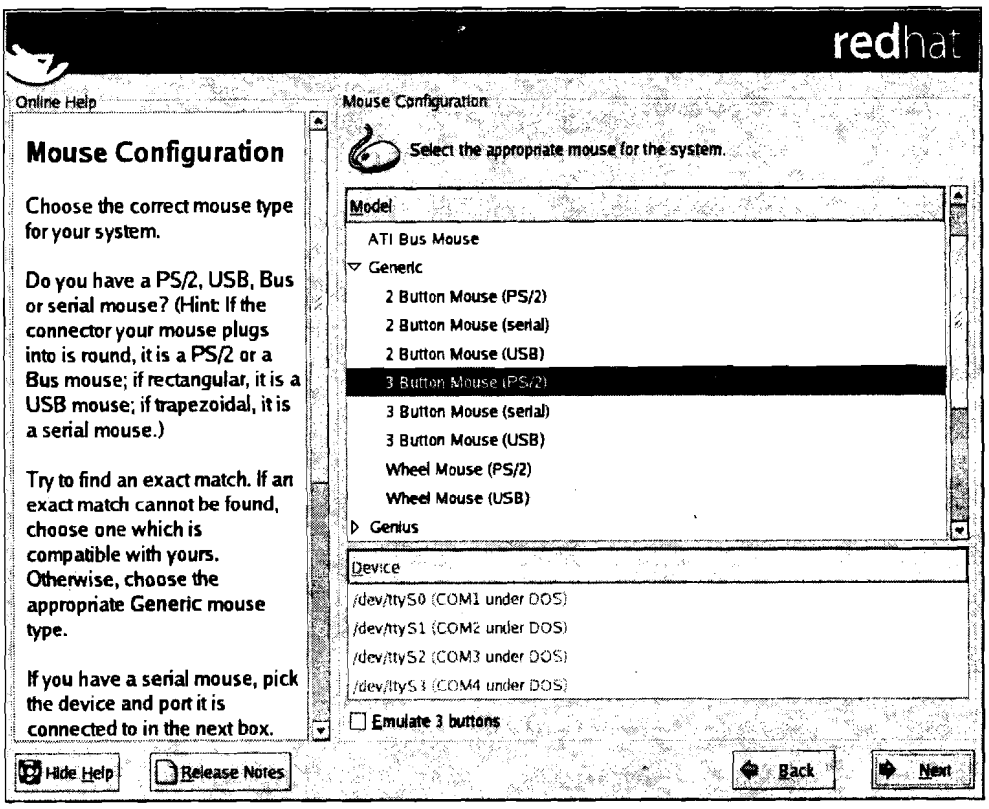

Figure 1: The Mouse Selection Screen

would have done in the previous section is what will now come in useful. You need to choose from among the many mouse types supported. Since you already know the kind of interface your mouse uses (PS/2, AT, serial, USB) and the number of buttons that it has, you will be easily to make the appropriate selection. *Figure 1* shows this screen to make things clearer for you.

What does one do when one cannot find an entry that seems to match our mouse? You can try the Generic type. If your mouse has a scroll wheel, you can make the selection as applicable, by choosing USB or PS/2. Another selection that you have to make is whether to emulate three buttons when your mouse has only two. This can make it easier to use a graphical user interface. The emulation is done by considering the middle button to be substituted by both the left and right buttons. So if you press both of them simultaneously, it is equivalent to pressing the middle button.

After completing the installation, you can make your mouse left handed. This is more convenient for left handers as it corresponds to their natural hand. Here the functions of the left and right mouse buttons are interchanged. So the right button becomes the main button.

Finally, if your mouse is a serial mouse, you will have to specify the device or port (such as COM1 or COM2) that your mouse connects to. Now having answered all the questions related to your mouse, you can click on the Next button and proceed to the next screen.

The installation program can detect a previous version of Linux that is already present on your system. In such a case, you will now come to a special screen that will prompt you and ask whether you want to upgrade your existing installation. Should you choose to upgrade, all your existing data will remain safe. None of your partitions will be changed and only the required files will be altered and overwritten. This option will work for Linux versions 6.2 and later. You will have the option to customise the installation and to choose the packages you want upgraded.

However, it might be that you simply want to throw away your old installation and begin again from scratch. This time your data might or might not be preserved, depending on what kind of partitions you make in your fresh installation. If they are the same as the existing ones, your data will be safe. Should you choose a different partitioning scheme, then your data will be erased and will no longer be accessible after the process is over.

Once you have made your choice, you need to click on the "Next" button to move on to the next screen. This is where you choose your installation class or type. You already know about the differences between the Personal, Workstation, Server and Custom installations. If your machine will be used by developers in an office environment, the Workstation type might be best for you. After making your selection, go to the next part.

Now you come to an important screen where you have to partition your hard disks. This can be a daunting task for a beginner, but since you are a system administrator, it should be easy for you. Linux comes with a tool called Disk Druid to help you do this. Whenever, you perform an installation, you should be prepared for the possibility of losing all data on the disk. Therefore, it is important to back up all your important data before commencing the operation. In this discussion, we have not so far dwelt on the point because we assume you are installing on a new machine that does not have anything on it.

When using Disk Druid, you will have full control over the partitions. You will be able to choose the partition sizes and the types of the file systems you want to create on them. You will be able to decide where they will be mounted when Linux runs. However, if you do not want to go through this, you can ask the program to perform automatic partitioning. This does not give you much control but is a good option if you do not want to change anything or are doing your first Linux installation.

Even automatic partitioning will allow you to choose what kind of existing partitions are to be deleted from your disk. These choices are presented to you on the next screen. You can decide that you want to delete all old Linux partitions, or all existing

partitions that might have other operating systems or file system types installed on them. Instead, you can also choose to preserve all existing partitions and use whatever free space is available on the hard disk. Since you might have more than one hard disk, the screen allows you to choose the one on which you want to create these partitions. All the partitioning choices will apply only to the disk that you have selected.

