Agustin’s Linux manual

By Agustin Velasco

Agustín's Linux Manual

System Administration

Volume 2

ISBN: 0-9752804-1-4

Written and assembled by:
Agustin Velasco

Published by:
Vegaslocal.com

About the author

Agustin Velasco has over 15 years of experience in computers and electronics. Throughout the years he has earned a career in the technology arena, specializing in computer security and Data recovery.
By the end of 1995, he had an opportunity, and worked for a subdivision of Acer America, where he spent four years developing his skills in computer technology. Thereafter he was self employed, deploying networks and applying security at large scale. As a security specialist, he saw the need and mastered a technique in data manipulation which now he can use to recover lost or erased data from a variety of platforms.

As Linux became popular on the market, he started to experiment with it, and found that Linux is a highly reliable operating system. He started working with various Linux distributions including Slackware and Debian. Realizing that the end user might have problems working with some distributions, he started working with other more friendly packages. Soon after, he developed a technique based upon the Mandrake distribution.

He is currently an active supporter of the open source movement. Due to the lack of technical reference for the end users, he decided to write Agustin's Linux Manual "the series". Because of this documentation he receives the respect of the Linux community. On a day to day basis, Agustin's Linux Manual is used among top IT professionals and is now reaching educational institutions. Agustin currently participates in various forums, including chat rooms, where he answers questions related to the Linux Operating system.
Agustin is currently holding a position as technical director at www.netcontrol.org and is author of the second edition of these series based on Mandrake 10 Community Edition.

The purpose of this series and why it was written

This book has been written to help all of those who are interested in learning, are open minded and loves freedom. The book is written especially to assist educational institutions to teach people who have zero knowledge of Linux and perhaps for those who can not afford the pricy schooling but want to become a well respected system administrator.

The book takes one step by step from installation to system administration. It teaches how to set up Apache web server, Bind DNS server, Postfix email servers, Samba server and of course security. It gives you details on how to close unnecessary ports. It covers configuration on the Squid proxy server and demonstrates many of the available utilities that will assist you in system administration

Dedication

For my wife Amelia and my two kids Caroline and Kevin. I am really happy for having such a wonderful family, my wife for understanding and supporting me with all of my crazy ideas and my kids for not bothering me when I am writing or working on projects at home.

And last but not least to all of those who struggle in life to have an education, but never give up to demonstrate their abilities of accomplishing something. I myself have witnessed people without a degree who have accomplished the most wonderful skills but because a lack of a degree they have been put out of the practical field.

Acknowledgement

I'd like to thank my friend Anthony Whitaker (who lives in the shadows and wishes to remain anonymous); an idea man who undoubtedly could make any company number one and has been so helpful in the process of this book. Without his support this book wouldn't be completed. Anthony has a wide experience in the field of computers which made him a perfect person to review this book as an end user.

Content

Chapter 3

Chapter 4

Chapter 3

Administration

The most wonderful thing about any operating system is administration. No system is secure and no system is reliable if there is no administration at all. And the worse comes when a wonderful system like Linux is being managed and maintained by a clueless system administrator. The administrator is a hacker, and must know what he/she is working with.

Please do not confuse hackers with crackers or script kiddies.

The best, well-respected hackers are good system administrators who spent their entire lives deploying and protecting systems. These are people who know about real securities such as Network Detection Systems, Network IDS, Finger Printing, etc. Most crackers and script kiddies only know how to destroy systems. Fakers know how to scan for open ports, launch some Distributed Denial of Service (DDOS), and call themselves hackers. What is worse is that the news media confuse them as hackers.

Of course there are exceptions. Sometimes security professionals turn into criminals. Believe me some of them cannot even pay their bills or feed their families because employers rarely value real skills.
Employers say, "I am sorry you are over qualified; or, it seems that you are very unstable, you had more than four jobs during the past two years". Professionals should be respected and paid for what they know or can do.

Oh! Make note that when I say, "professionals", I am not referring to those who hold a degree or PHD. I am referring to those who struggle every night to offer something to the community and say, "Hey people I discovered last night that the OS Ver. Xx has a security bridge… here's how to fix it". See, you don't need a degree to say how things are done.
Many people forget that a lot of the most skillful professionals did not have enough money to get enrolled in a college or university. And some of those lucky enough to go through certification programs are still waiting for an opportunity for an entry-level position.

Employers look at their resumes and tell them, "I am sorry I can't hire you because you don't have experience". This person can have control of an entire company's network within three minutes.

Think about it, a computer technician now earns around $7.00 an hour. Why should one work as a computer technician? One can earn $7.00 an hour working at a fast food Restaurant. Most people that are interested in computers don't stop with basic technical skills.

What you see next is for those persons who want to be the best. If you want to be the best, read on. If you want a certificate, print one. It holds just as much value.

Note to employers: Don't ask for a certification from a real I.T. professional. Most real ones don't have one. Instead, test them and pay them for the time they are there.

Welcome to system administration

It is very important that you learn where files are located. You probably will be doing some administration in the near future. If you are a technical person, you have to know your stuff. I am sure you don't want to look clueless when a supervisor asks you, "How I do this". If he appreciates your work, you will be compensated for your knowledge.

Did you know that you *could* use Linux without knowing anything about the shell? You can boot your system directly into X and do all kinds of administration from there. You can use the Mandrake Control Center, Webmin and Linuxconf to administer every aspect of your system.

Some people don't like to use console text modes, but others loves it. Believe me you can't say you are a Linux user without knowing how to use the console. Yeah, yeah… the GUI is great and looks nice, etc. Serious users must know how to use the shell.

You must have to know all these amazing things that you can do with the console. In the shell console you can accomplish very highly complex tasks because UNIX isn't just a simple command interpreter; instead it is a highly flexible programming environment.

Terminals

UNIX has been an operating system running on a wide variety of machines interconnected with other machines called terminals (dumb terminals) consisting of keyboards, and monitors interconnected to the central computer. Users at these terminals were basically teletyping, using string 'tty' for terminal device files.

There were no standards that comply with the requirements and every brand had its own "specs" such as its own keyboard, its own display, its own ideas in the signal transmission and reception, characters control codes and so on.

Linux terminals mostly use either 'vt100' or 'Linux' as their terminal type. In order to clean up the mess, a central file was created, the termcap '/etc/termcap'.

Xterms

In the early 90s the XFree86 was fine tuned and soon ported to Intel-based UNIX clones like FreeBSD, NetBSD or Linux. X has the capability of running multiple 'virtual' terminals. X even came with such an application, 'xterm'. Therefore you'll find that 'xterm' and 'virtual terminal' are often used.

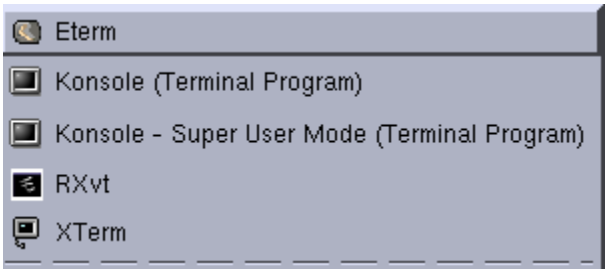


Fig. 3.1

Shells

The shell is part of the operating system (kernel), which translates the input/output (IO), allowing the user to communicate with the system by using commands. The first UNIX shell (sh) was written by Steve Bourne, and is called the 'Bourne shell. Many others shells were developed based on the original Bourne Shell. Linux's standard shell is 'bash', the GNU Bourne.

Command aliases

This table describes some aliases that you can use when executing commands. I though to present it here before you actually start working in the console

Alias	commands	Description
cd..	executes 'cd ..'	go to parent directory
d	executes 'ls'	list directory
l	executes 'ls'	list directory
la	executes 'ls -a'	list complete directory, i.e. including files starting with a dot
ll	executes 'ls -l -k'	list directory in long format, i.e. with file attributes, print file size in KB and not in bytes
ls	executes 'ls -F --color=auto'	list directories, append file type indicators and use colors
lsd	executes 'ls -d */'	list subdirectories only, no files
md	executes 'mkdir'	create directory
p	executes 'cd -'	go back to previous directory
rd	executes 'rmdir'	delete (empty) directory
s	executes 'cd ..'	go to parent directory
used	executes 'du -sm * | sort -n'	display disk usage of subdirectories in MB, list by size

Table 3.1

Note. *The **tab** key is also used as shortcut, when typing a command and some of the first characters of a file name – hit the tab key and the file name will be auto completed.*

Command basics

Do not use the shell as 'root' for everyday tasks…

When you log in as user you are automatically placed inside your home directory */home/user*

Look at your command prompt it tells you where you are. The following command demonstrates your profile, your desktop, your document folder, your mail folder and the temp directory.

```
[agustin@server2 agustin]$ ls
Desktop/  Documents/ mail/ temp/
```

Try the next command lists everything that is inside the folder Desktop.

```
[agustin@server2 agustin]$ ls Desktop
befdsr41w_eng_ds.pdf      xvnc.html      myfolder/
trash/ Home.desktop       Mandrake Expert.desktop Removable media/
```

That command is also similar as: cd Desktop

```
[agustin@server2 agustin]$ cd Desktop
[agustin@server2 Desktop]$ls
befdsr41w_eng_ds.pdf      xvnc.html      myfolder/
trash/ Home.desktop             Mandrake Expert.desktop Removable media/
```

The next command is: cd.. Takes you one step back.

```
[agustin@server2 Desktop]$cd..
[agustin@server2 agustin]$
```

The root Directory

Command ls / this command lists the root directory

```
[agustin@server2 agustin]$ ls /
      bin/  boot/ dev/  etc/  home/      initrd/      lib/   mnt/  opt/
      proc/ root/ sbin/ tmp/ usr/  var/
```

Throughout the decade, developers had tried to define standards for the file system hierarchy and for what each of these directories should be used for. But even with the efforts of all these people there are still variations among all distributions.

/	root directory of the entire system
/bin	holds system executables
/sbin	holds system executables and are essential for starting up the system
/boot	holds the files needed during the booting process including the kernel
/dev	it is a special directory that holds information regarding peripherals /dev/ttys0, /dev/had, etc.
/home	holds all the home directories for all users except root
/lib	holds system binary libraries, shared libraries and kernel module
/opt	here is where optional applications might go
/root	this is the home directory for super user, do not confuse this folder with **/**
/tmp	Here is where temporary files are stored; it is usually emptied when systems restart.
/var	is where variable system files go, system logging, file locks, printer Spooling, mail spooling and many others.
/etc	This directory holds almost all configuration files. As administrator you will spending most of your time tweaking settings in this folder.
/initrd	this directory is used at boot time, in the initrd to perform pivot_root
/mnt	This directory is used as a mount point. Here you can temporarily mount medias such as CD-ROM, zip and other file systems. Example: /mnt/windows, /mnt/floppy, mnt/cd-rom

/proc	this directory is used as a kernel information access hooks, example of usage:
	`[agustin@server2 proc]$cat cpuinfo`
	`[agustin@server2 agustin]$cat filesystems`

/usr	It is a very large directory, holds application programs; it also has several important additional directories.
/usr/bin	contains binaries executables
/usr/include	This directory contains C headers with various libraries applications.
/usr/local	application programs used locally

The Print working directory command: pwd

```
      [agustin@server2 agustin]$ pwd
      /home/agustin
      [agustin@server2 agustin]$
```

The command whoami, displays who you are at the current prompt

```
[agustin@server2 agustin]$ whoami
agustin

[agustin@server2 agustin]$
```

If you want to know who is logged into the entire system use the who command

```
[agustin@server2 agustin]$ who
agustin      vc/1  Aug 17 07:38
root         vc/2  Aug 19 06:51
user1        vc/3  Aug 19 06:46

[agustin@server2 agustin]$
```

Switching from regular user to root
To gain root's power temporarily use: su

```
[agustin@server2 agustin]$ su
Password:*******      (when you  are typing the password, you can not  see it)

[root@server2 agustin]# whoami
root

[root@server2 agustin]#
```

Observe your prompt, it has been changed. When you are in this mode you can do anything; be careful how you use the super user account. Protect the root account at all cost.

The root account is strictly used for system administration. Any regular user cannot do things that are strictly for root unless root grants the right to the user.

Executing commands as root

Let's have some fun with root so you can see what root can do. We are going to be writing in a home account named user1

```
[root@server2 agustin]# cd /home/user1
```

Create a directory using: mkdir

```
[root@server2 user1]# mkdir collections
```

Change to directory collections

```
[root@server2 user1]#cd collections
[root@server2 collections]#
```

So far we created a directory called collections, we moved into it and now **collections** is our current working directory. You can send data to a file or device on the fly by using the **echo** command**.**

```
[root@server2 collections]#echo paste this information to a file > myfile
```

So how do you know the information has been sent to **myfile**

The cat command

```
[root@server2 collections]#cat myfile
paste this information to a file
```

```
[root@server2 collections]#
```

At this point, you should have a file in your collections directory, **create another directory**

```
[root@server2 collections]# mkdir onother
[root@server2 collections]#ls
afile   file2    myfile onother/

[root@server2 collections]#
```

We can easily make a back up of a file inside our current directory; this is useful when you need to edit a file. For security reasons always backup a file when you need to edit it.

The copy command: cp

```
[root@server2 collections]#cp myfile original.myfile
[root@server2 collections]#
```

To view the content of a directory with details, we just add some switches to our ls command.

```
[root@server2 collections]#ls –l
total
-rw-r--r--      1 root      root        6       Aug 17        09:09 afile
-rw-r--r--      1 root      root        27      Aug 17        09:46 file2
-rw-r--  r--    1 root      root        14      Aug 17        09:46 myfile
drwxr-xr-x      2 root      root        4096     Aug 17       10:34 another/
-rw-r—r--       1 root      root        14      Aug 17        10:46 original.myfile

[root@server2 collections]#
```

These parameters are useful when digging inside directories. There are many others that you may want to look at. –l –R –n – I –a –all

```
[root@server2 collections]#man ls
```

Use **man ls** to read the manual and look at all the switches available to the command. Use the up and down arrow to scroll the manual page and press "q" to exit the manual.

File specs

Let's give a quick look at the following listing

```
[root@server2 collections]#ls –l
total
```

-rw-r--r--	1 root	root	6	Aug 17	09:09 afile
-rw-r--r--	1 root	root	27	Aug 17	09:46 file2
-rw-r-- r--	1 root	root	14	Aug 17	09:46 myfile
drwxr-xr-x	2 root	root	4096	Aug 17	10:34 another/
-rw-r—r--	1 root	root	14	Aug 17	10:46 original.myfile

```
[root@server2 collections]#
```

As you can see on the ls output, it gives you details of who owns the file, types of file and so on.

On the first column **–rw-r--r--** **drwxr-xr-x** these letters represent the rights on the files.

r read
w write
x execute
d means it is a directory

You can also see a column **1 root** it means that belongs to root. The third column **root** means **group root**. On the very right column it shows the date and hour when it was created. Because of that fact, those files belong to root; only root can modify them. To prove this theory, **exit the super user mode** go into your user's home directory and subdirectory collections.

Try to backup a file, use the cp command

```
[user1@server2 collections]$cp file2 file3
cp: can not create regular file 'file3': Permission denied
[user1@server2 collections]$
```

Now you can see how neat this is, you cannot do anything to those files even though it is sitting in a regular user's home directory because root has ownership of those files.

Try to remove the file using the remove command: rm

```
 [user1@server2 collections]$ rm afile
rm: remove write-protected regular file 'afile'? y
rm: can not remove 'afile': Permission denied

[user1@server2 collections]$
```

See you cannot even remove the file or work at all in the directory collections. When the directory collection was created by root, it inherited its permission to all files and subdirectories. Only root can change the permission to these files and probably grant some permission to other users.
Now if you go one step up in your home directory, there you can write, delete or remove.

File permission with chmod

The `chmod` command is used to give and set file permissions

Syntax

`Chmod [permissions] filenames`

Permissions: Specifies what rights are you granting

Filenames: File or directory to which you are assigning the permissions.

When you start granting permissions, you might opt for any of the following options: letters or numerical (I prefer numerical).

Permissions that you can grant:

By letter		Numerical	
U	User who owns the file	400	Read by owner
g	group that owns the file	040	Read by group

o	Other	004	Read by others
a	All	200	Write by owner
r	Readable file	020	Write by group
w	Writeable file	002	Write by others
x	Executable file	100	Execute by owner
		010	Execute by group
		001	Execute by others

Table 3.2

There is something else that we need to understand before we can actually give permissions. First we have to know what type of permissions we are granting, and to whom it will be granted.

User IDS and Group IDS UID/GID

Under the UNIX operating system, every user is member of a group by default when you create a new user that user is member of its own group or member of users. The administrator can make specific users be part of any other group. Keep in mind that when the system executes or does something under a user name, that system does not actually see that user name, instead it sees just a user ID.

- A user ID stands as a number
- A user name stands as a string and it is associated to the ID number

This is exactly the same for groups:

- A group ID is a number
- A group name is a string associated to the group ID number.

How permissions are assigned?

The basic format of chmod is: **chmod** xyz file
The xyz represent value that goes from 0-7; each number represents permissions in a group.

