A
Training Report
at

Jawahar Shikshan Sansthan (JSS), Jodhpur

JSS – PROFILE

Established in 1965, founded by Veteran Educationist Late R.C. Bora, who had a dream of an ideal center to provide quality education to youngsters of nation, Jawahar Shikshan Sansthan is the oldest premier technical education institute in Western Rajasthan. At present, Smt. Asha Dinesh Bora, daughter of freedom fighter Late Shri Gopi Kishan Ji "Kathin" is looking after various activities of the institute.

Keeping the changing scenario in mind, the institute introduced computer education in 1994. The main purpose behind the pioneering step was to impart IT education to every section of the society. This motto was reflected clearly in the functioning of the institute. The institute started computer classes in the old walled city of Jodhpur and fees were retained at the lowest level. Camps and Seminars were also organized time to time in the city with the help and financial assistance from big giants of Industries.

Looking at its reputation, many departments of state government like SCDC, District Industries Centre, Nagar Nigam Jodhpur, Govt. Polytechnic College, Mahila Polytechnic College, and Deptt. of Science & Technology, Rajasthan ordered the institute to conduct free training courses for students. Many extension centres were opened to accommodate increasing number of students. Initially this work was done for Jodhpur city only but afterward many centres were established outside the city including rural areas. Today JSS have 20 ext. centres at different locations of the state where about 1000 students are getting quality technical education. The institute changes its syllabus according to the changing needs of the employment market. The certificate of the institute is well recognized at the Employment Centre.

Besides providing quality technical education, the Sansthan has also opened a "Sahitya Evam Sanskritik Parishad" and many activities have been undertaken by it during last years. The sansthan has also started publishing yearly souvenir and four editions have been published upto the date.

PREFACE

The main aim of practical training is to enhance the technical skills and learn how things are done practically what we have been learning in our college. The practical training gives us an exposure to the real time industry requirements of skillset in today's engineers. Needless to say, I have gained undoubtedly very much from this training and it will surely add to my knowledge about the various system administrtion tasks using Fedora Core Linux.

The title of the training report assigned to me for my industrial training is Linux System Administration. It involved the installation, using, and administration of Fedora Core 4.

I was also assigned the task to study the Installation of Networking and sharing of resources on different platforms across each other. I had to setup and administer networking of computers with various Operating Systems installed like FC4 and Windows 2003 Server and SuSE 10.0.

Nikhil Karnawat
II BE ECE
JECRC

TABLE OF CONTENTS

1. AN OVERVIEW OF FEDORA CORE

OPERATING SYSTEM*:*

An operating system (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications or application programs. The application programs make use of the operating system by making requests for services through a defined application program interface (API). There are variety of basic services needed to operate a computer, some of them are listed below:

FILE SYSTEM:

The file system provides the structure in which information is stored on the Computer.Information is stored in files,primarily on hard disks inside the computer,but also on removable media such as CDs and DVDs. Files are organized within a hierarchy of directories.

DEVICE DRIVERS:

These provide the interface to each of the hardware devices connected to your computer . a device driver enables a program to write to a device without needing to know details about how each piece of hardware is implemented.

USER INTERFACE:

An operating system needs to provide a way for users to run programs and access the file system. There are two types of interfaces one is graphical and another is text based user interfaces.

SYSTEM SERVICES:

An operating system provides system services, many of which can be started automatically when computer boots. It include processes that mount file system, start our network , and run schedule tasks.

WHAT IS LINUX ?

Linux is the core, or kernel, of a free operating system first developed and released to the world by Linus Benedict Torvalds in 1991. Torvalds, then a graduate student at the University of Helsinki, Finland, is now a Fellow at the Open Source Development Lab .He is an engineer and had previously worked for the CPU design and fabrication company Transmeta, Inc. Fortunately for all Linux users, Torvalds chose to distribute Linux under a free software license named the GNU General Public License (GPL). Linux is the free version of Unix.

Linux, pronounced "lih-nucks," is free software. Combining the Linux kernel with GNU software tools—drivers, utilities, user interfaces, and other software such as The X.Org Foundation's X Window System—creates a Linux distribution. There are many different Linux distributions from different vendors, but many are derived from or closely mimic Red Hat's distribution of Linux—Red Hat Linux.