You can then review the partition selections that will apply and confirm or decide to modify them. Here you will be working with the Disk Druid utility, as you would have had you chosen to partition manually. At this point you will be faced with some detail, as you have to decide where you want Linux to be installed. You would have already made these choices while preparing for the installation.

The Disk Druid shows you the hard disk and its model number at the top of the screen. You also see the number of cylinders, heads and sectors that collectively describe the drive's geometry. You should make sure that this is in tune with what you already know about your hard disk. The tool then shows the device file corresponding to the device, the point in the directory hierarchy at which it will be mounted, the type of the file system it will contain, whether the partition will be formatted, its size and the start and end cylinders for the partition. This is shown for every partition.

Let us take a brief look at the different kinds of file systems that are available to you. A swap partition is used to increase the amount of virtual memory that your Linux system can use, as it supplements the RAM. Whenever required, pages are swapped from RAM to the swap partition on the disk and are loaded back when possible. Usually the size of the swap partition is made twice the RAM that you have. Linux has a file system called VFAT that is compatible with Microsoft's FAT file system and supports its long filenames.

The tool also allows you to create RAID partitions for redundancy that makes for more safety of your data, because if one partition develops an error, you can still access your data from the other. However, in this first shot at Linux installation, we will not venture into configuring RAID partitions. But this can be done by first creating two or more partitions that have a RAID file system type.

You can also create logical volumes using the tool. Here you can use one or more partitions on the same or different hard disks to work like one single logical partition or volume. This can allow you to have volumes that are larger than any single hard disk that you have. Again, in this introduction, we will not go into more detail about creating and maintaining logical volumes. You can create physical logical volumes by selecting that as your file system type.

The ext2 file system is the basic Unix file system and ext3 is the journalling version of ext2. Journalling allows you to quickly recover from system crashes. The default file system type in Linux is ext3, and is also the recommended choice.

Let us now look at the operations we can perform with the tool. You can add, remove or modify partitions. You also have a reset button that lets you restore the initial state of the disk, the situation that prevailed at the time you started the session. If you reset, the changes that you might have asked for in the session will be lost.

You can remove a partition from the disk. If you do so, you will be asked to confirm, as this has the potential to cause loss of data if it was an existing partition that was in use.

When you choose to add a partition, you have to provide information about it. The first thing is the mount point. To help you, there is a pull down menu that you can use to select the appropriate value here. For example, the boot partition should be mounted on `/boot` and the root partition on /. Then you need to enter the type of the file

that you want the partition to contain. The next selection is where you specify the hard disks that can contain the partition. If you do not select a disk, then your partition will not be created on that disk. You would usually let the tool decide where to place the partition.

You now need to enter the size of the partition. You can either enter a fixed size in MB, or choose to allow the partition grow from a base size to an upper limit as required. You can even choose to let the partition grow to fill up the entire available space on the disk. Next you can decide to let this be one of the primary, or first four, partitions on the hard disk. If not, it would become a logical partition. The last option while adding a partition is specifying whether you want to check for bad blocks while formatting. While it is a good thing to do, checking for bad blocks can take a fair amount of time, especially with the large capacity hard disks of today.

Similarly, when you select a partition for editing, you can change its attributes such as the file system type or size. If the partition information has been already written to the disk, you can only change the mount point of the partition. Should you want to change other attributes, the only way is to remove the partition and create it again with the new attributes.

Once you have done partitioning your hard disks, you need to move ahead to the next installation screen that lets you install your boot loader. A boot loader is needed so that it can load Linux. Whenever the computer is started up, its BIOS loads the program that is installed on the Master Boot Record (MBR) of the hard disk. This program then loads the operating system. You can also install the boot loader on the first sector of your boot partition, in which case the boot loader on the MBR will need to be asked to start up your boot loader. So if your disk has only Linux as the operating system, you should place your boot loader on the MBR.

Linux has two boot loaders called Grub and Lilo. Grub is powerful and can load Linux as well as other operating systems. Lilo is also a good boot loader and can boot Linux from several different sources. You will also have to choose which operating system to boot from by default, in case you have another already installed on your hard disk. Then when you boot your machine, you will have to choose the other manually if it is not the default.

You need to remember that if you do not install a boot loader, you will be able to boot Linux only through a boot diskette. So you should install one unless you have some special reason for not doing so. This could be because you already have your favourite boot loader, such as a third party commercial offering like Partition Magic, installed on the hard disk. After the boot loader installation screen, the next screen you reach will depend on whether you have a network interface card on your computer. If so, you will reach the network screen. In an organisational set up, this is the most likely situation. So let us now look at the configuration to be done here.

If you were installing off a network, then you would have already used a network driver diskette to be able to work. But if you started installing using, say, a CD-ROM, then you can now configure your network cards. You have to select from the devices that are detected during installation and decide whether they should be activated automatically at boot time. For each device, you need to edit its properties, namely, its IP address and netmask. If these will be supplied by a DHCP server, you can specify this here. These values will depend on what is used in your organisation.

You can now enter the hostname and let it be detected automatically by a DHCP server. These decisions you would have already made as part of your pre-installation preparation. Now you also need to put in the IP addresses of the gateway for your network that connect it to the outside world and the IP addresses of up to 3 DNS servers for it. If you are using DHCP, these will be provided automatically and you

need to enter this information only if you are providing the IP address of the machine manually.

It is quite all right to provide this information manually for one network interface card and to set these values for another card through DHCP. Once you are done with the network configuration you can select the Next button to move on to the next screen where you will set up your firewall.