For instance:

x would be **for the owner** of the file
y would be **for the group** that owns the file(group the user belongs to)

z would be **for everybody**
file **name of the file being modified**

Refer to the following table for a better understanding

Number	Permissions
0	None = can not read, write or execute
1	Can execute, but can not read or write
2	Write only, can not read or execute
3	Can write, can execute
4	Read only, can not write to or execute
5	Read only, executable, can not write to
6	Writeable, readable file, but not executable
7	Readable, writeable and executable file

Table 3.3

There are several ways to give permission to a file as you could see on the last two tables. You could basically use any part of the table to assign these permissions.

Example
I will use the numerical part of the first table to assign permission to an html file that can be viewed over the Internet.

```
[root@server2 collections]#chmod 644 internal.html
```

How I determined that? I simply added 400+200+40+4 = 644 from table 3.2

- Read by owner
- Write by owner
- Read by group
- Read by others

If I do an ls –l that would look like this:

```
[root@server2 collections]#ls -l
total
-rw-r--r--  1 root   root  6    Aug    17   09:09   afile
-rw-r--r--  1 root   root  19  Aug    18   12:47 internal.html
[root@server2 collections]#
```

What would happen if I make that writeable by others (I would be a dumb administrator), but for demonstration purposes lest make that file writeable by others.

```
[root@server2 collections]# chmod 646 internal.html
```
Now I do an: **ls –l**

```
[root@server2 collections]#ls -l
total
-rw-r--r--  1 root  root    6   Aug   17   09:09   afile
-rw-r--rw-  1 root          root     19   Aug 18 12:47 internal.html

[root@server2 collections]#
```

Now internal.html is world writeable…be careful how you assign permissions. Normally, don't leave a file as 777 (that is full access to the file), anyone can replace or delete it.

Change ownership chown

As I already mentioned earlier, the owner is the file's creator; therefore, the file is owned by a user and the user is owned by a group. This basically means the file is also owned by the group. A regular user is not able to take ownership of a file created by a different user, but the administrator (root) can and there after can reassign permissions.

This is much simpler; all you have to do is be root

```
[root@server2 collections]# chown user1 afile
[root@server2 collections]#ls -l
total
rw-r--r--       1 user1      root      6         Aug 17                09:09 afile
-rw-r--r--      1 root       root      27        Aug 17                09:46 file2
-rw-r--  r--    1 root       root      14        Aug 17                09:46 myfile
drwxr-xr-x      2 root       root      4096      Aug 17                10:34 another/

[root@server2 collections]#
```

As you can see the new owner now is **user1**, even though user1 belongs to group root.

How can you change the group?

Look at the following example

I will add user1 to **group user1:**

```
root@server2 collections]#chown user1.user1 afile
```

Now I will do the ls –l

```
[root@server2 collections]#ls –l
total
rw-r--r--      1 user1    user1    6       Aug 17          09:09 afile
-rw-r--r--     1 root     root     27      Aug 17          09:46 file2
-rw-r--  r--   1 root     root     14      Aug 17          09:46 myfile
drwxr-xr-x     2 root     root     4096    Aug 17          10:34 another/

[root@server2 collections]#
```

Now **afile** belongs to User1, User1 can now do anything to the file.

Note: *An owner can be from any group, and still can have full control of the specified file if proper permission is granted.*

Running multiple commands

When you become more familiar with the command line, you probably will need to run multiple commands. The shell let's you insert special queuing characters between commands. Here is how it is done.

```
[user1@server2 collections]$ command1 ; command2
```

The command is executed in the order it was written, but command 2 is executed even if there was an error in command 1.

```
[user1@server2 collections]$ command1 && command2
```

The command *command2* is executed only if *command1* was successful, no errors.

Note. *You can write more than just two commands…*

Multiple Virtual Terminals

Now if you really want to get fancy and execute all that you have learned…you can work on several virtual terminals or consoles. For example you might want to leave one process running in one terminal while you keep working in a different one. These terminals are called **/tty1 through /tty7**.

Your graphical interface normally runs on terminal seven also known as vt7 even though you are logged into a tty#.

When you execute `startx` you are automatically ported to **vt7.** By pressing the combination **ATL** key and any of the **F1 through F7,** you are switched to a different terminal, no matter if you are on your desktop.

If you are on a terminal, and you are also running the graphical interface, you can get back to your desktop by pressing, **ALT & F7**.

All commands you have been typing so far are **running in terminal mode**, which means that if you close the terminal, all the processes under that term are terminated.
However on the same terminal you can run commands in the background and release the terminal for a new task.

So this is how it is done, all you have to do is place **&** right after command:

```
[user1@server2 user1]$Command &
```

To see which jobs have been sent to the background, type jobs at the prompt.

```
[user1@server2 user1]$ jobs
[1]+ Running application &
```

Keep in mind that some commands requires super user in order to run.

Killing Processes

Sometimes it is very necessary to terminate a process. A **process** is the job being executed by an application and is identified by a number called **pid**. In order to kill a process you have to be **root** or **super-user.**

```
[root@server2 agustin]# ps –aux
```

That command will display all the running processes.

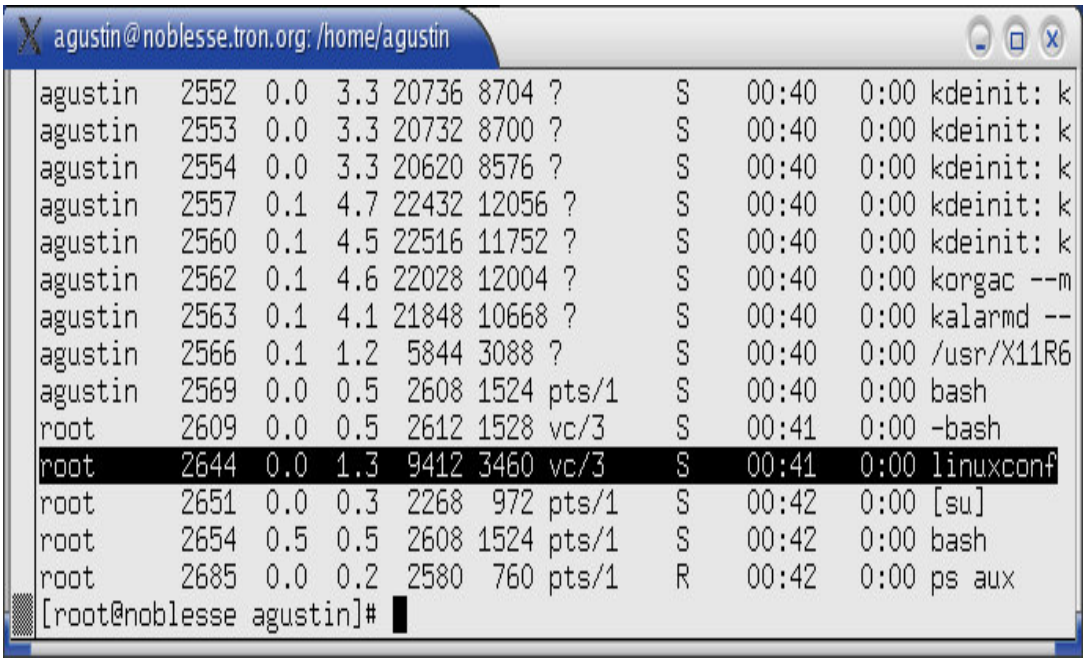


Fig. 3.2

It is not difficult to identify the processes. Search through the output of your command and find the PID number. The PID is the process number of your running application.

To kill the application, execute the following:

```
[root@server2 Agustin]# kill 2644 (This command would kill linuxconf, fig 3.2)
```

The kill command is very useful when you have a non-responding application. Another way of finding the process is searching by name of the application.

```
[root@server2 agustin]# pidof Xvnc
8613
```

Now kill the process:

```
root@server2 agustin]# kill 8613
```

Very simple…

Bash configuration files

The bash controls some special files, which are part of every user's profile. These files are sitting right in your home directory.

```
[agustin@server2 agustin]$ ls .bash*
```

File name	Description
.bash_history	Keeps a list of the commands you have been typing
.bash_logout	A list of auto run commands to be executed when you leave the shell,
.bash_profile	A list of commands to be executed when you log in.
.bashrc	contains a list of commands that is executed every time you open a new shell

Table 3.4

Changing the prompt

This is not so important it is just a matter of personal taste. Here I will demonstrate how to modify the prompt. This modification is for general users, and the file to be modified is `/etc/bashrc`

```
[root@server2 agustin]# vi /etc/bashrc
```

```
1 # /etc/bashrc
2
3 # System wide functions and aliases
4 # Environment stuff goes in /etc/profile
5
6 # by default, we want this to get set.
7 # Even for non-interactive, non-login shells.
8 if [ `id -gn` = `id -un` -a `id -u` -gt 99 ]; then
9     umask 002
10 else
11    umask 022
12 fi
13
14 # are we an interactive shell?
15 if [ "$PS1" ]; then
16    case $TERM in
17    xterm*)
18        PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
19        ;;
20    *)
```

```
21        ;;
22    esac
23 #    [ "$PS1" = "\\s-\\v\\$ " ] && PS1="[\u@\h \W]\\$ "
24
25    [ "$PS1" = "\\s-\\v\\$ " ] && PS1="\[\e[1;32m\] \w\\$\[\e[1;37m\]"
26
27    if [ -z "$loginsh" ]; then # We're not a login shell
28        for i in /etc/profile.d/*.sh; do
29        if [ -x $i ]; then
30            . $i
31        fi
32    done
33    fi
34 fi
35
36 unset loginsh
```

Comment line 23 and add line 25.

- Press **ESC**
- Type the colon "**:**"
- Type **wq**

The next time you login your prompt will look like this:

For root: ~#
For users: ~$

Setting number to vi editor

There is something that I consider important. Whenever I edit something I want to make it easy to debug. So, I edit the `vimrc` to set numbers to each line.

Note: *this file is sitting under root's directory and it applies to root's profile..*

```
# vi /root/.vimrc
```

In the third or fourth line add **`set number`**

- Press **ESC**
- Type the colon "**:**"
- Type **wq**

From now on when you edit something as root, it will be numbered.

Note. *When you edit something and you made changes but don't want to save it, you can ignore it by quitting without saving.*

When you use

- Press **ESC**
- Type the colon "**:**"
- Type **q**

In case it gives you an error.

- Type **q!** instead

Creating path environment

The **$path** works like a variable that can hold any information. In this case it will hold an exact route to get to a specific directory. When it is executed, the system will remember it. The system itself has all kind of variables many are defined in the shell's configuration files and are part of any users profile including root defined in /etc.

For example **X** has variables of its own set by the start-up files of the windows manager.

This is how it is used:

```
PATH=/usr/bin:/bin:/usr/local/bin:/usr/X11R6/bin

PATH=$PATH:/some/directory
```

When you define a *local* environment it is restricted to the terminal you defined it to; however you can export it to any terminal you like or make it global to all terminals.

```
export PATH=$PATH:/some/directory
```

Once you have exported to a directory; you can now set it permanently to your $PATH, just add the 'export' command line to your '**.bash_profile**'.

Writing and executing bash shell script

When the time comes and you have the need of writing automated tasks the answer is scripts. Under UNIX, scripts are executable batch files. The bash shell has the power of writing and executing large complicated programs. If you have created batch files under dos, then scripts will be very simple to understand.

Let's write a simple program so you can understand the basics.

- Create a directory under your regular username, in your Documents folder
- Call it myscript
- Change to myscript

```
[user1@server2 Documents]$mkdir myscript
[user1@server2 Documents]$cd myscript
[user1@server2 myscript]$
```

At this point I am going to edit a file named **hello**, using my favorite editor… Linux comes with many editors including vim, emacs. You can use any editor that you wish. Just save it as a plain text when you finish (files have no extensions under Unix). Under Linux, extensions are not used; instead, there is a reference bit to each file that accomplishes the task. Following this rule you can name the file whatever you want. If you choose an editor and it is not installed, don't worry, it is very easy to install.

If you need any application that runs under Linux (before you waste your time looking it up on the Internet), I suggest you first look in the installation CDs. If you don't know how to install it, jump to the package manager (software installation in chapter 4)

Start the editor…

```
[user1@server2 myscript]$vi hello
```

Press the insert key
Start typing the following:

```
#! /bin/bash
echo "\"Hello I am a little program\""
echo "I am in the directory:"
echo
pwd
echo
echo 'do an ls -l'
ls -l
echo
echo
```

When finished typing, press the Esc key
Use the shift key to type the colon (:)
Pres the w & q keys (*write and quit)*
Your last line should look:
:wq
Press enter

You should be back to your prompt

```
[user1@server2 myscript]$
```

Type `ls -l hello` file should be in your **myscript** directory

Programs are normally run by typing their names some may require special options.
Try:

```
[user1@server2 myscript]$hello  -bash: hello: command not found
[user1@server2 myscript]$
```

The bash shell responded that it couldn't find the file hello. I then specify bash to look in the current directory:

```
[user1@server2 myscript]$./hello      -bash: ./hello: Permission denied
[user1@server2 myscript]$
```

Now it found it, but it does not have permission to execute it. So, in order to make the hello file an executable, I will have to give it the executable permission.

```
[user1@server2 myscript]$ chmod 745 hello
```

- Read by owner
- Write by owner
- Execute/search by owner
- Read by group
- Read by others
- Execute/search by others

If you execute ls –l, you should see the hello file turned green.

Try to run it now:

```
[user1@server2 myscript]$ ./hello
"Hello I am a little program"
I am in the directory:

/home/user1/Documents/myscript
```

do ls –l

Total 4
-rwxr—r-x 1 user1 user1 141 Aug 19 00:53 hello

```
[user1@server2 myscript]$
```

Sometimes it is a good idea to automate tasks, scripts becomes handy once you get to know the system. I suggest you get a book focused on shell programming.

The midnight commander

The midnight commander is a server network file management system; this server allows you manipulate files on a remote machine as if they were local. But of course this is only possible if the server is running.

In this section I will show you how to use midnight commander locally. Probably most of your administration will be done here if you decide to go this way. As a regular user, you can only use midnight commander to manage files in your home directory. If you need to do administration globally you need to run **mc** as root.

Become a super user and type (mc) on your command prompt.

```
[user1@server2 user1]$su
Password:**********
[root@server2 user1]#mc
```

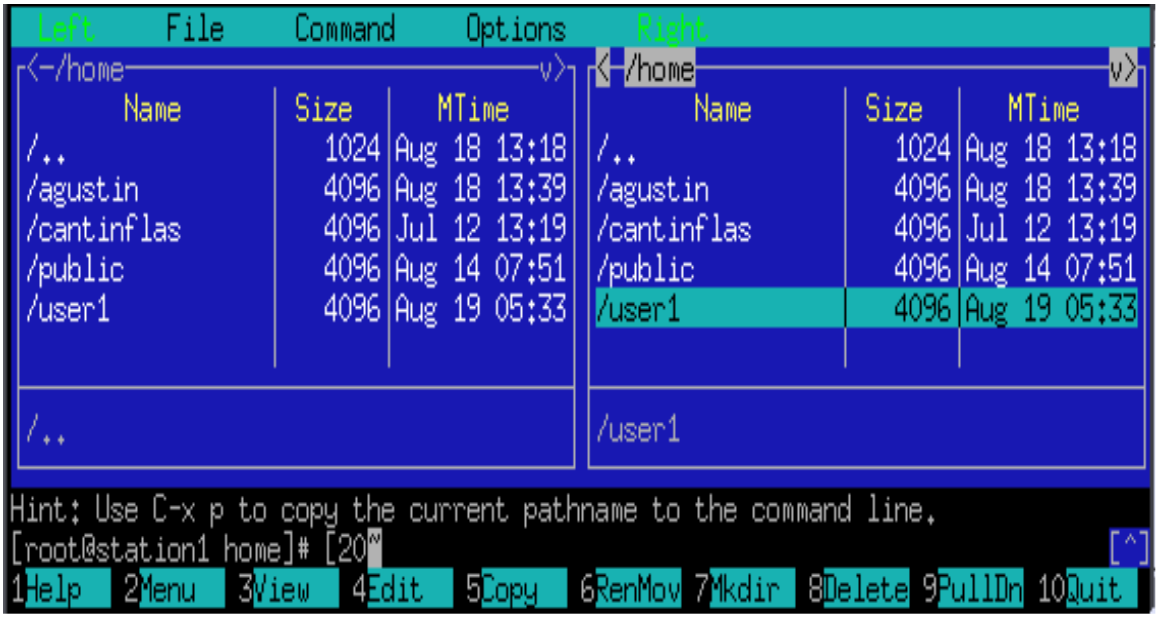


Fig. 3.2

This is the midnight commander console, it may not be exotic; but I bet you it will become a lifesaver. Observe the console screen. It has two panels **left** and **right**. You can move between panels by pressing the tab key.
To scroll inside the panel use the **up** and down arrow.

Copying File with mc

To copy files from one directory to another, you can select the directory from one panel (source), and make the destination into another panel. You can select single files or a whole directory.

Make sure you know where the destination is. Select the destination directory (when selected press **enter**) it opens and display its content. Select the file to copy. When ready to copy, press F5.