Today ,there are thousands of software developers around the world contributing software to the open source community that feeds the Linux initiative . Because the software is freely available ,anyone can work on it,change it,or enhance it.

SOME COMMON LINUX FEATURES :

MULTIUSER :

We can have multiple user logged in and working on the system at the same time,user can have their on environments arranged in the way they want : their own home directories for storing files and their own desktop interface.User account can be password protected,so that user can control who has access to their applications and data.

MULTI –TASKING :

In Linux, it is possible to have many programs running at the same time,which means that not only user have many programs going at once,but that the linux operating system can itself have programs running in the background.

NETWORKING CONNECTIVITY :

To connect linux system to network ,Linux offers support for a variety of locl area network(LAN)cards,modems,and serial devices.In addition toLAN protocols ,such as Ethernet ,all the most popular upper level networking protocols can be built-in.The most popular of these protocols is TCP/IP.Other protocols,such as IPXand X.25 are also available.

NETWORK SERVERS :

Providing networking services to the client computers on the LAN or the entire internet is what Linux does best. A variety of software packages are available that enable user to use linux as a print server,file server,mail server ,FTP server,web server,news server,workgroup(DHCP or NIS) server.

APPLICATION SUPPORT :

Because of compatibility with posix and several different programming interfaces,a wide range of freeware and software is available for Linux.

HARDWARE SUPPORT:

User can configure support for almost every type of hardware that can be connected to the computer. there is support for floppy disk drives, CD-ROM’S, pen drives, sound cards etc

WHY USE LINUX ?

Over the last year, many individuals; small office/home office (SOHO) users; businesses; corporations; colleges; nonprofits; and local, state, and federal agencies in a number of countries have incorporated Linux with great success. And today, Linux is being incorporated into many IS/IT environments as part of improvements in efficiency, security, and cost savings. Using Linux is a good idea for a number of reasons. These reasons include

- Linux provides an excellent return on investment (ROI)— There is little or no cost on a per-seat basis. Unlike commercial operating systems, Linux has no royalty or licensing fees and a single Linux distribution on CD-ROM can form the basis of an enterprise-wide software distribution, replete with applications and productivity software. Custom corporate CD-ROMs can be easily crafted to provide specific installs on enterprise-wide hardware. This feature alone can save hundreds of thousands, if not millions, of dollars in information service/information technology costs—all without the threat of a software audit from the commercial software monopoly or the need for licensing accounting and controls of base operating system installations.

- Linux can be put to work as a server platform— Linux is fast, secure, stable, scalable, and robust. Latest versions of the Linux kernel easily support multiple-processor computers (optimized for eight CPUs), large amounts of system memory (up to 64GB RAM), individual file sizes in excess of hundreds of gigabytes, a choice of modern journaling file systems, hundreds of process monitoring and control utilities, and the (theoretical) capability to simultaneously support more than four billion users. IBM, Oracle, and other major database vendors all have versions of their enterprise software available for Linux.

- Linux has a low entry and deployment cost barrier— Maintenance costs can also be reduced because Linux works well on a variety of PCs, including legacy hardware, such as some Intel-based 486 and early Pentium CPUs. Although the best program performance will be realized with newer hardware because clients can be recompiled and optimized for Pentium-class CPUs, base installs can even be performed on lower-end computers or embedded devices with only 8MB of RAM. This feature provides for a much wider user base; extends the life of older working hardware; and can help save money for home, small business, and corporate users.

Linux provides a royalty-free development platform for cross-platform development—Because of the open-source development model and availability of free, high-quality development tools, Linux provides a low-cost entry point to budding developers and tech industry startups.

IS LINUX DIFFICULT?

Whether Linux is difficult to learn depends on the person you're asking. Experienced UNIX users will say no, because Linux is an ideal operating system for power-users and programmers, because it has been and is being developed by such people.

Everything a good programmer can wish for is available: compilers, libraries, development and debugging tools. These packages come with every standard Linux distribution. The C-compiler is included for free, all the documentation and manuals are there, and examples are often included to help you get started in no time. It feels like UNIX and switching between UNIX and Linux is a natural thing.