In these days of networks, your computer is vulnerable to all manner of attacks by persons so inclined. A firewall offers protection against intruders over the network. Well configured, it reduces the chances of an attack greatly. You can choose from three levels of predetermined security policies. The first is the option of not using a firewall at all. While it might seem strange after what we have just said, this can be a good choice if you are sure your machine is going to be on a trusted network, such as a corporate network protected by other firewalls. Also, you might be planning to perform a more elaborate firewall configuration later.

The next level of security that you can choose is medium. This disables access from the outside to reserved ports, that is, up to port 1023. So services like HTTP, FTP and so on will not work. Also barred are NFS servers and clients and X-Window display access to remote machines. The X font server is also disallowed.

The highest level of security bars all but DNS and DHCP. If the pre-configured firewall rules seem too restrictive or are not what you want, you can always perform additional customization. One thing that is possible is to declare some devices as trusted, whereupon no firewall checking will be done for them. You could do this on a multi-homed machine, where some of the networks are trusted. So if you are on the Internet through one interface and are connected to your company network through another, you can decide to declare the company network as trusted. You can also choose to allow access to additional ports beyond those allowed by your security level. Some of these are listed as service options that you can select through a checkbox, for instance mail and FTP. Besides, you can allow any arbitrary ports by using the notation

```
port: protocol
```

such as `1111:tcp`.

Having secured your system, you can select the Next button to move on to the succeeding screen where you can set your language options. Linux allows you to work in multiple natural languages. As you might imagine, you have to choose at least one language to work with. If you choose only one language, it is the default as well. If you choose more than one language, you need to choose one language that will be your default.

The language that you chose to use for installation at the beginning of the installation process might not be the same as the language you choose to install for use thereafter. However, that is the language selected by default. If they are different, then after the installation is over, you will be able to use only that language. For example, if you use English (USA) as the language for installation, and select French (France) as the language in this screen, then your installation will continue in English. Once the installation is over, you will be able to use only French.

You should choose all the languages that you might want to use during normal working. But it might be better to avoid choosing languages that you are not likely to use, because of the extra disk space that will be taken up by putting them in.

Well, that has been a lot of choosing and decision making! Now it is time to sit back and let the machine do some work for a change. When you go to the next screen, you are at a point where you have to make one final decision about whether to go ahead with the installation as you have chosen. This is the last chance you have to abort safely, because if you go ahead here, the partition information will be written to disk and the installation will begin. Even so, to abort the installation, you need to reboot the computer.

To select the time zone, you have two methods. You can enter the offset from UTC for your location. So for India choose the option for +5:30, as Indian Standard Time is 5 hours 30 minutes ahead of UTC. For countries that use daylight saving time, you can set that too.

The second method is to set the time zone interactively, based on your location. You see a map of the world with many important cities marked out with yellow dots. The place you select will be shown with a red X.

Once the time zone has been set, it is time to set up your root password. This is an important password, as the root or superuser has complete control over the system. Restrictions and permission settings that apply to ordinary user accounts are no bar for the root user. So this password must be set with care. Make sure that it is not easy to guess. You have to enter the password twice and both the entries must match for the installation to move forward. If you are going to be administering this system, you must preserve the password carefully. But even then, do not use this account for ordinary work, because a small mistake as root could damage your installation. Use it only for administrative work on the machine.

The next screen is for setting up authentication information. You need not really do anything here unless you are going to set up network passwords. But you could choose the "Enable shadow passwords" option. This keeps your password more secure because the actual password is stored in the file `/etc/shadow` instead of `/etc/passwd`. The shadow file is readable only by the superuser, unlike the `passwd` file that is readable by all.

After this you come to another important screen where you configure the packages to be installed on your machine. This is where choosing an installation class is useful. Depending on what has been chosen, a list of package groups appears. You have the option of accepting the recommended packages for installation or of deciding on them yourself. Each group of packages can have optional packages that can be installed depending on your preference, besides base packages that are installed with that group by default.

When you choose to customise the packages to be installed, you have to select the checkbox next to the package group. Then you can click on the details link to obtain a list of all packages that constitute the group. Here you can select the individual packages that you want to have. After selecting the package groups, you can see all the packages that will be installed on your machine. This can be done in an alphabetical listing or as a tree structure under each group. Certain required packages needed to run Linux cannot be selected or deselected as they do not appear in the package listings. They are always installed. Information about a package can be had by clicking on it.

What you need to be aware of is that some packages might be dependent on others in order to work properly. You need not worry about what these dependencies are as the install program finds that out automatically for you. After you have completed your package selection, you get a list of such unresolved dependencies. You are then given the option of resolving these dependencies by including the dependent packages, ignoring the dependencies or simply discarding the packages that have the dependencies. Remember that if you choose to ignore the dependencies, the packages with the dependencies might not work as expected. Of course, if there are no unresolved dependencies to start with, you will not see this screen.

You can see the amount of disk space that will be required by your selection, so if there are constraints you can adjust your package selection. However, in these days of large disks, it is not likely to be a problem.

If you have another operating system such as Microsoft Windows 2000 loaded on your machine, you would have the choice of selecting it to boot from. If you choose to take no action, the default operating system will be booted up anyway after the timeout period has elapsed.

need to enter this information only if you are providing the IP address of the machine manually.

It is quite all right to provide this information manually for one network interface card and to set these values for another card through DHCP. Once you are done with the network configuration you can select the Next button to move on to the next screen where you will set up your firewall.

In these days of networks, your computer is vulnerable to all manner of attacks by persons so inclined. A firewall offers protection against intruders over the network. Well configured, it reduces the chances of an attack greatly. You can choose from three levels of predetermined security policies. The first is the option of not using a firewall at all. While it might seem strange after what we have just said, this can be a good choice if you are sure your machine is going to be on a trusted network, such as a corporate network protected by other firewalls. Also, you might be planning to perform a more elaborate firewall configuration later.