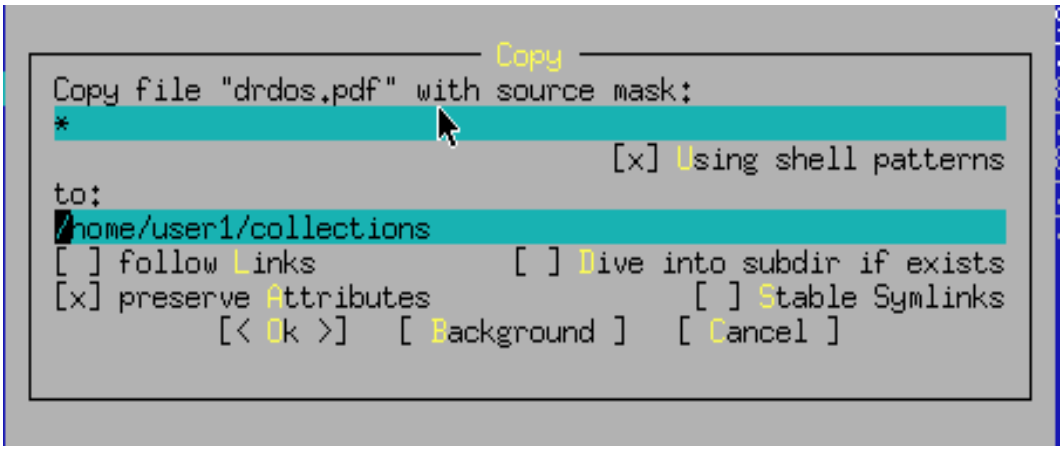


Fig. 3.3

If it is a single file that is being copied, just use the **tab key** to move on **OK** and hit **enter. If you were copying a directory with files and subdirectories, then you would mark the option [X] Dive into subdir if exist.**

MC's F commands

At the bottom of fig. 3.2, you can see a command line prompt; you can execute commands from here. At the very bottom are other options; these are the F1 through F10 commands.

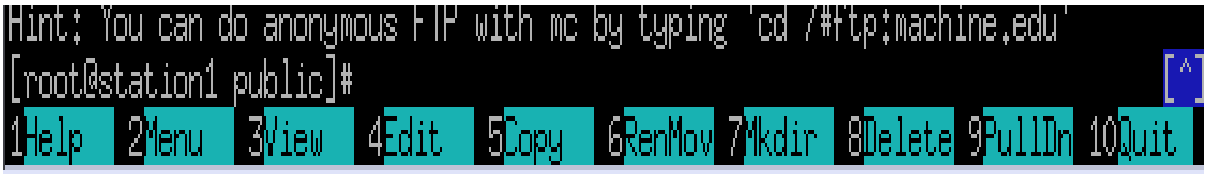


Fig. 3.4

Most of the F commands are very logical and self-explanatory; so I am not going to explain them, except the F9. The **F9** is used to jump to the upper pull down menu.

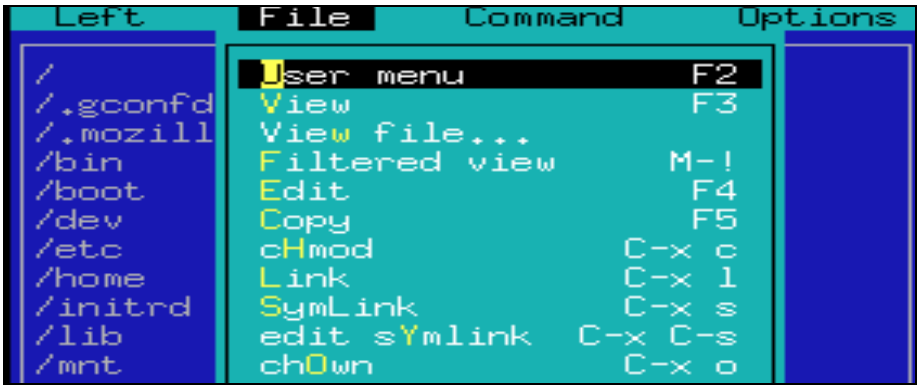


Fig. 3.5

After pressing F9, use the arrow keys to browse through the sub-menus. Observe that under the file option you can access options such as **cHmod** and **chOwn**; in other words file permissions.

File permission with mc

The file menu is very useful, here you can change file permissions and ownerships.

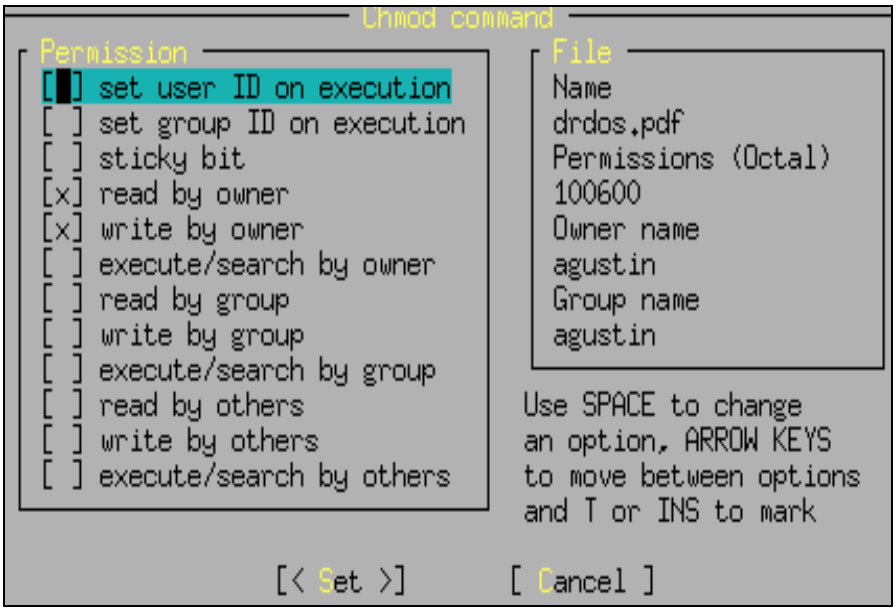


Fig. 3.6

If you did not understand file permission earlier, you have the easiest way to set permissions. Select the **cHmod** on the file menu to see the chmod screen, figure 3.6.
On this screen, you can set the permission type.

Observe the **chmod command screen**, on the right panel it describes the file being modified. As you change permissions the numerical (octal) permission of the file also changes.

Searching files with mc

Finding files has never been easier. Just select **Find file** from this menu and fill out the search starting point, the file name, Select OK and hit Enter.

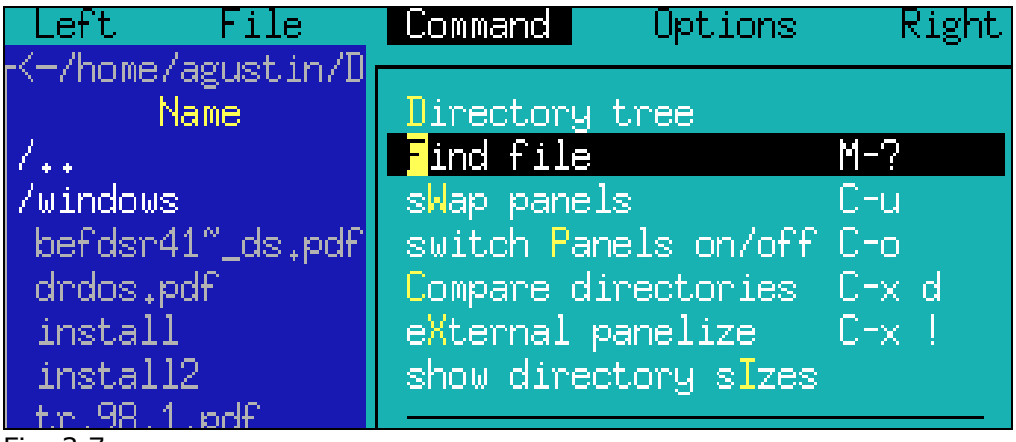


Fig. 3.7

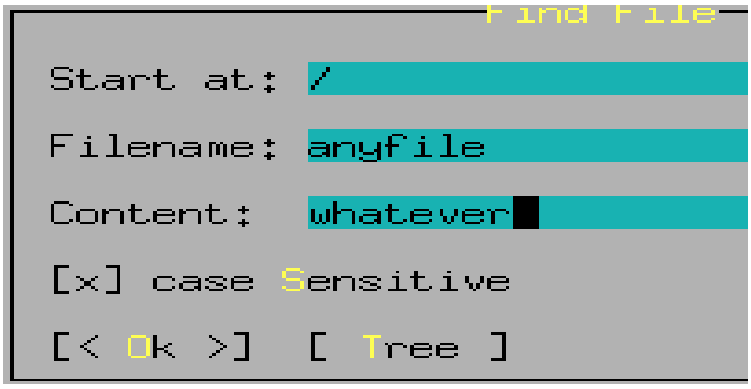


Fig. 3.8

Look at Figure 3.8; the **start at** is where you want to start searching for the file (the root directory). You can change that with any folder name or a particular partition.

Midnight commander can help you with most of the file administration. Browse through all the options and menus to find out what it is for. You may not need to use all the options. If you feel like reading, you can always read the manual by typing **man mc** at your command prompt. If **mc** is not installed, refer to the installation section in chapter 4.

The Linuxconf Utility

If you read chapter 2 and configured your net card, the settings will be already in the net card properties. If not, proceed as follows.

Welcome to the heart of the system administration. This is the control center and holds all administration utilities. The Linuxconf can be run under text mode and graphical mode. If you run the utility under text mode use the tab key to move between fields.
The only difference between the text mode and graphical mode is that in the graphical mode you can use your mouse (if the appropriate driver is loaded for your mouse, may work under text mode too), the rest of the options are exactly the same. I will discuss linuxconf in graphical mode, because my guess is that in the next couple of years most of the distributions will use graphical administration mode.

Note: *The first time you run Linuxconf you will see a welcome screen, select **qui**t continuing to the main entry.*

Start your X graphical interface:

```
[agustin@server2 agustin]$startx
```

Once you are at the graphical interface at the run command type linuxconf.

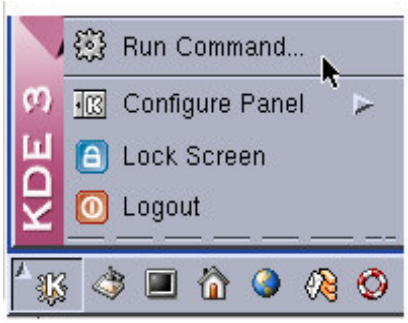


Fig. 3.9

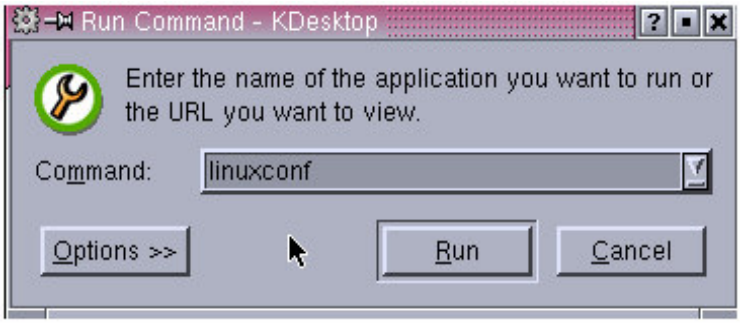


Fig. 3.10

When you click run or hit enter you will be prompted for a password. That password **is root's** password. Type the password and hit enter. If you get a bad command error, it is most likely that linuxconf is not installed. Refer to software installation in chapter 4. The main screen has three important tabs: **Config, control,** and **status.**

You can do almost everything with this administration utility. But remember linuxconf is only for system administrators. During your practice of system administration, do not be scared to make changes to any part of the system. Keep in mind that whatever goes wrong in the real world, you the system administrator will have to fix it.

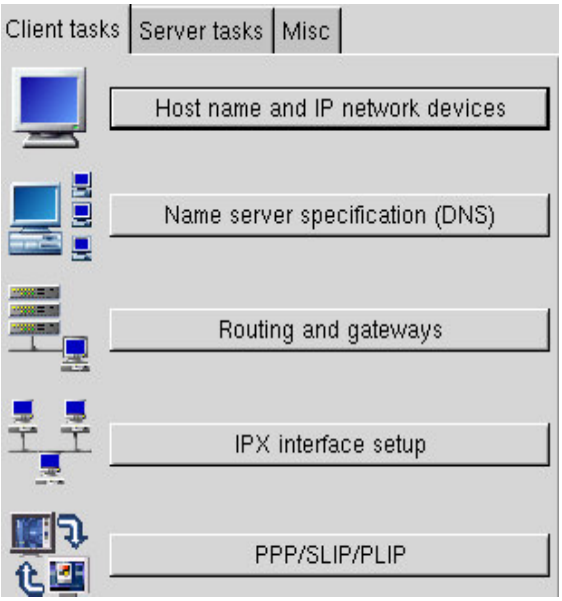
**Learn how to use this utility before you try to use it on someone else's server.*

If you have not configured your system yet, I will walk you through to make it a success. I do believe that this book will assist you better than any out there. Stick with me, if you have encountered difficulties, read chapter 2, **quick start.** It may clarify your thoughts.

Networking with linuxconf

Static IP Address Configuration

Open **Config** => **Networking** => **Client tasks** => **Host names and IP network devices**



I have planned to demonstrate how to setup the most common servers. So the configuration for the network I will use is static IP. I will assume that this will be a public address.

Fig. 3.11

Public IP: Physical IP addresses visible over the Internet.

Private IP: Physical IP addresses visible internally within the company in a local area network.

The networking section has two main tabs; Client and Server.

Before a system becomes a server on the Internet it is a client first, afterwards it is promoted. First you connect to the Internet to prove or test that your connection is active.

Grab your tools and test the line yourself if you know how to do it. But never trust the Telco or ISP that the line is active until you actually set up the computer and browse the Internet.

On the client tasks: Click on **Host name and IP network device** to get to the host name configuration:

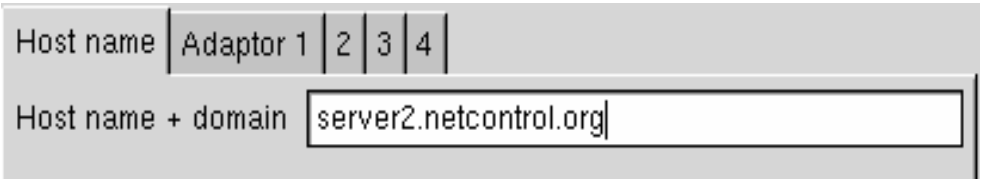


Fig. 3.12

- **Enter the computer name + the domain name**

The domain name will be identified over the Internet when you run the web server. For practice and demonstration purposes you don't need to be connected to the Internet. Just be aware that it is the same scenario. The difference is only on the IP address (public or private).

- Click on Adaptor1

The adaptor1 is your first net card. You have the option of installing and configuring four net cards.

Note: ***Each net card is configured in its own subnet***

- Make sure the card is enabled.

- Configure mode must be manual

- Computer name + Domain stay the same

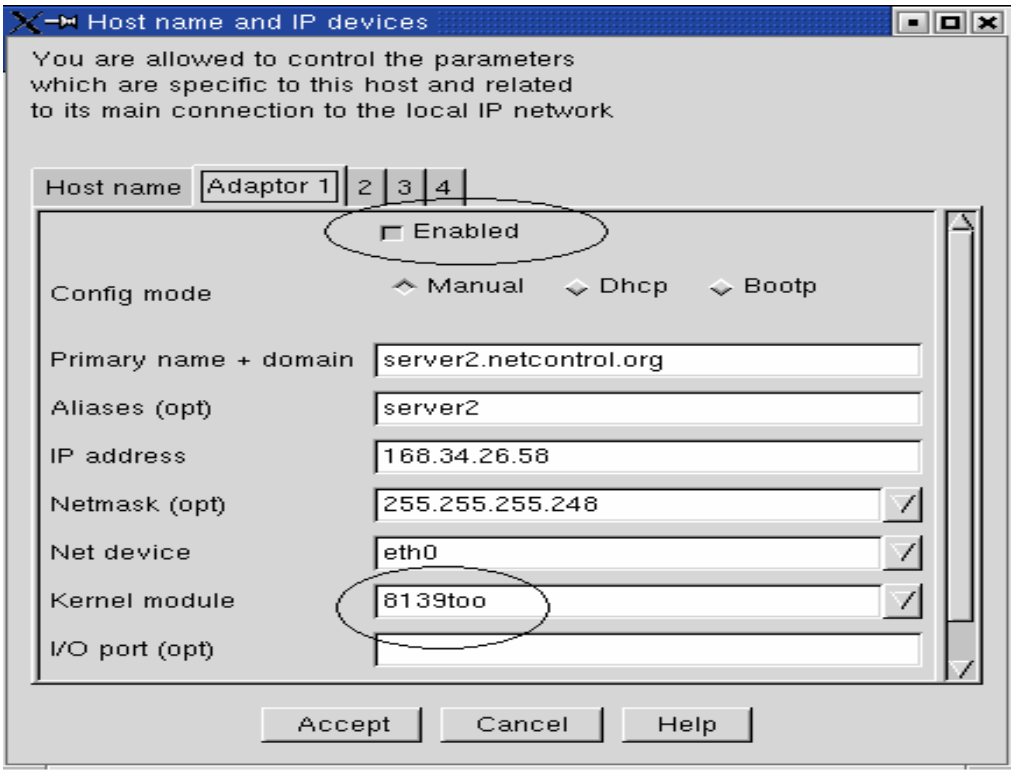


Fig. 3.13

-The aliases are how you want the computer to be known or found as.