In the early days of Linux, being an expert was kind of required to start using the system. Those who mastered Linux felt better than the rest of the "lusers" who hadn't seen the light yet. It was common practice to tell a beginning user to "RTFM" (read the manuals). While the manuals were on every system, it was difficult to find the documentation, and even if someone did, explanations were in such technical terms that the new user became easily discouraged from learning the system.

The Linux-using community started to realize that if Linux was ever to be an important player on the operating system market, there had to be some serious changes in the accessibility of the system.

LINUX FOR NON-EXPERIENCED USERS

Companies such as RedHat, SuSE and Mandrake have sprung up, providing packaged Linux distributions suitable for mass consumption. They integrated a great deal of graphical user interfaces (GUIs), developed by the community, in order to ease management of programs and services. As a Linux user today you have all the means of getting to know your system inside out, but it is no longer necessary to have that knowledge in order to make the system comply to your requests.

Nowadays you can log in graphically and start all required applications without even having to type a single character, while you still have the ability to access the core of the system if needed. Because of its structure, Linux allows a user to grow into the system: it equally fits new and experienced users. New users are not forced to do difficult things, while experienced users are not forced to work in the same way they did when they first started learning Linux.

While development in the service area continues, great things are being done for desktop users, generally considered as the group least likely to know how a system works. Developers of desktop applications are making incredible efforts to make the most beautiful desktops you've ever seen, or to make your Linux machine look just like your former MS Windows or MacIntosh workstation. The latest developments also include 3D acceleration support and support for USB devices, single-click updates of system and packages, and so on. Linux has these, and tries to present all available services in a logical form that ordinary people can understand.

The screenshot below shows how each item in the Channel list (RH 7.2, StarOffice, Opera, Ximian Gnome, Loki games and CodeWeavers) can be updated with one mouse click. Adding or removing software packages or keeping the system up to date is simple with tools like this one, called Red Carpet:

DOES LINUX HAVE A FUTURE?

Open Source

The idea behind Open Source software is rather simple: when programmers can read, distribute and change code, the code will mature. People can adapt it, fix it, debug it, and they can do it at a speed that dwarfs the performance of software developers at conventional companies. This software will be more flexible and of a better quality than software that has been developed using the conventional channels, because more people have tested it in more different conditions than the closed software developer ever can.

The Open Source initiative started to make this clear to the commercial world, and very slowly, commercial vendors are starting to see the point. While lots of academics and technical people have already been convinced for 20 years now that this is the way to go, commercial vendors needed applications like the Internet to make them realize they can profit from Open Source. Now Linux has grown past the stage where it was almost exclusively an academic system, useful only to a handful of people with a technical background. Now Linux provides more than the operating system: there is an entire infrastructure supporting the chain of effort of creating an operating system, of making and testing programs for it, of bringing everything to the users, of supplying maintenance, updates and support and customizations, etcetera. Today, Linux is ready to accept the challenge of a fast-changing world.

TEN YEARS OF EXPERIENCE AT OUR SERVICE

While Linux is probably the most well-known Open Source initiative, there is another project that contributed enormously to the popularity of the Linux operating system. This project is called SAMBA, and its achievement is the reverse engineering of the Server Message Block (SMB)/Common Internet File System (CIFS) protocol used for file- and print-serving on PC-related machines, natively supported by MS Windows NT and OS/2, and Linux. Packages are now available for almost every system and provide interconnection solutions in mixed environments using MS Windows protocols: Windows-compatible (up to and including Win2K) file- and print-servers.

Maybe even more successful than the SAMBA project is the Apache HTTP server project. The server runs on UNIX, Windows NT and many other operating systems. Originally known as "A PAtCHy server", based on existing code and a series of "patch files", the name for the matured code deserves to be connoted with the native American tribe of the Apache, well-known for their superior skills in warfare strategy and inexhaustible endurance. Apache has been shown to be substantially faster, more stable and more feature-full than many other web servers. Apache is run on sites that get millions of visitors per day, and while no official support is provided by the developers, the Apache user community provides answers to all your questions. Commercial support is now being provided by a number of third parties.