The next level of security that you can choose is medium. This disables access from the outside to reserved ports, that is, up to port 1023. So services like HTTP, FTP and so on will not work. Also barred are NFS servers and clients and X-Window display access to remote machines. The X font server is also disallowed.

The highest level of security bars all but DNS and DHCP. If the pre-configured firewall rules seem too restrictive or are not what you want, you can always perform additional customization. One thing that is possible is to declare some devices as trusted, whereupon no firewall checking will be done for them. You could do this on a multi-homed machine, where some of the networks are trusted. So if you are on the Internet through one interface and are connected to your company network through another, you can decide to declare the company network as trusted. You can also choose to allow access to additional ports beyond those allowed by your security level. Some of these are listed as service options that you can select through a checkbox, for instance mail and FTP. Besides, you can allow any arbitrary ports by using the notation

```
port: protocol
```

such as `1111:tcp`.

Having secured your system, you can select the Next button to move on to the succeeding screen where you can set your language options. Linux allows you to work in multiple natural languages. As you might imagine, you have to choose at least one language to work with. If you choose only one language, it is the default as well. If you choose more than one language, you need to choose one language that will be your default.

The language that you chose to use for installation at the beginning of the installation process might not be the same as the language you choose to install for use thereafter. However, that is the language selected by default. If they are different, then after the installation is over, you will be able to use only that language. For example, if you use English (USA) as the language for installation, and select French (France) as the language in this screen, then your installation will continue in English. Once the installation is over, you will be able to use only French.

You should choose all the languages that you might want to use during normal working. But it might be better to avoid choosing languages that you are not likely to use, because of the extra disk space that will be taken up by putting them in.

You are now at the tail end of the installation process. The next item to be configured is the time zone. Here you can choose to set your system clock to Universal Time Coordinated (UTC) that is based on the 0^{o} longitude that passes through Greenwich. The time that you will then see will be based on UTC and the time zone that you enter.

To select the time zone, you have two methods. You can enter the offset from UTC for your location. So for India choose the option for +5:30, as Indian Standard Time is 5 hours 30 minutes ahead of UTC. For countries that use daylight saving time, you can set that too.

The second method is to set the time zone interactively, based on your location. You see a map of the world with many important cities marked out with yellow dots. The place you select will be shown with a red X.

Once the time zone has been set, it is time to set up your root password. This is an important password, as the root or superuser has complete control over the system. Restrictions and permission settings that apply to ordinary user accounts are no bar for the root user. So this password must be set with care. Make sure that it is not easy to guess. You have to enter the password twice and both the entries must match for the installation to move forward. If you are going to be administering this system, you must preserve the password carefully. But even then, do not use this account for ordinary work, because a small mistake as root could damage your installation. Use it only for administrative work on the machine.

The next screen is for setting up authentication information. You need not really do anything here unless you are going to set up network passwords. But you could choose the "Enable shadow passwords" option. This keeps your password more secure because the actual password is stored in the file `/etc/shadow` instead of `/etc/passwd`. The shadow file is readable only by the superuser, unlike the `passwd` file that is readable by all.

After this you come to another important screen where you configure the packages to be installed on your machine. This is where choosing an installation class is useful. Depending on what has been chosen, a list of package groups appears. You have the option of accepting the recommended packages for installation or of deciding on them yourself. Each group of packages can have optional packages that can be installed depending on your preference, besides base packages that are installed with that group by default.

When you choose to customise the packages to be installed, you have to select the checkbox next to the package group. Then you can click on the details link to obtain a list of all packages that constitute the group. Here you can select the individual packages that you want to have. After selecting the package groups, you can see all the packages that will be installed on your machine. This can be done in an alphabetical listing or as a tree structure under each group. Certain required packages needed to run Linux cannot be selected or deselected as they do not appear in the package listings. They are always installed. Information about a package can be had by clicking on it.

What you need to be aware of is that some packages might be dependent on others in order to work properly. You need not worry about what these dependencies are as the install program finds that out automatically for you. After you have completed your package selection, you get a list of such unresolved dependencies. You are then given the option of resolving these dependencies by including the dependent packages, ignoring the dependencies or simply discarding the packages that have the dependencies. Remember that if you choose to ignore the dependencies, the packages with the dependencies might not work as expected. Of course, if there are no unresolved dependencies to start with, you will not see this screen.

You can see the amount of disk space that will be required by your selection, so if there are constraints you can adjust your package selection. However, in these days of large disks, it is not likely to be a problem.

Well, that has been a lot of choosing and decision making! Now it is time to sit back and let the machine do some work for a change. When you go to the next screen, you are at a point where you have to make one final decision about whether to go ahead with the installation as you have chosen. This is the last chance you have to abort safely, because if you go ahead here, the partition information will be written to disk and the installation will begin. Even so, to abort the installation, you need to reboot the computer.

Once you click on the Next button here, the install program will start installing Linux and all the selected packages according to the options that you have provided. There is nothing for you to do but to wait and watch the installation proceed. To relieve the monotony and to reassure you that progress is indeed being made, you can see a bar and other screen messages that give the latest situation regarding the install. As you can imagine, the time taken here will depend on how fast your computer is and what packages you have chosen for installation.

Presently your installation will be completed. You will then be asked whether you want to create a boot diskette. You should create one, because it will enable you to boot should anything happen to your boot loader. You can create the diskette even after the installation is over and you have started working on it. For that matter, you can perform most of the steps in the installation such as configuring devices, language selection, package selection, configuration of services, firewalling and so on at any time even after the initial installation is over. The only requirement is that you know the root password as only the superuser can perform such maintenance.

If you want, you can now configure the X-Window system server that is needed to get your graphical user interface. You have to choose the video card that your machine has from the list provided. If you know your card characteristics well, you can select the unlisted card and configure it, but in general, if your card does not appear in the program's list, it is not supported by the X-Window system. After selecting the card, you have to specify the amount of memory it has. Try to give the correct value and consult the card documentation if needed. While specifying more memory will not harm anything, it can mean that you have trouble with your X server.