-Enter the IP address given by your ISP with the subnet mask

-Select the network device (card 1 = eth0)
-Enter the kernel module (driver module)
-Click Accept.

- **Aliases** — shorthand for the fully qualified domain name. This is often the same as the primary name. For example, if the fully qualified domain name is server2.onetraining.net, you could set server2 as an alias.

Domain Name Service DNS (workstation / client)

On the client task

The name service specification

Open Config => Networking => Client tasks => Name server specification (DNS).

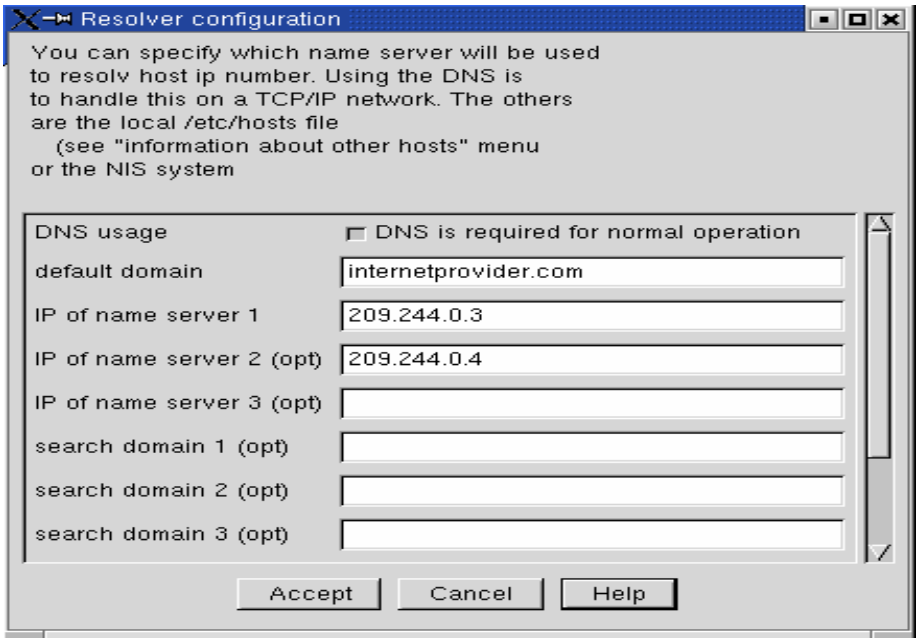


Fig. 3.14

Before our client computer can make appropriate negotiations to authenticate and login, it must have to know where to ask to obtain the correct path (IP) to its destination; that's when the DNS takes place (the ISP's DNS).

This DNS information is the server provided by the ISP, and it is given to you when you get your static IP.

Enter the IP addresses of the DNS servers
These servers are contacted first when you connect to the Internet.

When you request a web page from your browser, these servers are contacted to find the shortest route to obtain that page.

- When finished click Accept

Note: Do not confuse these DNS servers with the one you have in your internal network. Read chapter 9 about servers.

Router and Gateway

The DNS is not the only one required to accomplish the connection to the server. Before it actually contacts the DNS, the client computer needs to know the door to get out. That door is known as **gateway**. Without the gateway, the connection will not be possible. The computer may actually look for the default local host, but the local host (127.0.0.1) is not the correct path to get out. That is the reason that whenever you declare values to the net card it needs to know all this information.

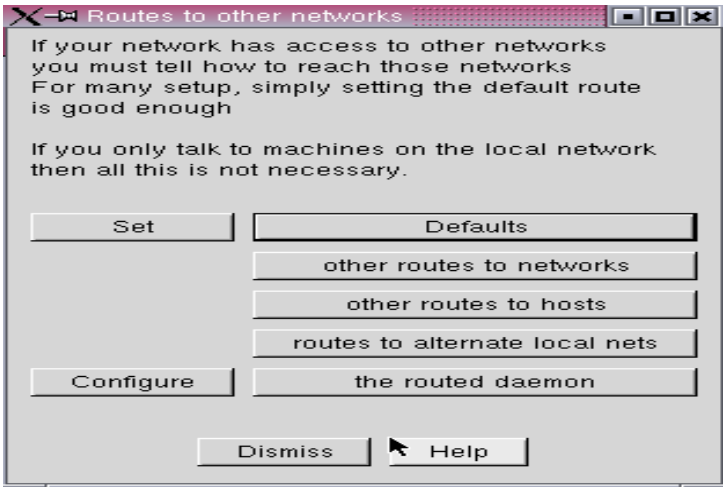


Fig. 3.15

The information is given in two ways… static or dynamic. Static means you place the values manually and dynamic means it is assigned automatically by the remote server.

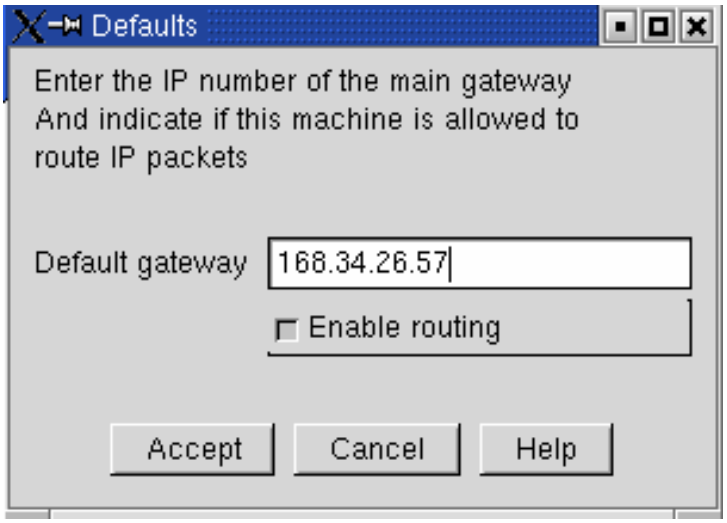


Fig. 3.16

- Enter the default gateway IP address number and make sure it is enabled.
- Click on Accept.
- Click on Dismiss
- Click on Dismiss again
- Click on Quit

On figure 3.17, my gateway is the router, because the router is the actual door to the Internet (read chapter 2 routers). Note that you cannot assign that IP number to another host instead all hosts must have this number as its gateway if they are in the same subnet.

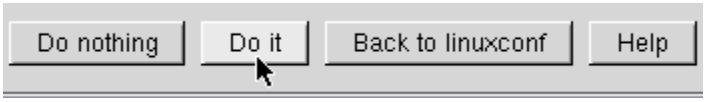


Fig. 3.17

- Click on Do it

Once you click on **Do it**, the changes are saved. You can now reboot the system. At boot time you will see your network adapter (Bringing interface eth0 up …….OK)
Congratulations you successfully configured your network adapter.

Adding users from Linuxconf

Open **Config** => **Users** => **Normal** => **User accounts**.
In this panel you can create new users, delete users, groups and even change your root password.

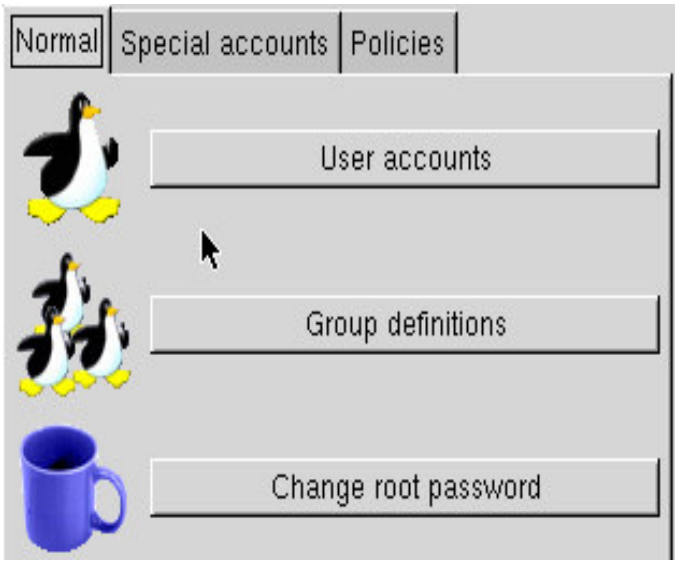


Fig 3.18
To add a new user click on User accounts

- Click on **Add**
- Enter the **login name**
- Enter the **full name**
- Enter the **group or select the group** you want the user to belong to.

Supplementary group, means **additional group** you want the user to belong to or be part of.

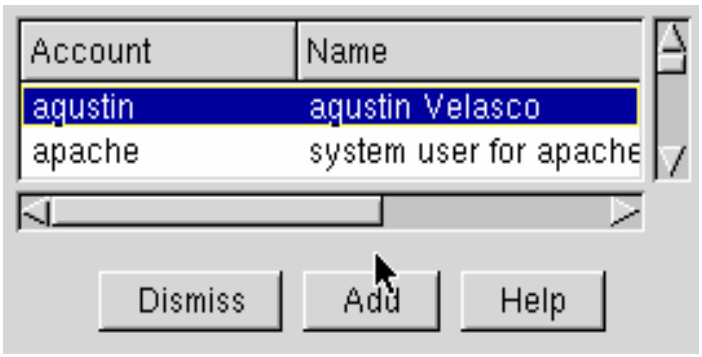


Fig. 3.19

- You can specify a **home directory** or leave it as default
- Leave command interpreter as **default**
- Leave **user ID blank**, let the system assign it automatically

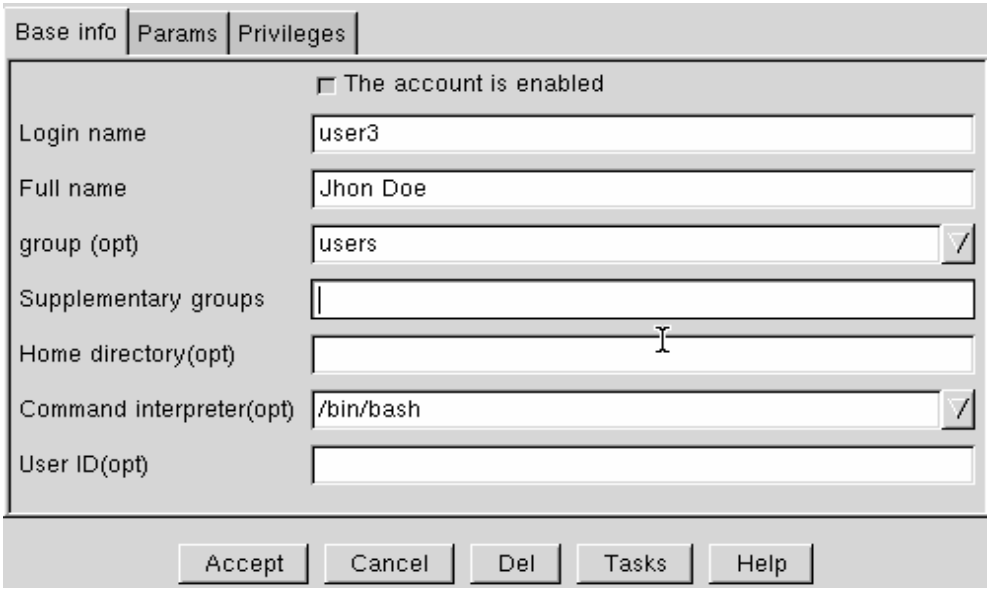


Fig. 3.20

-To delete a user, select user and press delete.

Accept your changes, when quitting Linuxconf; click on **Do it** to apply changes.

Enabling User Accounts

By default, all newly created user accounts are enabled. If you need to enable an account, you can use **Linuxconf** to do it.

Open **Config** => **Users** => **Normal** => **User accounts**.

- Select an account.
- Select -**The account is enabled** checkbox (Fig. 3.20).

Disabling User Accounts

You can temporarily disable a user account. If the user is gone forever from the company, it is preferable to delete the user's account. Back up all data from the user's home folder if needed.

Open **Config** => **Users accounts** => **Normal** => **User accounts**.

- Select an account.
- Unselect the checkbox that states, **The account is enabled.**
- Select the Accept button at the bottom of the window and you're all set.

The account is disabled and can be enabled later using the same steps.

Params for User Accounts

These are settings that control the account. By default, all of the settings are **ignored**, so they are unused. **Must keep # days** minimum number of days for the user's password.

The **Must change after # days** field can be set to make a user's password expire after a certain number of days. It is a good idea to let the user know that his/her password will expire soon. The **Warn # days before expiration** field should be used.

If you want an account set to expire after a certain number of days, use the **Account expire after # days** field. Enter the expiration date.

Privileges for User Accounts

In the **Privileges** section, you can grant power to the user and/or control over various aspects of system configuration. As default, regular users are denied all privileges on this screen. If you want the user to be able to do something, think and decide what rights you want to grant them. Let the user do something. In many companies users don't do anything anyways.

The difference between **Granted** and **Granted/silent,** if the privilege is **granted**, **Linuxconf** will ask for the user's password before allowing them to execute the task. Privileges **granted silently**, are not prompted for their password.
My advice is; do not grant users any privileges unless it is absolutely necessary. Be careful when you grant privileges, **especially silently**. Remember, any user at any time could sit at a particular workstation and start executing tasks that they shouldn't.

May use Linuxconf: These users are allowed to access all of **linuxconf**'s capabilities, and they can set up or change any parameter.

May shutdown: Grant this right only if you want the user to be able to shutdown the system.
Never give a user too much power. If you do, sooner or later you will be locked out. For a regular station it may be Ok (grant them), but not for a server machine.

Account policies

Users => **Policies** => **Password & Account Policies**
This panel controls the password enforcement policies; here you can specify the length of the password, the restrictions of numbers and letters.

You can enforce the restrictions required at your wish. Good passwords contain a combination of letters, numbers, and special characters. A password should use both upper case and lower case letters. As a good practice never use your username, your anniversary, your social security number, the dog's name, you mamas name, your middle name or the word root. Don't use any variation of a word associated with your account or with yourself. Always avoid dictionary words; dictionary words are easy to crack. Oh, and forget these: "love, sex and god".

Managing groups

Users => Normal => Group Definitions
Administration is being organized. Organization is a keyword to successfully maintaining a Linux system. Like I said earlier, every user by default is in their own group and if we have 5000 users in a domain, we don't need 5000 groups. Correct?

So in order to make our job easier as System Administrator, it really makes sense to have logical groups or different departments as usually known in the company. Here is an example; we don't want users from marketing to be messing around in the engineering or manufacturing department right? So that is why it is nice to create each respective department.

For example:

- Marketing
- Engineering
- Accounting
- Human resource

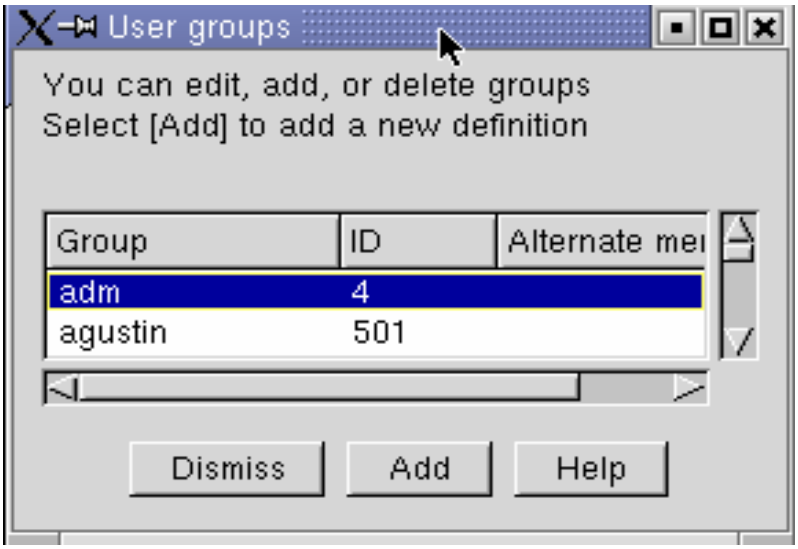


Fig. 3.21

Every time a new employee is hired we can add him in the appropriate department, with his respective rights. Or he will wine and end up in the human resource department.

- Click on add to create a group

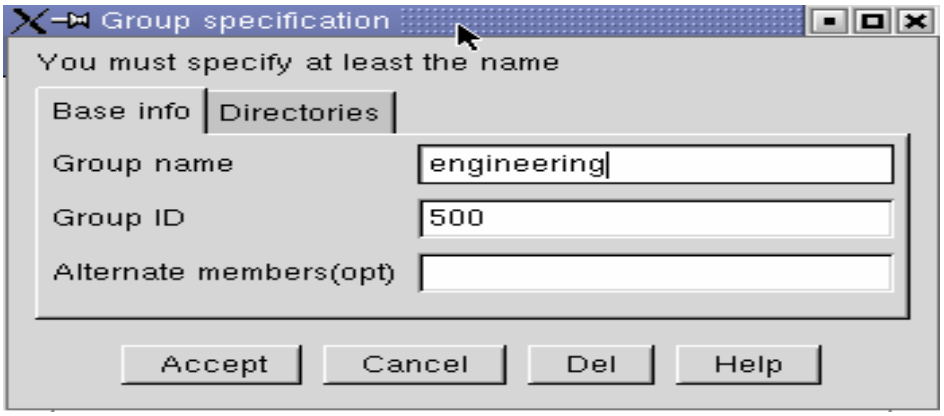


Fig. 3.23

- Enter the name of the group
- Leave group ID as default
- Leave alternate blank
- If you click on directories, you can specify the home directory for the whole group.