In the category of office applications, a choice of MS Office suite clones is available, ranging from partial to full implementations of the applications available on MS Windows workstations. These initiatives helped a great deal to make Linux acceptable for the desktop market, because the users don't need extra training to learn how to work with new systems. With the desktop comes the praise of the common users, and not only their praise, but also their specific requirements, which are growing more intricate and demanding by the day.

The Open Source community, consisting largely of people who have been contributing for over half a decade, assures Linux' position as an important player on the desktop market as well as in general IT application. Paid employees and volunteers alike are working diligently so that Linux can maintain a position in the market. The more users, the more questions. The Open Source community makes sure answers keep coming, and watches the quality of the answers with a suspicious eye, resulting in ever more stability and accessibility.

Listing all the available Linux software is beyond the scope of this guide, as there are tens of thousands of packages. Throughout this course we will present you with the most common packages, which are almost all freely available. In order to take away some of the fear of the beginning user, here's a screenshot of one of your most-wanted programs. You can see for yourself the Properties of Linux

LINUX PROS

A lot of the advantages of Linux are a consequence of Linux' origins, deeply rooted in UNIX, except for the first advantage, of course:

Linux is free:

As in free beer, they say. If you want to spend absolutely nothing, you don't even have to pay the price of a CD. Linux can be downloaded in its entirety from the Internet completely for free. No registration fees, no costs per user, free updates, and freely available source code in case you want to change the behavior of your system.

Most of all, Linux is free as in free speech:

The license commonly used is the GNU Public License (GPL). The license says that anybody who may want to do so, has the right to change Linux and eventually to redistribute a changed version, on the one condition that the code is still available after redistribution. In practice, you are free to grab a kernel image, for instance to add support for teletransportation machines or time travel and sell your new code, as long as your customers can still have a copy of that code.

- *Linux is portable to any hardware platform*:

A vendor who wants to sell a new type of computer and who doesn't know what kind of OS his new machine will run (say the CPU in your car or washing machine), can take a Linux kernel and make it work on his hardware, because documentation related to this activity is freely available.

- *Linux was made to keep on running*:

As with UNIX, a Linux system expects to run without rebooting all the time. That is why a lot of tasks are being executed at night or scheduled automatically for other calm moments, resulting in higher availability during busier periods and a more balanced use of the hardware. This property allows for Linux to be applicable also in environments where people don't have the time or the possibility to control their systems night and day.

- *Linux is secure and versatile*:

The security model used in Linux is based on the UNIX idea of security, which is known to be robust and of proven quality. But Linux is not only fit for use as a fort against enemy attacks from the Internet: it will adapt equally to other situations, utilizing the same high standards for security. Your development machine or control station will be as secure as your firewall.

- *Linux is scalable*:

From a Palmtop with 2 MB of memory to a petabyte storage cluster with hundreds of nodes: add or remove the appropriate packages and Linux fits all. You don't need a supercomputer anymore, because you can use Linux to do big things using the building blocks provided with the system. If you want to do little things, such as making an operating system for an embedded processor or just recycling your old 486, Linux will do that as well.

- *The Linux OS and Linux applications have very short debug-times*:

Because Linux has been developed and tested by thousands of people, both errors and people to fix them are found very quickly. It often happens that there are only a couple of hours between discovery and fixing of a bug.

LINUX CONS

There are far too many different distributions:
"Quot capites, tot rationes", as the Romans already said: the more people, the more opinions. At first glance, the amount of Linux distributions can be frightening, or ridiculous, depending on your point of view. But it also means that everyone will find what he or she needs. You don't need to be an expert to find a suitable release.
When asked, generally every Linux user will say that the best distribution is the specific version he is using. So which one should you choose? Don't worry too much about that:

all releases contain more or less the same set of basic packages. On top of the basics, special third party software is added making, for example, TurboLinux more suitable for the small and medium enterprise, RedHat for servers and SuSE for workstations. However, the differences are likely to be very superficial. The best strategy is to test a couple of distributions; unfortunately not everybody has the time for this. Luckily, there is plenty of advice on the subject of choosing your Linux. One place is LinuxJournal, which discusses hardware and support, among many other subjects. The Installation HOWTO also discusses choosing your distribution.