The next screen lets you configure your monitor. You will be presented with a list of monitors from which you should choose your display, or the one closest to it. If your monitor does not appear on the list, choose an appropriate Generic monitor. Here you have to be careful that you do not select a monitor that has capabilities beyond yours. Your monitor can be damaged permanently if the selected monitor has horizontal or vertical synchronization frequencies beyond those of your display. Your monitor could get overclocked and be destroyed in such a case.

Now decide your colour depth and display resolution. You can also decide whether after booting you want to land up in graphics or text mode. In the latter case you will be presented with a command prompt from which you can issue any Linux commands that you wish. It might be better to set up the machine to get into graphics mode directly. Finally you can see your efforts bearing fruit. When you select the Next button on this screen, you will see the long awaited message that tells you the installation is complete. You will now be asked to reboot the machine. You should remove your CD-ROM or diskette from which you had booted the machine for installation, otherwise the computer will boot again from that device and not from your hard disk.

5.4 BOOTING THE SYSTEM

Now you are ready to boot up the machine from your hard disk, using your freshly installed Linux. You can reset the computer or power it off and on again. After the

machine's preliminary power on checks are over, you will come to a screen where you have the choice of booting the default operating system. Let us assume here that you have configured Linux to be your default system.

If you have another operating system such as Microsoft Windows 2000 loaded on your machine, you would have the choice of selecting it to boot from. If you choose to take no action, the default operating system will be booted up anyway after the timeout period has elapsed.

Once Linux starts to boot, you will see several checks being performed, at the end of which you are presented with the prompt to login. This assumes you have not chosen to start up the graphical user interface, in which case you see a graphical login screen rather than a text based terminal.

When you boot up Linux for the first time there is some configuration you might like to do, such as setting the system date. You will be presented with a Setup Agent that will lead you on through such tasks.

Booting is so called because the job involves something akin to lifting oneself up by one's bootstraps, that is, from a system which is off you need to have a system running a complex operating system like Linux. This task is done in stages, with a very simple program in the computer's ROM that runs and loads a boot loader program on say, the hard disk, which is then able to load the whole of the Linux kernel.

Once the Linux kernel is loaded, it brings the system state to the run level that is specified in the file `/etc/inittab`. In this state you have the system in multiuser mode with NFS services available, if configured. This is the default state for a Linux system. If you want to perform some maintenance on the machine you would do it in single user mode that is run level `1`. In this state only the console is available for logging in and other users cannot come in.

The tasks to be done when entering a particular run level are determined through a file called `/etc/rc.d/rcn.d`, where *n* is the run level. This gives a list of scripts that are run, and consists chiefly of services that are started up.

Together with booting up, you need to know how to shut down the system safely. When in operation, the file system is buffered in RAM, meaning that it is stored in the RAM and is then flushed to the disk from time to time. Thus the file system on the hard disk is not always in synchronization with that in RAM. So abruptly powering off the computer can badly damage the file system, sometimes beyond repair. To power off a computer running Linux, use the shutdown command, which really is a user friendly front end to the init command.

You can look at the manual entry for shutdown to see all of its many options. There are only two that you are likely to use frequently. To initiate a shutdown immediately, say:

```
[root@linux root]# shutdown -h now
```

You can also give an absolute time in the form hh:mm, such as `23:45` to shutdown the computer at that time. More likely you want to specify the amount of time to wait by specifying `+m` for the number of minutes you want to give as the grace period. The keyword now is equivalent to `+0`.

Sometimes you want to not just shutdown but to reboot as well. For this you can use the `-r` option to the command.

```
[root@linux root]# shutdown -r now
```

This command will perform all the necessary work to shutdown your machine in an orderly manner.

☞ Check Your Progress 1

1) List some of the duties of a system administrator.

.....

2) Turn off the computer abruptly when you and other are working on it. See how a file system consistency check is performed. Is it possible that some data gets lost.

.....

3) Find how to force a file system consistency check.

.....

5.5 MAINTAINING USER ACCOUNTS

You have seen in the second unit how users can login into the system and how passwords are used to prevent unauthorised access. You also saw how one or more users could be associated with a particular group. When you studied the long listing provided by the `-l` option to the `ls` command, you saw how the user name and group were also given for each file in the listing.

You also know that an ordinary user cannot help you if you have forgotten your password, and that only the superuser can set somebody's password without already knowing what it is. One of the duties of the system administrator is in fact maintaining user accounts. This activity encompasses creating new accounts, deleting accounts of users who are no longer permitted to access the site and helping people who might have forgotten their passwords. On many large installations the system administrator will run regular checks on user passwords to make sure that they cannot be guessed easily.

The Linux utility for setting passwords does perform some checks for the quality of the password, but do not rely on them completely. Some of the messages it can give are:

BAD PASSWORD: it is based on your username

BAD PASSWORD: it is too short

BAD PASSWORD: it does not contain enough DIFFERENT characters

BAD PASSWORD: it is too simplistic/systematic

These give you an idea of the kind of checks that are done, but the system administrator can also help here by setting a minimum and maximum time between permitted password changes. The check for the minimum time is based on the premise that an intruder will want to change the password as soon as he gains access. The user can also be given a warning some time before the password is due to expire and passwords not changed for a given time even after they expire can be taken as inactive. You should choose passwords that are not easy to guess and should change them periodically.