Once you click on accept, the group will be created. From now on the group will be available whenever you add new users or promote existing users.

Changing the Root Password

For security reasons, you must protect root password at all times. This requires you to reset the password with frequency.

- Open **Config** => **Users** => **Normal** => **Change root password**.

By clicking on the change root password you will be prompted to enter the new password. Use a strong password for this purpose. Once you have entered the new password, select **Accept** to apply the changes otherwise select cancel.

Alternatively you can use a command line to change the user's password:

```
[root@server1 root]# passwd username
```

Mounting file system

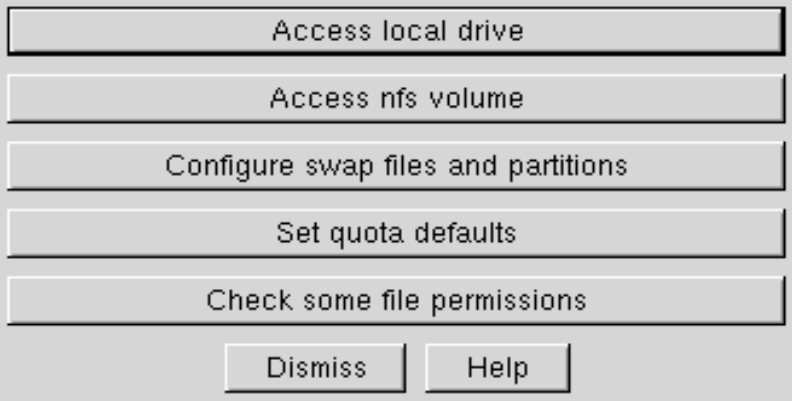


Fig. 3.24

This option allows your workstation to configure what file system can be accessed.

File systems reside on mass storage devices such as diskettes, hard drives, and CD-ROMs.

Each storage media can be a different type of file system such as FAT, FAT32, NTFS, and HPFS etc.
Under Linux, it is possible to link different file systems on a mass storage device into a single, larger file system. This is accomplished by placing mounting points of a device's file system in a directory on another file system. So while the root directory of a drive on a different machine may be referred to as c:\, the same drive on a Linux system may be accessible as /mnt/xdir; where xdir can be any name (it is a directory, known as mount point).

When a device is mounted, it is then accessible to the system's users who have proper permission to access it.
Linux conf is a way of mounting file systems. You can also mount it by command line.
For example, to mount the first diskette drive on /mnt/floppy, you would type the command mount `/dev/fd0 /mnt/floppy`

** Note that floppy is a subdirectory inside mnt directory.*

During the installation of Linux, a file that holds the information of mount points is created and it is located in `/etc/fstab`

To auto mount devices at boot time, this file can be edited to add new devices that points to file systems.

Reviewing Your Current File system

- Open **Config** => **File systems** => **Access local drive**.

The **source** here displays all mounted drives, **figure 3.23** displays **hda**, and this means it is an IDE drive.

- **fd** indicates a diskette drive
- **hd** indicates an IDE hard drive

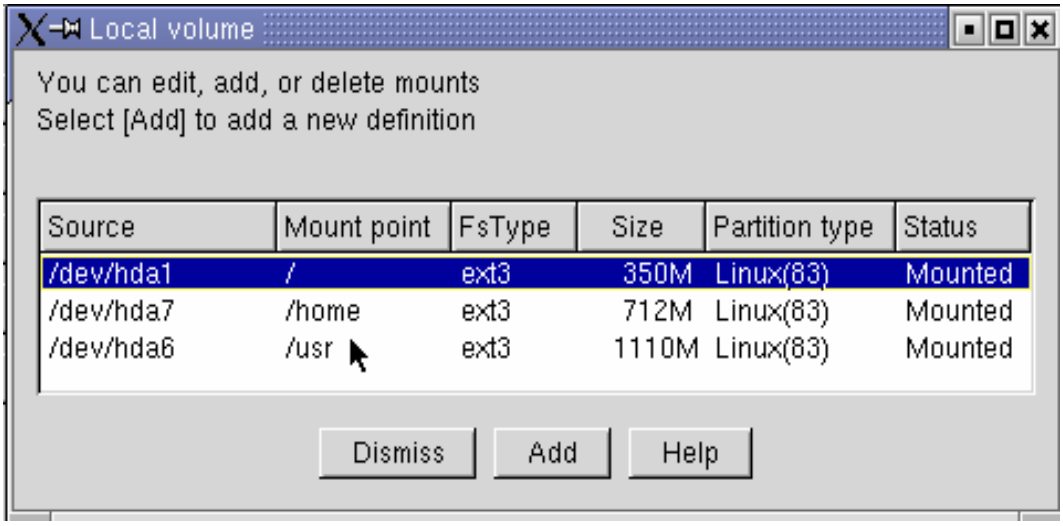


Fig. 3.25

If you have any other IDE drive, a second would be hdb, a third one would be hdc… and also follows a number, and these numbers represent the partitions.

Mount point: The actual location from which the file system is mounted and accessed.

FsType: The type of file system. A standard Linux partition uses the ext2 file system type, mandrake 9.0 uses ext3, DOS uses FAT16, Windows uses FAT16, FAT32, and Windows NT uses NTFS.

Size: Partition Size

Partition type: A description of the file system used on that partition

Status: Whether the device is mounted or not

NFS Mounts

If any NFS mounts exist you will see it here, but since this is a new installation most likely you don't have one.

- **Config** => **File systems** => **Access nfs volume**

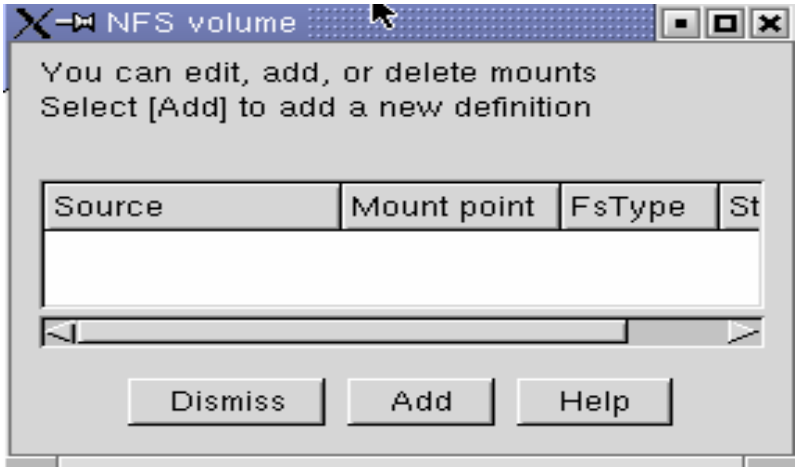


Fig. 3.26

When mounting network File systems from other machines in a network; it can be a small directory or an entire volume.

- The **source** will be the name of the machine serving the file system, followed by the remote directory.
- For example, you might see a value of machinex: `/var/spool/mail` where machinex is the machine serving the directory and `/var/spool/mail` is the directory being served.
- **FsType** — will always be "nfs."

Adding NFS Mounts

Let's add an nfs mount so you can see how it is done:

- On the **NFS volume** screen, select Add.

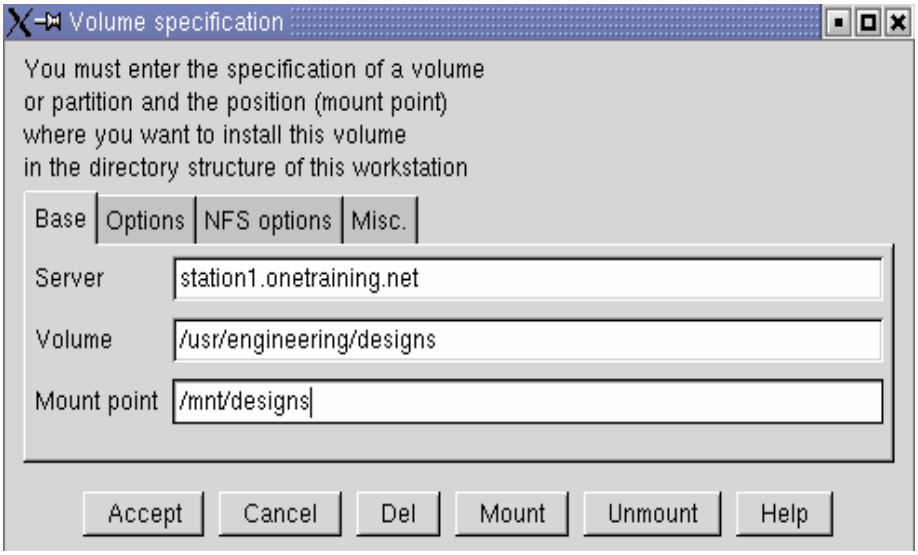


Fig. 3.27

- **Server**: The hostname of the machine on which the desired filesystem is located. For example, station1.onetraining.net
- **Volume**: The file system you wish to add. For example, `/usr/engineering /designs`.
- **Mount point**: The directory in your system from which you want the remote file system to be accessible. For example, /mnt/designs.

- Once you have entered the information, select Accept.

Note: *The mount point is the physical directory where you actually transport it. If your mountings are permanent, create directories for that purpose and secure it.*

The **options tab** is used to set the appropriate permissions and control how the NFS mount point will be accessed. The **NFS option** tells the mounting point how it is going to be mounted.

That's it. **Linuxconf** will update your `/etc/fstab` file accordingly. Please read the help file on the **Volume specification** screen and see the **mount** man page for more information.

Implementing disk quotas

Quotas are used to manage storage in distributed environments. Disk quotas are abilities to manage and limit disk resources to those who abuse the system in the form of storage facility.

Disk quotas allow you to monitor the amount of disk space left against the limit assigned to individual users or groups. Disk quotas can be controlled by per volume, per user and per group. If you suspect that a particular user is using disk space to download files from the Internet and is consuming a considerable amount of space… limit their space with quotas.

Note. *My advice is not to assign individual quotas, especially if you have hundreds of users in your server. That will lead to administrative nightmares. Set quotas for individuals only when there is a compelling reason to do so.*

Set quotas default is not the best way to set quotas; however you can use this option to set quotas for **default user and default group.** Before you can set quotas, a partition or volume must be quota enabled in the local access option.

File systems => **Access local drive** => **Select and click on a partition** => **Option**s => **User quota enabled.**

After the partition's quota is enabled, quotas will be available in any part, such as in user accounts and group definitions.

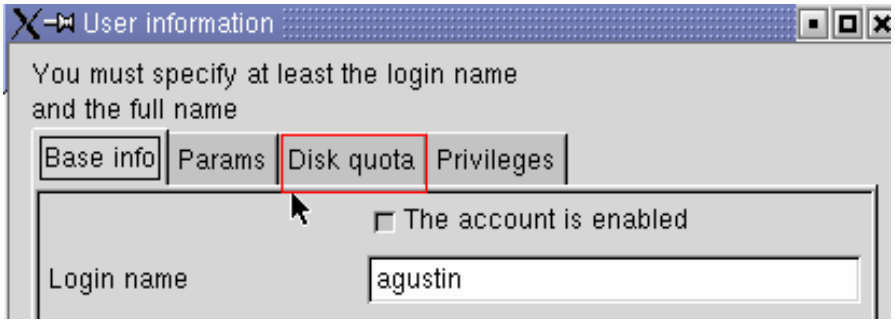


Fig. 3.28

In the user property the quota is enabled per user
The following is the group's property setting, very similar to the user's property.

The quotas are set in Mega Bytes. All quotas assigned to a group will be applied to all members in that group.

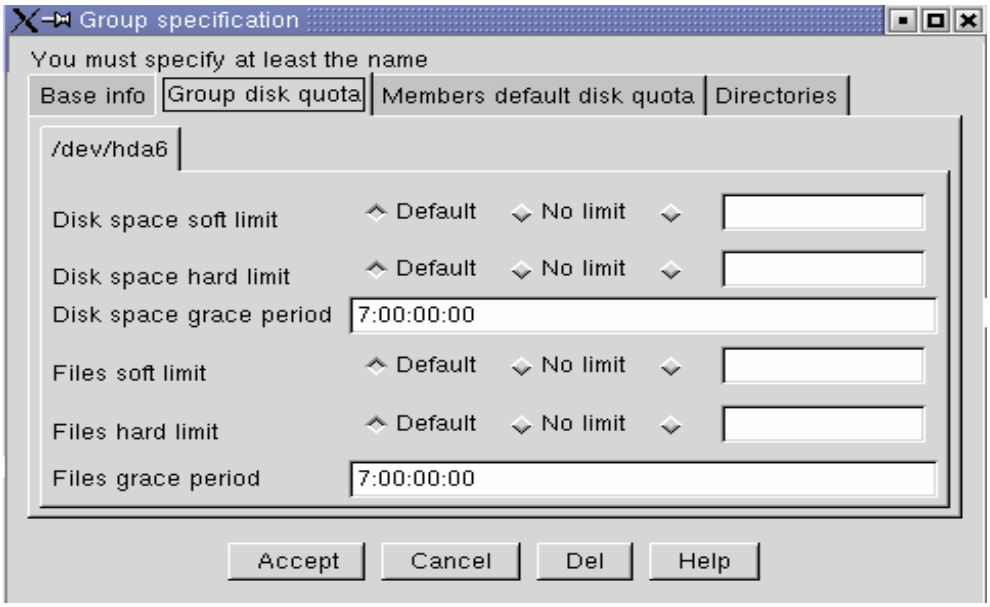


Fig. 3.29

Soft limit: the soft limit is a time limit set by the administrator. Users can exceed the soft limits assigned to them, but only for a limited amount of time--the time limit set by the administrator.

Grace period: This is governing the soft limit. When grace period is set; it acts as a borderline and times out. When a user reaches soft limit, **grace period** sent a warning to the user indicating that his limit is in violation.
Hard Limit: The hard limit represents an absolute limit on the resource, blocks or inodes, which the user can never exceed under any circumstances.

Effect of quotas on users

The following are the major effects of quotas on users:

- On soft limit, if a user exceeds the space limit (blocks or inodes), the timer is started. If the user then reduces usage, the timer is turned off and all returns to normal. But if the user has not reduced usage when the timer expires, any further attempts to acquire space resources fails, and the user receives error messages saying that the file system is full. These messages persist until the user reduces usage under the soft limit level.

- If a user reaches the hard limit at any time, the system will warn the user that there is not enough space and will automatically lock the space usage.

Miscellaneous

Config => Miscellaneous

You don't always have to use these options unless really necessary

Run levels

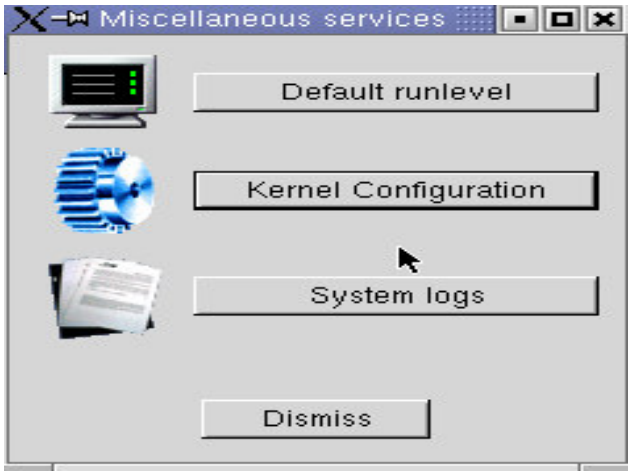


Fig. 3.30

- The run level controls the behavior of the system.

- During our installation (if you did this correctly) the system by default is now set to level 3 text console.
- If you want to automatically log in to graphical mode, this is where you change the run level to 5 graphical.

Kernel configuration

This option is very sensitive. I suggest you do not modify this unless you know what you are doing. After each installation the system is already default.

System logs

Here you specify where to store the system logs. Leave as default.

Peripherals

This is the section where you can configure some of your hardware. If you have or need to install any ISA card, this auto detection utility can help you to quickly configure it. In this option you can also configure your modem. Refer to modem installation in chapter 2 if you need assistance.

You may also configure your printer here via lpd. You can configure it now or read the section for printer installation.

The Linuxconf Control

The control panel has several options that are very useful; you probably will not be using everything. A lot of the tasks can still be accomplished manually.

All will depend on your abilities, sometimes it is much faster to execute a command line than to load x windows and execute Linuxconf graphically or execute linuxconf under text mode.