Linux is not very user friendly and confusing for beginners:

In light of its popularity, considerable effort has been made to make Linux even easier to use, especially for new users. More information is being released daily, such as this guide, to help fill the gap for documentation available to users at all levels.

- *Is an Open Source product trustworthy*?

How can something that is free also be reliable? Linux users have the choice whether to use Linux or not, which gives them an enormous advantage compared to users of proprietary software, who don't have that kind of freedom. After long periods of testing, most Linux users come to the conclusion that Linux is not only as good, but in many cases better and faster that the traditional solutions. If Linux were not trustworthy, it would have been long gone, never knowing the popularity it has now, with millions of users. Now users can influence their systems and share their remarks with the community, so the system gets better and better every day. It is a project that is never finished, that is true, but in an ever changing environment, Linux is also a project that continues to strive for perfection.

2. INSTALLING FEDORA CORE

QUICK INSTALLATION

If we have a little bit of experience with computers and computer with common hardware ,we can probably install Fedora easily.

REQUIREMENTS :

- A Pentium –class PC (at least 200 Mhz. For text mode ;400MHz Pentium II for GUI) with a built –in, bootable DVD or CD drive, at least 64 MB of RAM(for text mode)or 192 MB of RAM(for GUI mode)
- User need at least 620 MB of free hard disk space for Minimal custom install,at least 23 Gbof free space for workstation install,and atleast 1.1 GB for a server install. A custom everything install require at least 6.9 GB of hard disk.

HOW TO GET START :

- Insert Fedora installation DVD or CD#1 into computer's drive.
- Reboot computer.
- When user see the installation screen (with a boot: prompt at the bottom),press the enter key to begin installation.

During installation ,user are asked questions about user computer hardware and the network connections.after user has completed each answer ,click NEXT.
The following list describes the information user will need to enter .

- *Media Check* – Optionally check the DVD to be sure it is not damaged or corrupted .
- *Language Selection* – Choose the language used during the install.
- *Keyboard Configuration* – Choose user keyboard type.
- *Upgrade* – If user have an earlier version of Fedora installed ,user can choose Upgrade to upgrade user system without losing data files. Otherwise user can continue with a new installation.
- *Installation Type* – Choose a configuration, such as Personal Desktop ,workstation, server or custom
- *Disk partitioning Setup* – either have Fedora automatically choose user partitions or user himself create partition.
- *Disk Druid* – whether user choose Automatic or Manual partitioning,Disk Druid appears on screen to let user review or change the partitions.
- *Boot Loader Configuration*—Add the GRUB boot manager to control the boot process .with multiple operating systemon the computer ,select which one to boot by default.
- *Network Configuration*—set up the LAN connection .user can simply choose to get addresses using DHCP,or user can manually enter his computer's IP address,netmask, hostname, default gateway,and DNS servers .
- *Firewall Configuration*—Choose a default firewall configuration. Select Enable firewall if user want to block access to most services to user computer from from outside computer . if user do enable the firewall, user can select to open particular services to computers on network user can also enable Security Enhanced Linux to protect user system from attacks on selected services.
- *Time Zone Selection* – Identify the time zone in which user are located.
- *Set Root Password* –Add the root user account password.

- *Package Installation Defaults* – Select to install the current package list or customize it. For custom installations, choose groups of software packages to install, choose everything or choose Minimal.
- *About To Install*—to this point ,user can quit the install process without having written anything to disk. When user select Next , the disk is formatted and selected packages are installed.

When installation is done,remove thev Fedora DVD or CD and click to EXIT to reboot user computer .Linux should boot by defaultAfter Linux boots for the fiert time ,the fedora setup agent runs to let user read the license agreement, set the system date and time,configure user display,add a user account, configure your sound card, and install additional CDs. On subsequent reboots ,user will see a login prompt.user can log in and begin using Linux system.

DETAILED INSTALLAION INSTRUCTIONS:

- *Install Or Upgrade* **?**

First user should determine if he is doing a a new install or an upgrade.If user is upgrading an existing Red Hat Linux or Fedora system to the latest version, the installation process will try to leave user data files and configurations files intact as much as possible.This type of installation takes longer than a new install.A new install will simply erase all data on the Linux partitions that user choose.If user choose upgrade ,user can save time by removing software packages user don’t need.