With all this background, let us see just how user accounts are maintained. This information is kept in a file called /etc/passwd. This file looks like this:

```
[root@linux root]# cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

...

kumarr:x:500:500::/home/kumarr:/bin/bash

...
```

You should have been able to decipher some of this file. It contains a one line entry for every account. The different fields in this line are separated by a colon (:). The first field is the login name of the user. This is the name by which the user will be known on the system. The second field simply contains an x when you are using a shadow password file. Because the file is readable by everybody, placing the password, even though encrypted, in the shadow file gives you added security. The /etc/shadow file is readable only by root. So an intruder will not be able to easily read even the encrypted password. Look at the shadow file entries for the accounts shown above:

```
[root@linux root]# cat /etc/shadow

root:$1$oFtzPwDL$sw6qnXSqCTZeo5doxfpis0:12554:0:99999:7:::

bin:*:12554:0:99999:7:::

daemon:*:12554:0:99999:7:::

...

kumarr:$1$8yVJnCdk$HtTL8AIRNrX9hLj6dq0Ir.:12704:0:99999:7:::
```

The first field is the user's login name followed by the encrypted password. It can be up to 34 characters long depending on the algorithm used. A * in the password field means a user cannot login using that name because it will not match any password. But the same effect can be achieved by locking the account using the -l option to the passwd command. This does not apply to the superuser because in his case the password check is not performed at all.

Coming back to the passwd file, the third field is the user identification number, or user id or uid. The linux operating system works in terms of the user id rather than the name for most purposes. Any user with an id of 0 is a superuser, and ids below 100 are usually reserved for the use of Linux. Ordinary users get ids from 100 onwards. Now we will discover an interesting fact. Suppose you login as an ordinary user, kumarr, who has a user id of 500. Create a file /home/kumarr/checking, logout and login as root, and look its long listing.

```
[root@linux root]# cd /home/kumarr

[root@linux root]# ls -l checking
```

```
-rw-rw-r--    1 kumarr   kumarr         665 Nov 29 21:13
checking
```

Now edit the passwd file carefully and change kumarr in the first field to smith. Look at the listing of the file checking again.

```
[root@linux root]# ls -l checking

-rw-rw-r--    1 smith   kumarr         665 Nov 29 21:13
checking
```

You will see that ls now reports smith as the owner. This shows that the ls command uses the passwd file to translate the user id to the user name. If you delete the account of kumarr by removing his entry in the passwd file, you will see

```
[root@linux root]# ls -l checking

-rw-rw-r--    1 500   500         665 Nov 29 21:13
checking
```

This is because now ls is not able to find out who the owner is and therefore reports the user id instead. Do put back kumarr's account under his own name now!

The fourth field is the group identification number or group id or gid. The file /etc/group contains the group names corresponding to the group ids, and also contains information on which users belong to which group. This file is also used by the ls command to translate group ids to group names, just as it does with user names. The fifth field is a comment field containing up to 30 characters. The sixth field gives the home directory of the account and thus determines where he will reach when he logs in. The last field gives the shell he will be presented with. If the command there is not executable, the user will not be able to log in. The default shell is /bin/sh, used when the field is empty.

Managing User Accounts

You now need to know as a system administrator how to add new user accounts, remove or inactivate them and change their characteristics. This is quite simply done in Linux. You need to go to the start button which is the red hat icon with an upward pointing arrow, usually to the left of your tray. Then choose the appropriate options as shown here.

```
Start -> System Settings -> Users and Groups
```

If you are not the superuser, you will be prompted to enter the superuser password. You then reach the Red Hat User Manager screen. Here you will see a list of user accounts. This does not include system related accounts. You have buttons to Add an account, at which you will have to enter the relevant information for the user such as his group and initial password. You also have an option to manage groups, where you can change the groups to which a user belongs.

To change the attributes of an account, you need to select it and click the Properties button. This brings up a User Properties screen where you have four tabs. Using these you can change all information about the user, including setting his password and changing the groups he belongs to.

You can also delete an account if you need to, or you can just lock it and disable access to the account by any ordinary user.

5.6 FILE SYSTEMS AND SPECIAL FILES

So far we have looked at two kinds of files, directories and ordinary files. Linux looks at everything as a file. So all hardware devices like terminals, tape drives, floppy drives, CD-ROM or DVD-ROM drives, printers and scanners are considered to be files in Linux. What this means is that there is a filename associated with each device and you can read from or write to these files just as you would to an ordinary file. There is a device driver in the kernel for every device supported and the name of the file for the device points to it within the system. Thus when you perform an operation on such a device special file the device driver takes over.

There are two kinds of special files, character and block special, which are associated with character oriented devices and block oriented devices respectively. A tape is a character oriented device while a hard disk can be both character or block oriented. Thus you will find that both kinds of special files exist for your hard disk on the system, but that there are only character special files for any tape drives. Actually there are also pipe special files but we will not consider them here.

The bridge between the physical device name (the filename) and the driver for the device is located in the `/dev` directory. Let us look at a long listing of this directory.

```
[root@linux root]# cd /dev

[root@linux root]# ls -l

total 228
crw-------   1 root   root     10,  10 Jan 30  2003 adbmouse
crw-r--r--   1 root   root     10, 175 Jan 30  2003 agpgart
crw-------   1 root   root     10,   4 Jan 30  2003 amigamouse
crw-------   1 root   root     10,   7 Jan 30  2003 amigamouse1
crw-------   1 milind root     10, 134 Jan 30  2003 apm_bios
drwxr-xr-x   2 root   root      4096 May 16  2004 ataraid
crw-------   1 root   root     10,   5 Jan 30  2003 atarimouse
crw-------   1 root   root     10,   3 Jan 30  2003 atibm
crw-------   1 root   root     10,   3 Jan 30  2003 atimouse
crw-------   1 milind root     14,   4 Jan 30  2003 audio
crw-------   1 milind root     14,  20 Jan 30  2003 audio1
```

and many more such lines. Your listing might look somewhat different in terms of the devices and other fields here. But let us look at some of the main features of this listing.

The first thing you must have noticed is that the first character of the permission modes is no longer a hyphen (-), but is `c` or `b`. This indicates whether the device file is character or block special. The other permission modes have their usual meanings, except that you cannot execute a device no matter how disgusting its behaviour might be! So execute permission has no significance here.