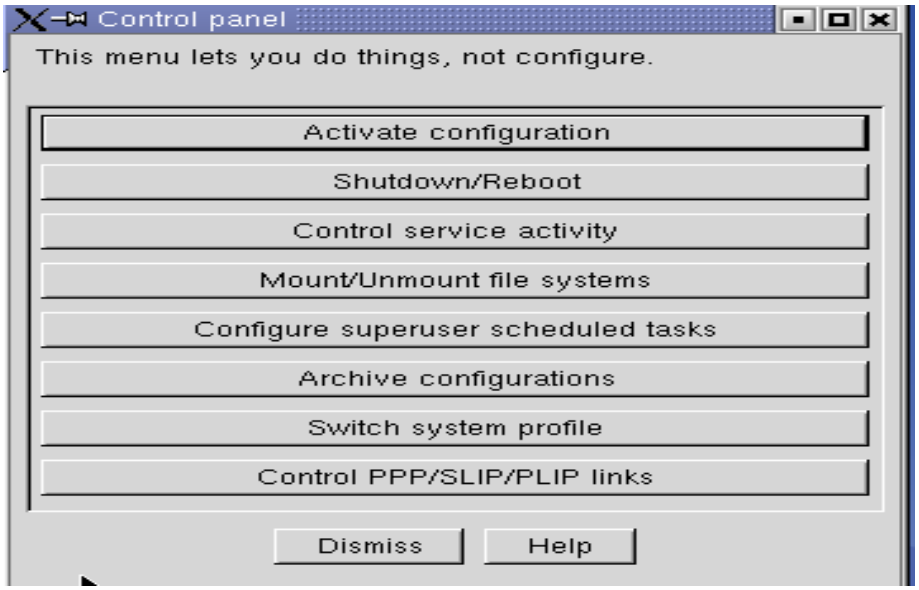


Fig. 3.32

Activate configuration: The first option in this menu. This let's you save all the changes you made in the Linuxconf without exiting.

Shutdown reboot: This option will let you set a timer in minutes for shutdown.

Controlling services

Control service activity: This is probably one of the most frequently used options in this panel. Many activities from this panel can be done through command line. By clicking on the Control service activity, you will be presented a panel with all the current services in the system. Some are already running and some you have to activate or stop.

Control panel => **control service activity** => **select the service module => select run level**

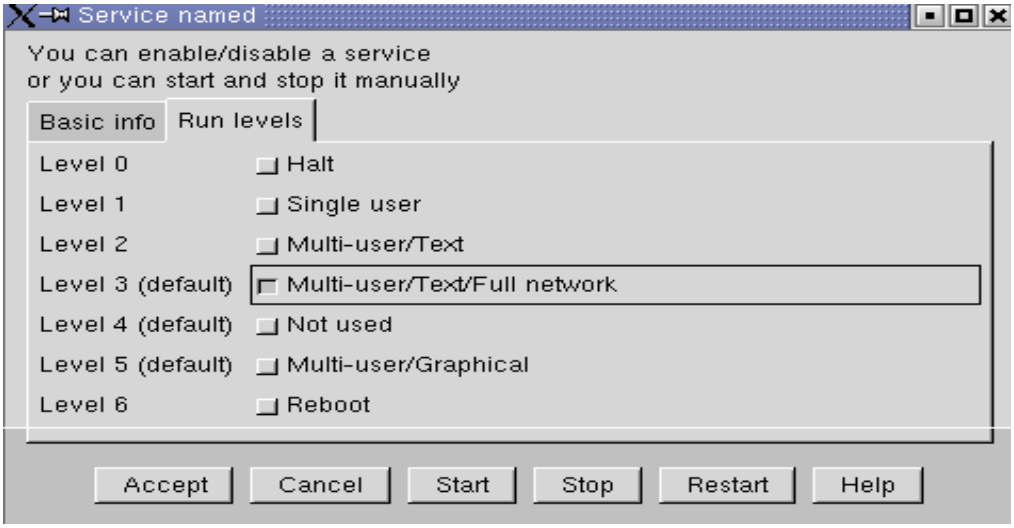


Fig. 3.33

Look at the previous picture, I have selected named (the DNS server)

This server will be activated automatically at start up, and it will be running at **level 3 multi users / full network**. I can even start the server from this panel by clicking the start button at the bottom.

When I accept the changes, and quit Linuxconf, the next time I will restart the system the **named** server will run automatically. (This is done only if the service is not run at start up…)

Note. *All other services are treated the same way. To learn more about services read **chapter 10** Security.*

Linuxconf Module management

In this panel the only option that I really use is modules.

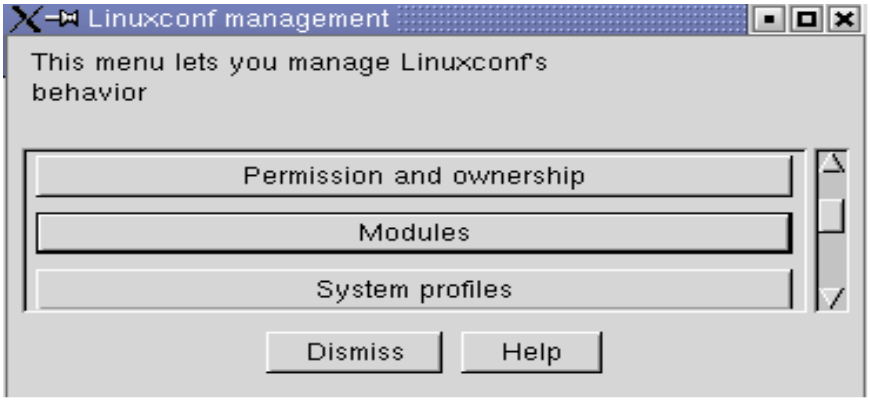


Fig. 3.34

Here you can add new modules to Linuxconf.
Each time you open Linuxconf the model will load and will be available to use.
It won't hurt if you load new modules here even if you will not use it, but why would you add modules that you will not use?

At this point you already learned how to use Linuxconf; it is a good practice if you want to play with the new modules. In the server section I will teach you how to manipulate them manually.

Note. If you happen to encounter errors when you try to use an administration tool; errors such gtmp is locked or present it is because you probably have two administration tools open. Check on all virtual terminals and graphical interface. Close all opened administration tools and erase the file mentioned in the error message (gtmp, ptmp) in /etc.

Chapter 4

Mandrake control center

Mandrake Control Center is the main configuration tool for your **Mandrake Linux**. It enables you, the system administrator, to configure many aspects of your system. This control center greatly simplifies system administration, notably by avoiding the use of the command line. However the control center is limited at certain points, many things are still required to do be done manually or with other utilities such as Linuxconf.

The Mandrake control center can be run under text mode and graphical mode known as `DrakConf` or `mcc`.

```
[user1@server2 user1]$mcc
```

Or

```
[user1@server2 user1]$drakconf
```

In chapter 2, we learned how to get to the control center.

In this chapter we will discus a little more in depth about the most common task in the control center.

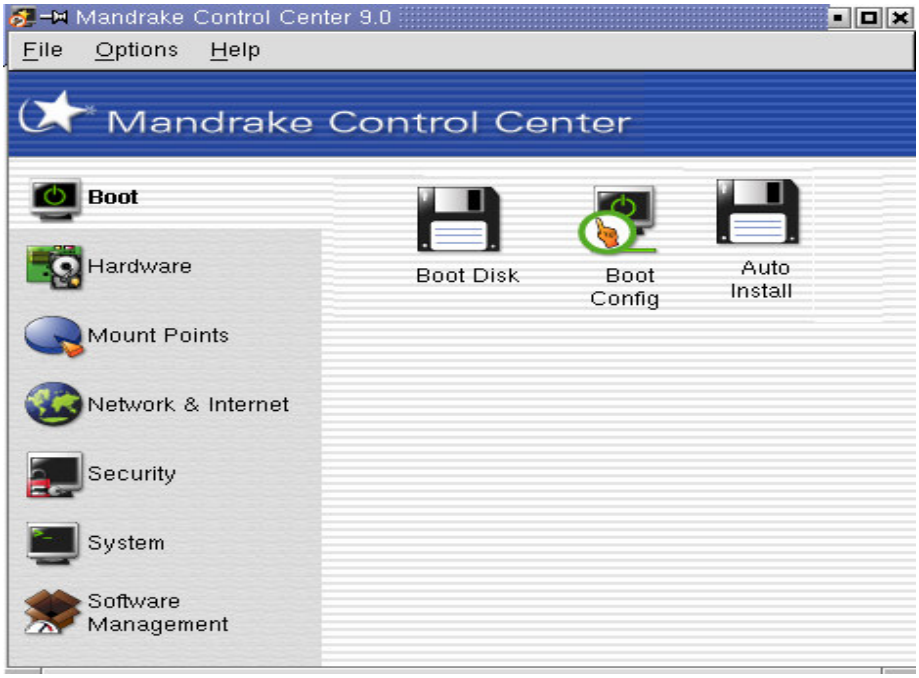


Fig. 4.1

The main menu on the left is the main access point to the configurations.
As an example, I clicked on the boot icon and the executable wizards appear to the right.

In chapter 2 & chapter 3 we already discussed some of these tools, for that reason I may not go over it again.

Creating a Boot Disk

During installation, you had the chance to create a boot disk. If you did not create it, here you have the option to create it. This boot diskette creation is a rescue disk and allows you to perform some maintenance tasks on your system in case of failure.

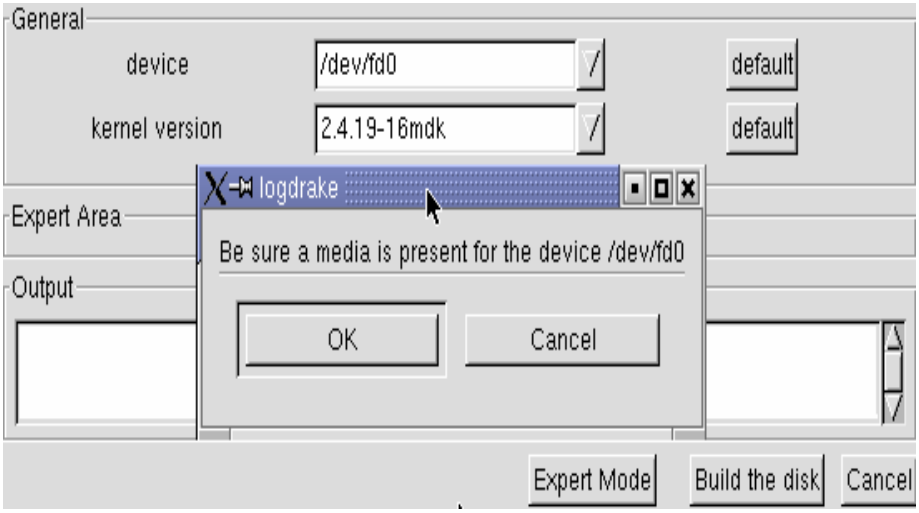


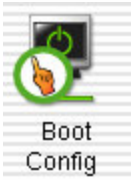
Fig. 4.2

By clicking the boot disk icon, the system starts to gather the necessary information to create the bootable floppy. When the information is ready to be written, make sure you have a floppy disk, and it is not write protected. Insert it in the floppy drive and click OK.

- **Build the disk**.
- **Click OK**

Wait for the drive to finish writing the floppy, when finished it will be ready for use.

Your Boot-Up Configuration



This tool allows you to change the setting in your Lilo/Grub boot manager. You can specify whether to boot the system in text or graphical login mode. By clicking this icon, it takes you to the configuration screen which displays your current boot loader. Figure 4.3 allows you to switch the boot mode from text to graphical. If the Launch graphical environment is selected, the system will boot prompting the login in graphical mode.

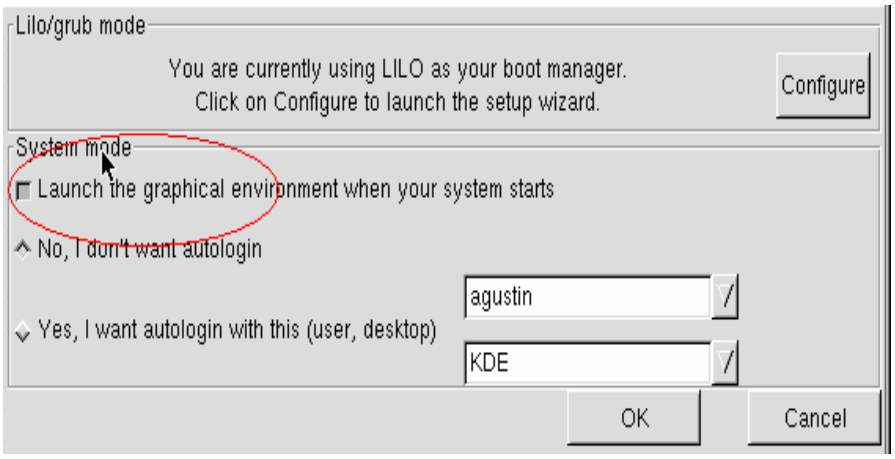


Fig. 4.3

If you click the Configure button, it launches the boot loader setup. You will be presented two dropdown arrows.

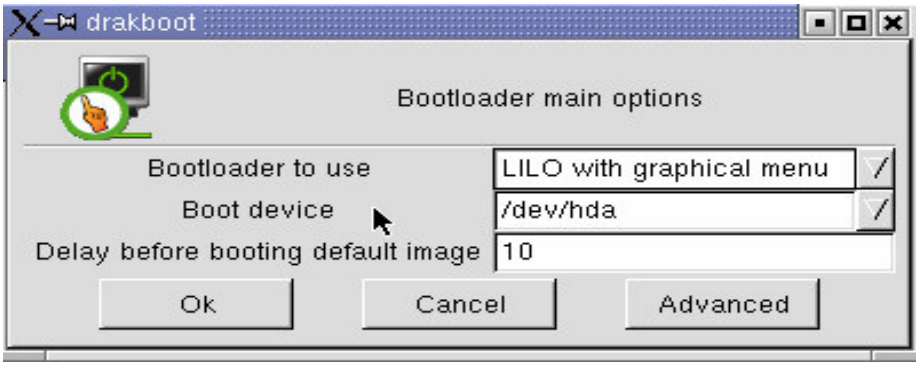


Fig. 4.4

The first drop down arrow enables you to switch from one boot loader to another with options to boot from graphical or text mode.

The second allows you to choose the device from which to boot. There is a third option for setting the timer in seconds, which is the delay on your menu if you are dual booting. I don't think you will need to change any of these settings, but it is nice to know if you need to troubleshoot. Remember, if it is working, don't fix it.

The advanced button keeps other interesting features, such as video mode startup (resolution), and cleaning up the `/tmp` at each boot.

Switching boot mode Text/Graphical

During installation, I mentioned that you should boot in text mode first because if you had any trouble getting to the desktop you could then troubleshoot. The main concern is your video configuration. I have seen many Linux installations not detecting the graphics properly. Therefore booting graphically with the wrong vertical/horizontal refresh rate synchronization may damage your video card or monitor.

Even though I just mentioned how to switch from graphical to text mode in this control center, what good is it if you are unable to get to the desktop? Luckily Linux offers an **Interactive-booting mode.** You can use this option to force the system to boot into the text mode by pressing "**I**" at boot time and answer **NO** to all the questions.

By answering **No** to all the questions, the system will drop you to the login prompt, (you should login as root here).

Mandrake itself offers a **fail-safe booting mode,** which will drop you to a menu**.** From the menu select **text mode/full network**, Login with your root password**.**

Once you logged in as root, edit `/etc/inittab`, this file holds the run level configuration boot modes.
Find the first uncommented line:

```
id:5:initdefault:       Number  5  in  this  line
                        means   to   boot   into
                        graphical mode
                        (observe above this line
                        you have a menu of
                        booting modes 0-6)
```

To switch your booting mode to **Text Full network multi user mode,** replace **5** with **3**. There after, when you need to log on to the desktop, just type **`startx`** at your command prompt to start the graphical interface.

To use the Mandrake control center under text mode, type **mcc** at your command prompt (use Display configuration), which will help you re-probe your graphics card. Have all the specs ready… good luck.

Creating a Pre-installation Disk

This option allows a system administrator to create an automated pre-configured installation. This is nice if you have many computers to set up, this saves you time by running an automated install.

- **Replay**: This reuses settings from your previous manual installation.
- **Manual**: Choose this for the installation to prompt you when manual settings will be enter during the automated installation.
- When you click Ok, you will be prompted to insert a floppy.
- After clicking OK again, the boot floppy disk will be created with the settings you used in your current machine. If the previous installation was done through CD_ROM, that setting will be used; if your installation was through LAN or FTP that is what will be used.

Note. *Most of your previous manual installation may be used as replay, except **configure X** and **partitions;** these two you may have to take into consideration; but if you have exactly the same systems then this wouldn't matter.*

When you are ready to install just insert the floppy disk you created into the new machine and the installation CD1. Turn the machine on and there you go.

Hardware configurations

Your monitor and your video resolution

Sometimes the screen resolution is not appropriate, or perhaps you made a mistake during installation, you can use this icon to set the proper resolution if the current one is not correct.
In case you need to reconfigure the video adapter you can do it by running the following command under text mode.