Instead of the file size, you find two numbers separated by a comma. These are called the major and minor device numbers. A major number stands for a class of

device like a terminal or a mouse, while the minor number gives the number of that kind of device. Thus different terminals might have minor device numbers 0 (for tty0), 1 (for tty1) and so on.

An entry for a device can be added by the `mknod` command. Suppose your terminal major device number is 4 and you have 32 entries in the /dev directory from 0 to 31. You will not be able to activate another terminal even if the driver can support it unless the device entry is made

```
[root@linux root]# cd /dev

[root@linux root]# /bin/mknod tty 32 c 4 32
```

The arguments to the command are the device name by which it will be known, the type (`c` for character and `b` for block) followed by the major and minor numbers. A device entry can be removed as usual with the rm command.

The `/dev` directory in Linux is itself organised into several directories like `/dev/raw` for the hard disk as a raw device, `/dev/ida` for the hard disk as a block device and so on. This is for convenience because of the large number of devices that are supported. You must remember that merely making a device entry is not enough. The Linux kernel must have support for that device. If you purchase a new device like a DVD-ROM it will come with a driver that you can install on your system. This will put the device driver for your device in the kernel so that you are able to use the device. The device entry is thus a link to the device driver for the device.

We will now look at hard disks and see how they are utilised in a Linux system. A file system is the complete hierarchy of directories and files starting from its root. A small device like a floppy diskette cannot hold many files but a large (80 GB) hard disk can easily hold several file systems. It is common to partition a large physical hard disk into several logical disks, on each of which a file system can then be created. This is done by the mkfs command. You have already seen about partitioning disks while installing Linux on your machine.

When you create a file system on a partition, you should use up all the space in the partition because otherwise the extra space is simply wasted. The device is named as a character device before the file system is made. When it has a file system on it, it is used as a block device. Although you could still read a disk with a file system as a character device, it would be very difficult for you to interpret the data stored on it unless you know intimately the structure imposed by the file system. Creating a file system is naturally done only in system maintenance mode.

What happens when a file system is created on a disk? The disk could previously be accessed only as a character device, but now a structure is imposed on this. You can now take advantage of the fact that you can access blocks on the disk randomly without having to go through all the previous blocks. So you can now look at the disk quickly. The file system structure consists of the boot block, the super block, the inodes and the data blocks.

The zeroeth block of every file system is reserved for storing booting information. It does not have any significance as far as the file system itself is concerned. It is the first block, called the super block, which contains information about the file system. Some of these items are the size of the file system, its name, the number of blocks kept apart for inodes, the list of inodes and the list of free blocks.

The index node or the inode blocks vary in number depending on the size of the file system and can actually be specified by the user while creating the file system. This number is the same as given in the super block. There is one inode for every file or directory in the file system and it contains information about the file such as the

number of links to the file, the permission modes and the block numbers occupied by the file. The first 10 such numbers are called direct blocks because they directly hold information about the data blocks. The eleventh number holds a block address and that block holds the addresses of the actual blocks. There are more levels of indirection available so that you can store very large files in your file system. You cannot have more files and directories in the file system than the number of inodes. The remaining blocks in the file system contain the actual data in the files.

When the computer is booted, these file systems are not immediately accessible to users. This is because each file system has to be attached to the main file system. To do this you have to use the mount command.

```
[root@linux root]# /bin/mount  /dev/hda4  /mnt
```

The first argument to the command is the device file associated with that file system. The second argument is the name of a directory. The mount command associates the logical device containing the file system with the directory. Now `/mnt` becomes the root of the directory hierarchy on the device. So if you had a directory called `khanz` on `/dev/hda4`, you can now access it as `/mnt/khanz`. The directory /mnt should preferably be empty before you mount some file system onto it, because while the file system is mounted you cannot access anything that was there on `/mnt` previously. To break the link between the file system and the directory say

```
[root@linux  root]#  /bin/umount  /dev/hda4
```

```
or simply
```

```
[root@linux  root]#  /bin/umount  /mnt
```

Now you can no longer get at the files in that file system. The various file systems are usually mounted automatically when the system reaches the multiuser state through commands in the `/etc/rc` shell script. If you issue the `mount` command by itself, it will list all the file systems currently mounted and the directories to which they are attached.

If somebody is working on a file system, it would be disastrous to unmount it because the file system would then become inconsistent when the device suddenly vanished. That is why you cannot unmount a file system unless no user or program is accessing it. The `umount` command will tell you that the device is busy and will not take any action.

In the booting process, a special root file system is mounted on the root directory (/). The major system directories like `bin`, etc and `dev` are under this directory. Since this file system is always in use, you cannot unmount or mount it yourself. All the other file systems that you mount are below / in the hierarchy, as you know. Sometimes `/tmp` is also mounted as a separate file system.

You have seen the intricate structure of the file system. This structure is subject to disruption due to many reasons. For example a block on the free list might also appear attached to a file, or a block might appear on neither. An inode might appear duplicated or a file might seem to be under no directory. Such situations potentially mean the loss of data. Fortunately the file system contains a fair amount of redundant information, and this enables a program to check whether it is consistent. If it is not, it is usually possible to repair the damage. The Linux system comes with a program called `/sbin/fsck` that performs a file system consistency check.

This program is run before mounting the various file systems because if the system is inconsistent to begin with it will get worse as users work on it. The `fsck` program looks for file systems to check in a file called `/etc/fstab`. Also, the fsck command is actually a front end to file system specific consistency check programs.

The file system check is not done every time the system reboots and is performed only if the system was shutdown abruptly leaving the file system in an inconsistent state. However after a certain number of reboots the check is forced anyway. The `ext3` file system that is the default in Linux allows journalling, which means that the check does not depend on the size of the file system but only on the size of the journal.