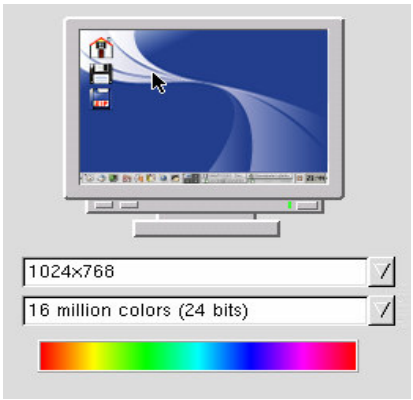


Fig. 4.5

```
[root@server2 root]#XFdrake
```

To run the Configuration under text mode login as root and execute **XFdrake** this will allow you to configure your hardware; this is same as in mcc.
XFdrake is an advanced tool and most likely will probe your hardware. If you are not getting anywhere with this utility, find out about your hardware – is it supported by Linux? What possibilities do you have to change your video adapter?

If you are going to change the video card, try NVIDIA. It works well and most likely will be supported. Whenever you make changes test your configuration before accepting the settings.

The graphical server configuration

In most cases you don't need to make changes here, it is automatically configured during installation. The server is what controls your interface. If the server is not running you simply don't have graphics.

Any time you configure a display adapter or monitor, you are only modifying your client settings, which must report the appropriate refresh rate and resolution for the server to send the correct display.

If you accept the changes the server updates its database, and there after keeps the information after reboot. So every time you start your Xwindow the server is contacted and the information is verified in order to display the correct resolution.

Note: *If the server holds the incorrect settings and you start the graphical interface, you have the chances of ruining your video adapter or monitor. Be careful, read about your hardware specs when you are configuring manually.*

Printer configuration

This icon is used to configure your printer. If your printer is supported it will be detected and installed.

I suggest before you run this wizard go to install packages and install:
LPRng-3.8.12-2mdk

Always install the most recent software whenever possible.

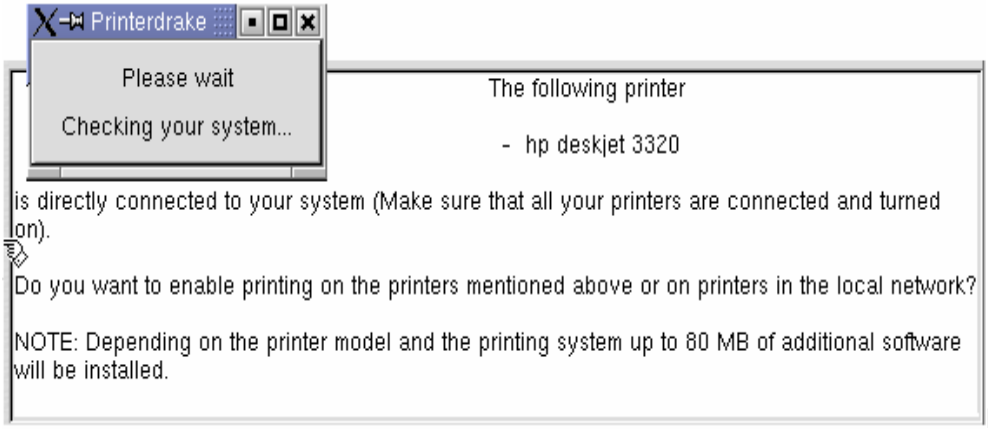


Fig. 4.6

- Click **yes** to continue, you will be prompted to insert the CD for the packages required to complete the installation and click OK.

Note: *Before I could do this printer installation, I installed the* ***LPRng-3.8.12-2mdk***

After all packages are installed the next options are presented:

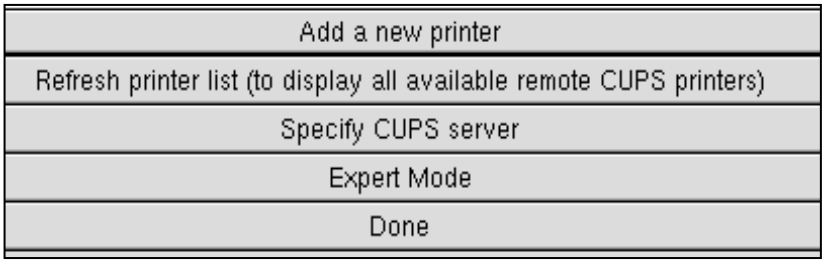


Fig. 4.7

If your printer is not detected in the first screen, you can still try to add it manually.

- Click on Add new printer
- Your welcome printer wizard is displayed
- Select one of the three auto detection options to continue

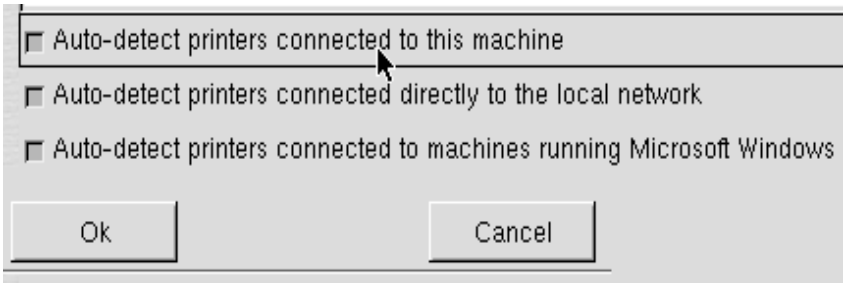


Fig. 4.8

- Click OK

The wizard goes through the detection, and the printer detected will be displayed.

- Make sure the detected printer is selected and **Click Ok**

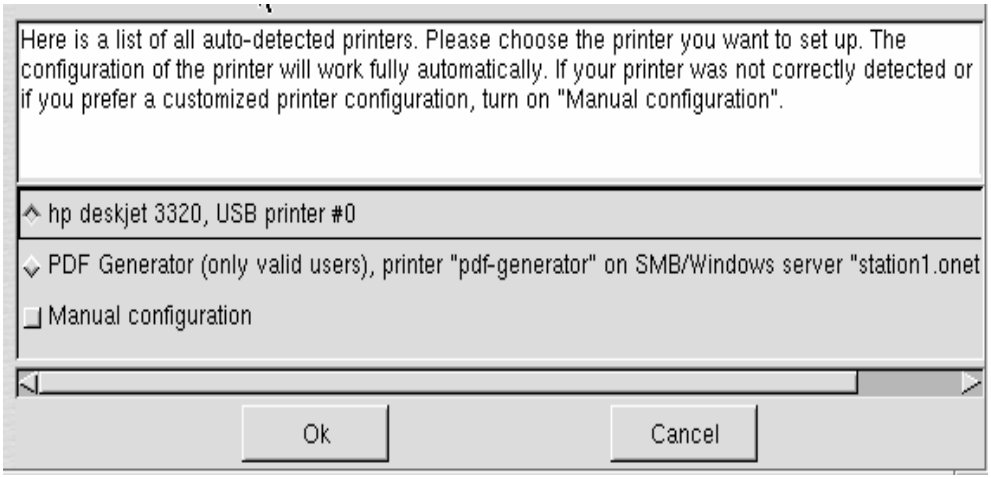


Fig. 4.9

Enter the printer name here and also the printer location if you want.

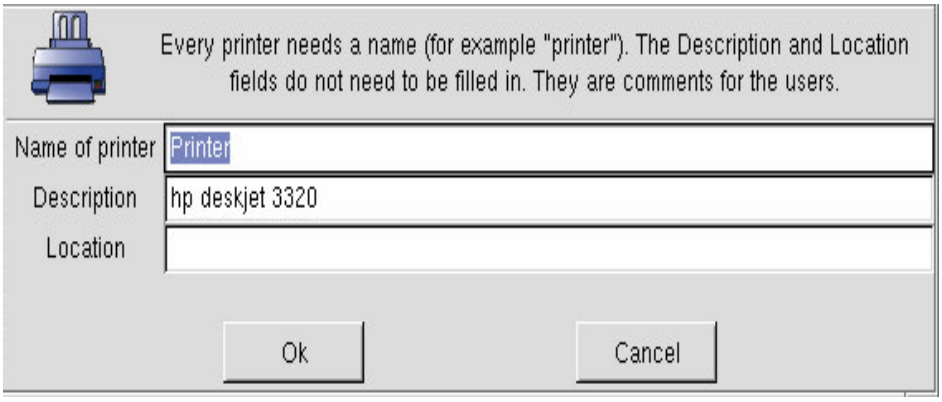


Fig. 4.10

- Click ok to continue

The Printer drake wizard compares the detected printer at the bottom of the detected result you have two options

Fig. 4.11

When you click the **model is correct,** or **Ok** from the manually selection. The print test option is displayed. Select the test option and click on **Print.**
The print test will be sent to the printer and you will receive a message saying, was the print successful?

- If the print test was successful, **answer yes**
- **Click done.**

If you answered no, the printer configuration is displayed to correct the settings.

- Select the print test again
- The print test mode
- Ok
- Close
- Done

Your printer should be now functioning. If for any reason your printer is not working, browse the Internet and find out if your printer is supported.

Installing printers in Expert Mode

If you have CUPS installed you will see it in this menu.

The expert mode basically has two additional features:

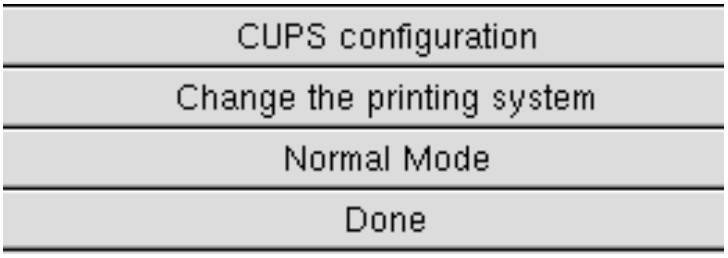


Fig. 4.12

Cups configuration: The cups configuration, display an option for IP address and port number

- And an automatic cups configuration

- **Change the printing system:** This allows you to queue or not to queue.

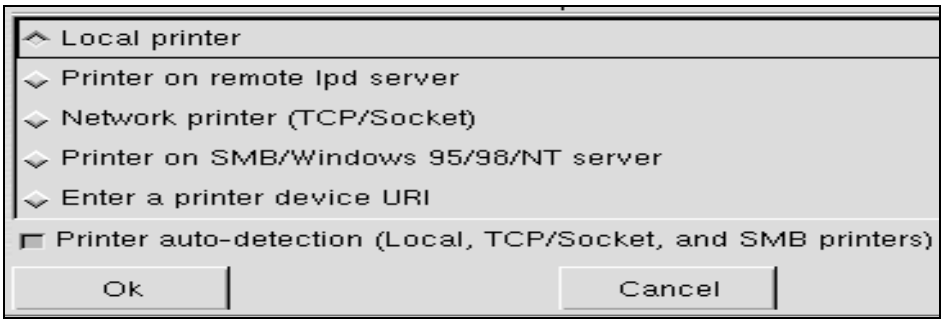


Fig. 4.13

Cups: Common Unix Printing system

PDQ: Print don't queue

If you started your printer installation in expert mode, and you clicked on add printer.

Five different configuration options are available:

- **Local printer:** a printer directly connected to a parallel or USB port. Some printers are not detected automatically but in most cases they will be detected

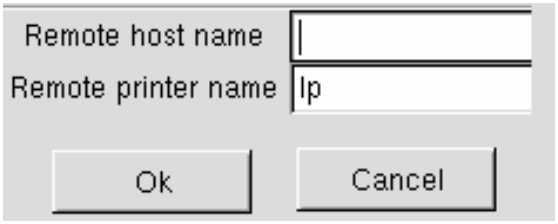


Fig. 4.14

- **Printer on remote lpd server:** A printer already served by another machine

- Enter the host name and the name of the printer exactly as on the remote machine

- **Network printer (TCP/socket):** A printer directly connected to your local network via IP address.

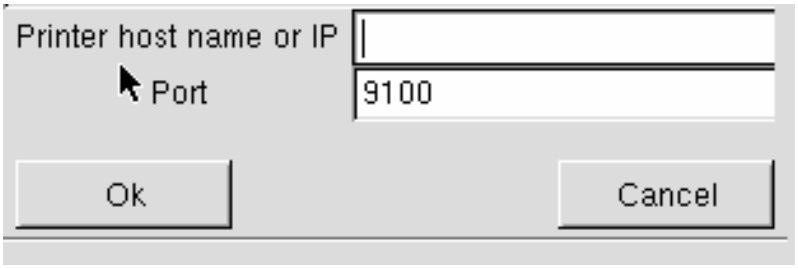


Fig. 4.15

Enter the IP Address of the remote system device. On a JetDirect server the port number is usually 9100.

Samba windows Printer

- **Printer on SMB/Windows 95/98/NT server**: Printers served through remote machines running windows or S*MB* protocol; *Samba* components will be automatically installed in this case.

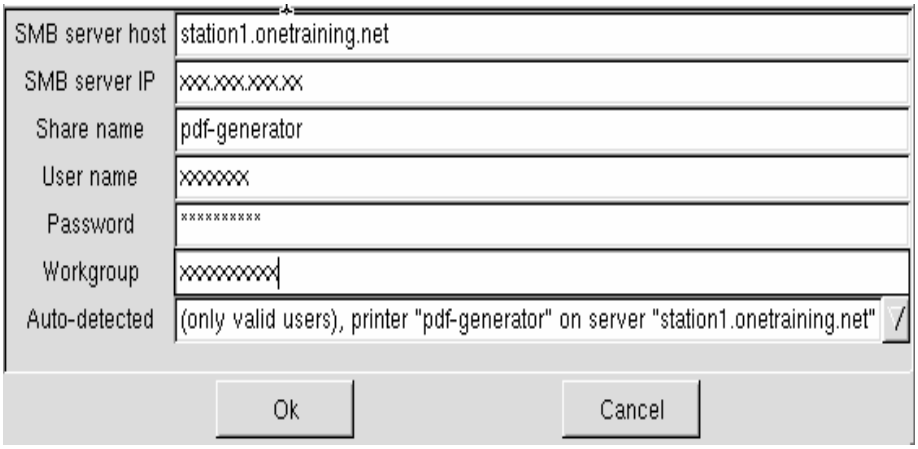


Fig. 4.16

- **Enter a printer device URI**: This option allows you to directly enter the Universal Resource Identifier over the network. It can be used for any of the above remote connections.

A lot of printers are not supported yet, but here is a list that might help you choose your printer when you buy. www.linuxprinting.org This website holds a big database of supported Linux printers.

Installing scanners

When you click the scanner icon the wizard is launched, and asks you to insert the required CD for package installation. Insert the disk and click OK.

If you need to find out if your scanner is supported, you might need to visit mandrake hardware list database at:

http:www.linux-mandrake.com/en/hardware.php

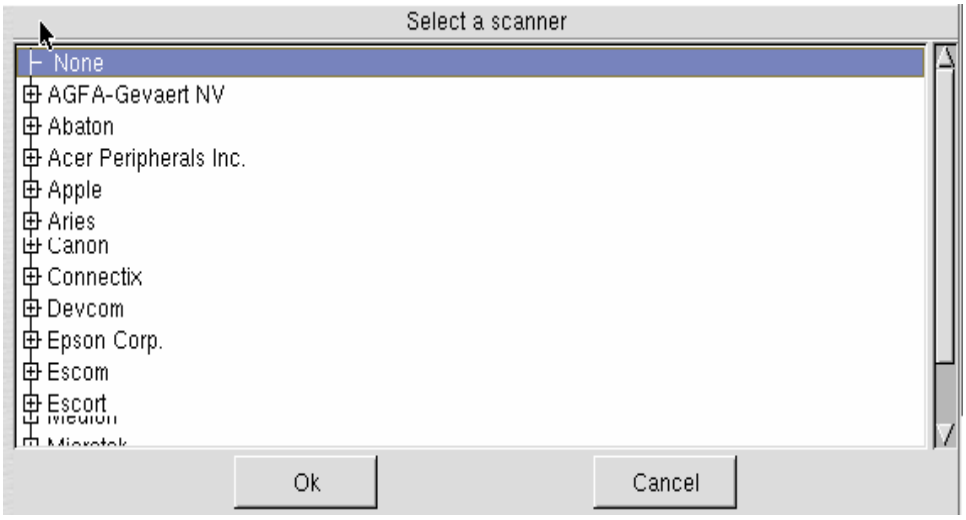


Fig. 4.17

- Select a model and click OK

You will receive **your scanner has been configured** notice. To use the scanner install **Xsane**, (it is an X based interface for SANE (Scanner Access Now Easy) library). This package provides access to scanners, digital cameras and other capture devices.

To install the package, search for Sane in the package installer and install everything including the library related to it.

Managing services

Your most common system administration will be in this section. Things that you don't feel like doing under text mode can be done here.

Services

Controlling services is very important; your system's security depends on it. Running unnecessary services may compromise the system**.** For a better understanding on which services are needed, or for a description, refer to chapter 10.
Services can be also managed by command line (start, stop & restart) or by using Linuxconf to set their run levels.

The following panel allows you to start and stop services. The **on boot** at the middle means that if that button is pressed and you click Ok, that service will be started when the system is powered on.