Every file system should contain a directory called `lost+found`, and this should be the first operation on it when the file system is made. Whenever `fsck` finds a file that is not linked to any directory, it places it in this directory. The program works in several phases and each phase performs some different check. You can set options to it that put it in interactive mode, where it expects a user response before taking any corrective action on a file system it is trying to repair.

Check Your Progress 2

1) Remove the device file for a terminal and see what happens. Also try renaming the file and see the consequences.

.....

2) Add a blank line to the beginning of the password file. What happens? What if there is a blank line in the middle?

.....

3) Try umounting a file system when users are working on it. What happens and why?

.....

5.7 BACKUPS AND RESTORATION

At a large installation, users do not usually have their own backups and the system administrator is responsible for the integrity of the system. On smaller installations and certainly on your own personal computer, you will be responsible for your own data and program files. So it is useful for every user to be able to backup data and know how to restore it if needed. As a computer professional you do not need to be told how important backups are.

There can be many different backup strategies and tools that you can use. We can classify backups into full backups, incremental backups and differential backups. A full backup is a complete backup of an installation or a part of its file system. If there is a complete crash, you can restore user data from this. But the operating system configuration files are also something that one produces over a period of time and with considerable effort. So you can consider a backup scheme for them as well. How often you should take backups depends on how much you are prepared to lose.

A full backup is easy to restore from, but given the large disk capacities of today, the amount of time taken to make a full backup can be non-trivial. So you can think of a full backup at periodic intervals with daily or more frequent incremental backups, where only files that have changed since the last backup are copied. But it can be difficult to locate a needed file in an incremental backup, so the concept of differential backups was introduced. Here you backup all files that have changed since the last

full backup. So the amount of backing up required is in between that of a full backup and an incremental backup.

It is important to consider what tne backup media should be as well. Very often it is a tape of some kind, but a USB disk or a network backup to a data centre can also be considered. You have to look at the reliability of a backup and make sure that you do not use media beyond their useful life. A backup is pointless if you cannot restore from it when you need to. So make sure to test your backups periodically. You cannot afford a single failure in a backup. You can also consider taking multiple backups each time.

Depending on the criticality of your business, you might keep different copies of your backup at different locations. But whatever your company characteristics, you have to make sure you have at least one backup offsite that is geographically sufficiently distant from your site.

There are several different kinds of backup tools. Some are sophisticated commercial offerings while at the other end you have the basic Linux commands such as tar and cpio. Both of them work quite well and you can decide what you will use.

The tar command allows you to take a backup of all or selected files in a directory hierarchy onto tape, floppy disk or the hard disk itself. Tar knows about directories and links, and maintains headers, checksums and file permissions and owners. To take a backup of all files under /home/khanz

```
[khanz@linux khanz]$ tar cvbf 40/dev/rmt0/home/khanz
```

Let us look at the meanings of the various letters after the `tar` command. The c stands for create, and it causes tar to create the backup. Remember that anything previously present on the backup medium gets erased thereby (unless it is a file on the hard disk). The v is the verbose option of `tar`, and makes it chatter about what it is backing up. The `b` is the blocking factor and defaults to 20. You then specify the file or backup medium where the backup is to be taken followed by the directories to backup at the end. Everything under the directories you mention is backed up. You can also specify individual files if you want to.

To look at the contents of a `tar file`, you can use the `t` option.

```
[khanz@linux khanz]$ tar tvf /dev/rmt0
```

For extracting, you use the x option. One thing you should be careful about is the use of absolute pathnames during the backing up. When you restore from such a backup, it will restore to that same pathname. So it might be better to use relative pathnames while creating a backup archive as you have the liberty of placing it wherever you want while restoring.

You can also use the z option to compress the archive, thereby saving a fair amount of space. The extent of the saving will depend on the kind of files that are being backed up.

Another useful command for creating and restoring from archives is `cpio`. It reads the list of files from the standard output and copies them to wherever you specify. For generating the list of filenames, you can use a program like find.

```
[khanz@linux khanz]$ find/home/khanz/|cpio-o>/dev/rmt0
```

You can use the many options of the find command to choose files that satisfy specific conditions so that only those files are backed up.

Check Your Progress 3

1) You have backed up a directory containing several files onto 12 floppies using tar. When you try to restore these after a crash, the 4th floppy is found to be corrupted. How much data do you lose?

.....

2) Why is it useful to take differential backups?

.....

5.8 SUMMARY

This has again been a long unit wherein we have tried to cover a lot of ground in a very small amount of space. You saw what the responsibilities of a system administrator were and how the exact composition of such a group depends on the organization characteristics. The major topic of this chapter was Linux installation and you saw how to perform a simple Linux installation on a machine. You also were introduced to file systems and how the system was booted, with some idea of run levels. As a system administrator, you would need to maintain user accounts and you saw how to add, delete or change user account information including their passwords. Finally we briefly looked at the important topic of taking backups and restoring from them using the `tar` command.

This block would now have given you a fair idea of the Linux operating system and its capabilities. It should have prepared you to read up the large amount of documentation available on the subject and to explore the various resources devoted to Linux on the Internet.

5.9 SOLUTIONS/ANSWERS

Check Your Progress 1

1) Try yourself

2) Try yourself

3) Try yourself

Check Your Progress 2

1) Try yourself

2) Try yourself

3) Try yourself

Check Your Progress 3

1) You will lose data from the 4th floppy onwards.

2) These allow us to save space that would be wasted by taking a complete backup every time. At the same time you do not have to puzzle over which incremental backup has a copy of the files you want to restore.

5.10 FURTHER READING

There are a host of resources available for further reading on the subject of Red Hat Linux version 9.0.

1) http://www.redhat.com/docs/manuals/linux

2) http://www.linux.org gives among other information, a list of good books on Red Hat Linux.

3) Consider joining a good linux mailing list.