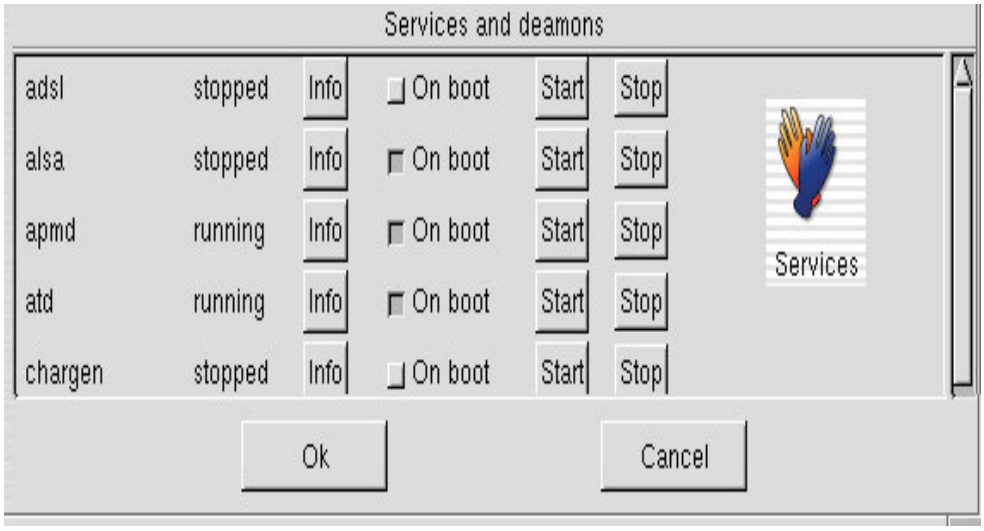


Fig. 4.18

If the button is not pressed, it means that the service is not started automatically. You must have to start it manually when needed.

Note: *If you are looking for a particular service and is not on this panel, this means that the package is not installed. Use the package manager to add the software.*

The Font

This icon is used if you want to change the fonts…

Date and time

This icon is used if you need to adjust the date and time…

The logs

The logs icon is used if you need to monitor a log on a specific date. You can program it here.

The console

This icon drops you to a command line. (Useful -while you are in the control center) You can execute any command.

- Type **exit** to exit from the console

Managing users

This wonderful utility allows you to manage your users.

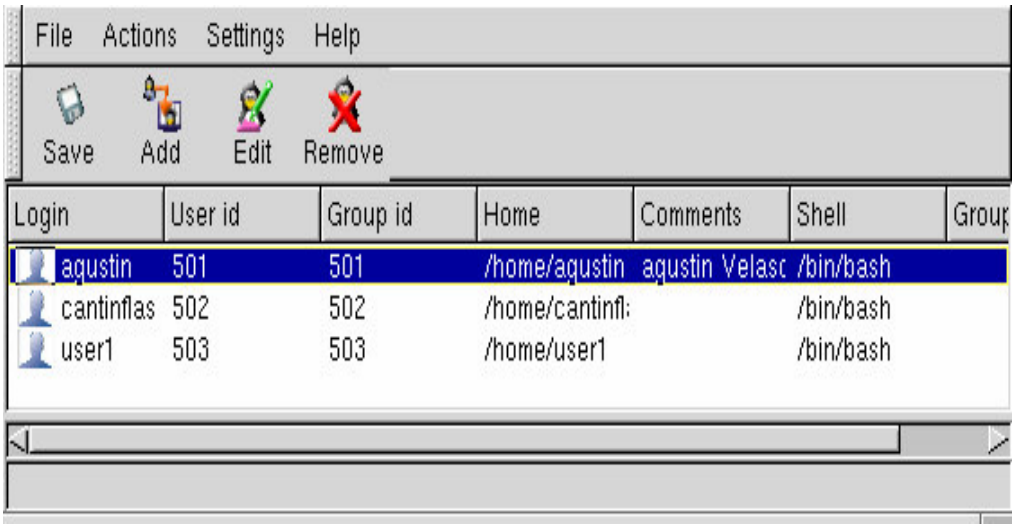


Fig. 4.19

The panel allows you to **add** new users, **edit** users and **remove** users.

- To edit a user's profile, select the user and double click.
- You can also edit a user by clicking the edit button.
- To remove a user, select the user and click on remove.
- If you right click on the user, it displays other options.

Look at this menu it is the same that appears on the action menu. You can reset the password or change the face (icon) etc.

Fig. 4.20

Note: *Back up the users personal files before you delete the user, in case you need them.*

Program scheduler

This programs an application to be executed at a certain time and date. Basically you enter a command to be executed, but the time of execution will depend on the timer you set.

- Select the user under which the command will be executed by.
- Click adds to add a task.
- Use the calendar to schedule the task or activate periodic tasks with the respective parameters.
- Add the command to be executed.
- Click OK.
- Click on add.
- Click on execute so it will be scheduled or quit.

To remove a scheduled task

- Select the scheduled task and Delete or modify accordingly.

Backups

This starts a wizard to back up your file.

- **Wizard Configuration**
- **Advanced Configuration**
- **Backup now**
- **Restore**

The wizard configuration: Gives two options **back up system** or **back up users.**

- To back up a user, click on select a user manually.
- To back up all users, select **back up users**

Backing up all users:

- Select back up users, and click next.
- Select the destination of your backup.

- Click on configure

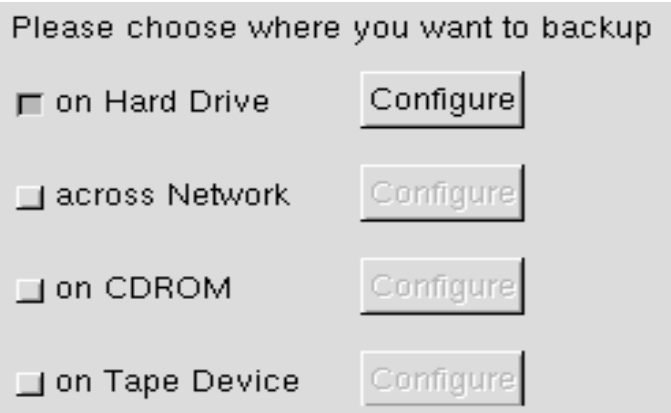


Fig. 4.21

- Configure allows you to set the directory for destination.
- When your settings are correct, click OK to continue.
- You are back to destination selection.

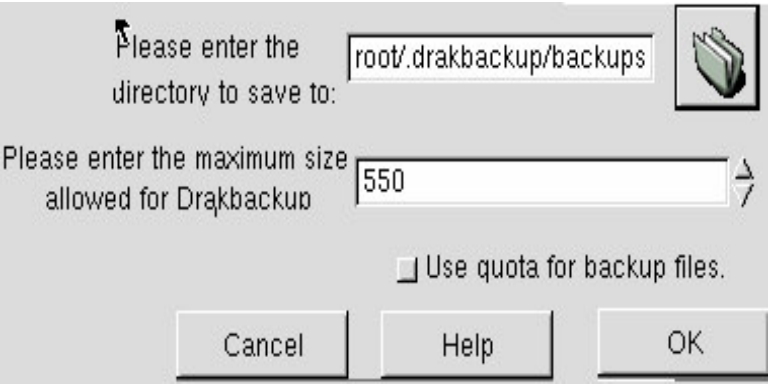
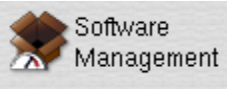


Fig.4.22

- Click next
- Click save
- Backup now from configuration file.
- Click build backup

Your Backup is complete…

Software management



I know how important this is to learn how to add and remove software. If you just starting to learn Linux, you are probably better off if you start learning this package manager.

The package manager is not the only way of installing software; however it makes it much easier than remembering commands. From the graphical interface (desktop), you can double click on any rpm package, and GnoRPM or KPackage will be opened to assist you with the installation.

An RPM consists of three parts: the **archive name**, the **archive version number** and the **version number of the package**.

Thus 'cups-serial-**1.1.16-0**.4**mdk**.i586.rpm' means: 'this package contains an archive called `'cups-serial'`, `version 1.1.16`. It is the fourth revision of this particular package. `'mdk'` denotes the distribution. A package version number has been implemented to keep track of fixes and upgrades.

It is very frequent in the rpm world that you will see packages that come in this form: package-name.**src**.rpm; this is the source code and is of no use to you if you don't know programming. It is provided for those who want to improve it or compile.

Installing packages using commands

If you prefer doing commands this is how it is done:

Example of install:

```
[root@server2 root]#rpm -ivh program-name.rpm
```

Options:

- rpm -i package Installs a package
- rpm -e archive Erases or uninstalls the package
- rpm -U package Upgrades an installed package with newer version
- rpm -v package Verbose mode

Alternatively, you can achieve the installation

```
[root@server2 root]# rpm -i cups-serial-1.1.16-0.4mdk.i586.rpm
```

Example of uninstall

```
[root@server2 root]# rpm -e cups-serial-1.1.16-0.4mdk.i586.rpm
```

Other common uses:

```
rpm -i cups*

rpm -e *gtk*
error: package *gtk* is not installed
```

There are other special modifiers during an installation,

`'--test'` and `'--verbose'` (or `'-v'`).

`'--test'` only executes the command to test the package.

`'--verbose'` (`'-v'`) reports messages on the screen. This is useful in case of errors. It can be used together with the `'--test'` modifier. Adding another `'-v'` (`'-vv'`) increases the level of verbosity even more.

`--force` Same as using `-replacepkgs`, `--replacefile`, and oldpackage.

`--nodeps` Used, generally on special situations, when you must install without dependencies.

`--allfiles` Installs or upgrades all files in the package, regardless if they exist

Querying

root privileges are not a requirement for this:

If you are querying **not-installed packages**, add the '-p' option to the '-q' option.

• rpm -q *archive*	**q**ueries installed package name and version:
• rpm -qp *package*	performs the same on package which isn't installed
• rpm -qi *archive*	**i**nforms about the package, who packaged it when and where, when it has been installed, its size etc.
• rpm -qpi *package*	query a not-installed package
• rpm -ql *archive*	**l**ists all files in an installed package
• rpm -qd *archive*	lists all **d**ocumentation of installed package
• rpm -qa	Lists **a**ll installed packages. Can be used in combination with 'grep'
• rpm -qa --last	lists installed packages sorted by their installation date
• rpm -q --changelog *archive*	Lists changes applied to a package by its maintainer(s).
• rpm -qf *file*	tells you which installed package *file* belongs to

Table 4.1

For more information on rpm, type **man rpm** at your command line.

OK, OK …if you don't feel like typing; then run your **control center** and click on the package manager.

Installing CUPS Using the Package Manager

From the package manager in the control center

- Click on install software

This launches the package manager for software installation….

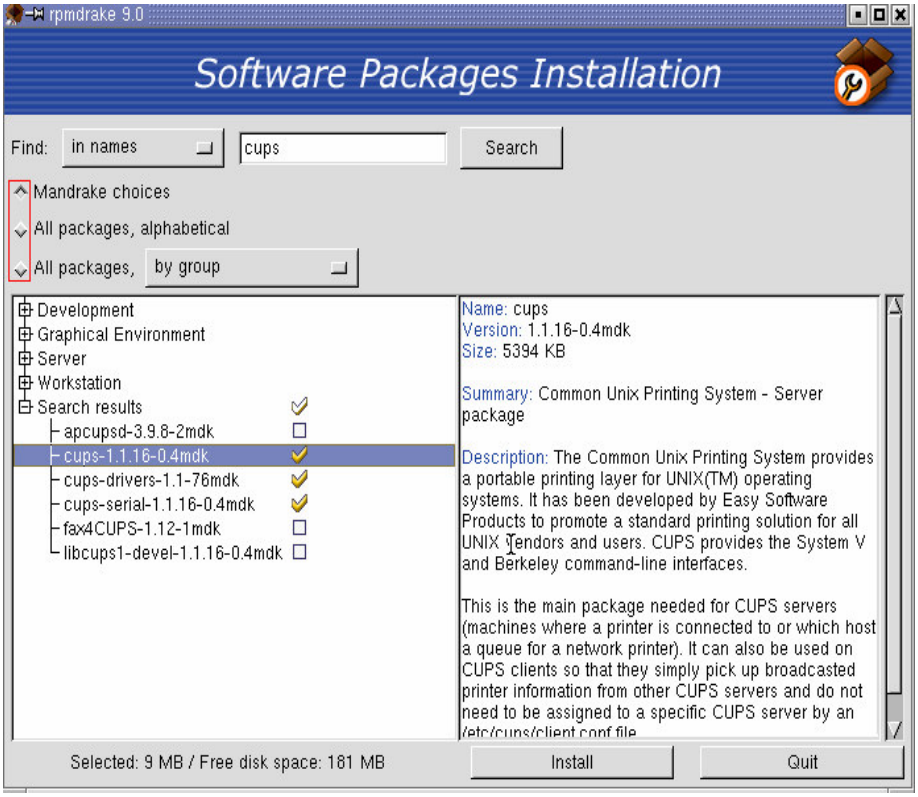


Fig. 4.23

You have three options:

- **Search by choices**
- **List by alphabetical order**, or
- **All packages by group.**

- Leave as default and **enter the name of the application**
- Click on the search button.
- On the search result, click on the correct package

Note: W*hen you click on packages, some of them require additional packages called dependencies. Click on the package and read the description to the right.*

- Click on install
- Enter the appropriate CDs and Click OK

You will be prompted when the installation is finished; you may also see a warning like the following.

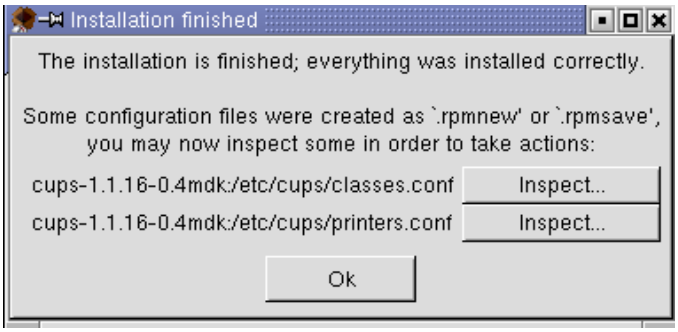


Fig. 4.24

This message appears if you just uninstalled, and are installing it again. If you see this message click on inspect and remove save file; that helps to keep the system clean.

- When finished click Ok.

- Click OK.

  - Go to services and start cups

Note: *You don't usually see this message when you are installing for the first time*.

Uninstalling software/packages

The procedure of uninstall is almost the same, launch the remove software icon the uninstall wizard opens. You can do a search on the package, select the package and click on **Remove**.
After uninstall is complete, just click on **Quit.**

Accessing cups via web browser

The cups server must be installed and **service running** or you won't be able to access it.
There are two ways to start this session:

- **Start** => **Configuration** => **Printing**

  You will have several printing options in your **printing** menu

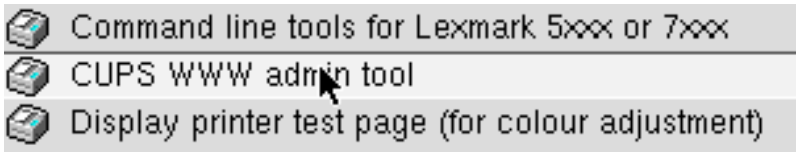


Fig. 4.25

From your menu select **Cups www admin tool**

- **Open your web browser, type the domain name or IP address and port 631**
- **http://localhost:631**
- **www.domain.com:631**
- **IP: 168.34.26.58:631**

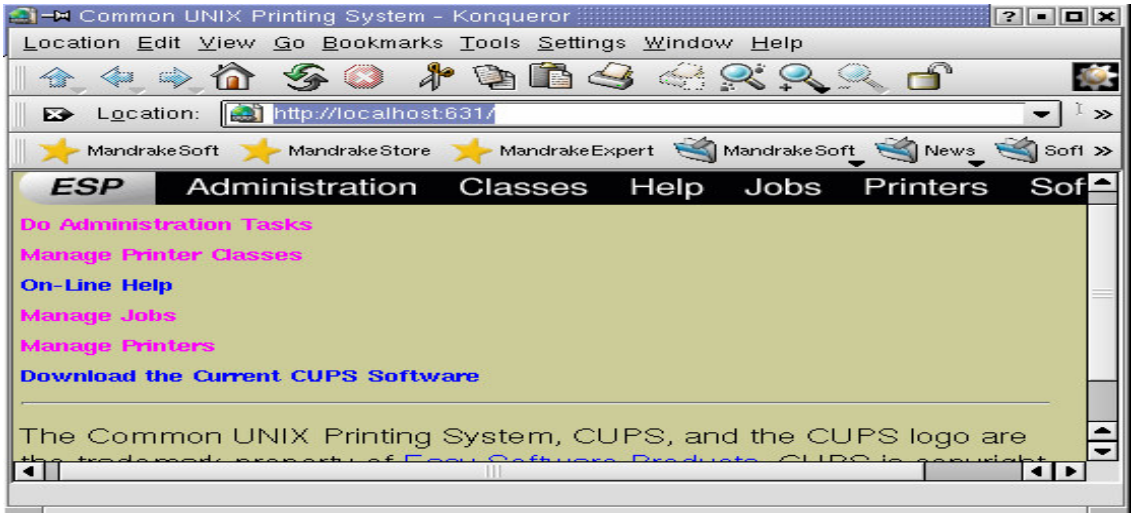


Fig. 4.26
This tool is so easy to use, and you should find your way out without problem.