- *From DVD/CD,network,or hard disk?*

There are many different ways to install Fedora Core, and selecting an installation method might depend on the equipment on hand, existing bandwidth, or equipment limitations.

Here are some of the most commonly used installation methods:

- *CD-ROM/DVD*— Using a compatible CD-ROM or DVD drive attached to the computer (laptop users with an external CD-ROM drive will need PCMCIA support from a driver disk image included under the first CD-ROM's `images` directory).
- *DOS*— By using LOADLIN, you can boot to a Linux install by pointing LOADLIN to use a Fedora installation kernel and ramdisk. Run the DOS batch file, `autoboot.bat`, found under the `dosutils` directory on the first Fedora CD-ROM or DVD.
- *Network File System* (NFS)— You can install Fedora from a remotely mounted hard drive containing the Fedora Core software. To do this installation, you need to have an installed and supported network interface card, along with a boot floppy with network support. (You learn how to make boot floppies later in this section of the chapter.)
- *File Transfer Protocol* (FTP)— As with an NFS install, installation via FTP requires that the Fedora software be available on a public FTP server. You also need an installed and supported network interface card, along with a boot floppy with network support.
- *Hypertext Transport Protocol* (HTTP)— As with the FTP and NFS installs, installation via HTTP requires that the Fedora software be available on an accessible website. You also need an installed and supported network interface card, along with a boot floppy with network support.
- *Installation via the Internet*— If you have the bandwidth, it may also be possible to install Fedora via the Internet; however, this method might not be as reliable as

using a Local Area Network (LAN) because of availability and current use of Fedora Project or other servers on mirror sites.

- *A hard drive partition*— By copying the .iso images to a hard drive partition, you can then boot to an install.
- *Preinstalled media*— It is also possible to install Linux on another hard drive and then transfer the hard drive to your computer. This is handy, especially if your site uses removable hard drives or other media.

CHOOSING COMPUTER HARDWARE

To install a 32-bit PC version of Fedora successfully, the computer must have the following:

1. *X86 Proccessor* – User computer needs an intel CPU. With the latest version, Fedora recommends that user have at least a Pentium –class processor to run Fedora. For a text –only installation, a 200 MHz Pentium is the minimum, while a 400 MHz Pentium II is the minimum for a GUI installation.
2. *DVD or CD-ROM drive* : user needto be able to boot up the installation process from a DVD,CD-ROM,or other bootable drive.Once user have booted from one of the media just described, user can use a LAN connection to install Fedora Core software packages from a server on the network or figure out a way to copy the contents of the DVD to a local hard disk to install from there.
3. *HARD DISK*-

The Fedora installer offers a choice of installation types or classes, and each has its own hard drive storage requirements:

- *Workstation*— You'll need a minimum of 3GB hard drive storage, but much more if you choose to install everything. This installation is intended for developers and other users who want to use the entire spectrum of Linux software offered by the distribution.
- *Personal Desktop*— This is a new installation class for SOHO (small office/home office) users that installs a basic graphical desktop, along with requisite office and

Internet productivity software; you'll need around 2.3GB of storage if you don't customize the default software selections.

- *Server*— You need at least 1.1GB of storage for the operating system and server software, but you also must take into consideration other storage requirements. For example, if you plan to run a website with a lot of graphics or serve other files, you might need to add storage to your system or accommodate remotely mounted storage locally.
- *Custom*— This installation supports a minimal install requiring a little over 600MB; however, you can also choose to install all the software in the distribution; in which case, you'll need 7GB or more of storage, along with several hundred megabytes of free space for temporary files.

4. *RAM* – User should have at leastb 64 MB of RAM to install Fedora core. If user is running in graphical mode ,user will want at least 192 MB .
5. *KEYBOARD AND MONITOR*- User need only a keyboard and a monitor during installation . user can operate Fedora core quite well over a LAN using either a shell interface from a network login or an X terminal.

BEGINNING THE INSTALLATION

Step-by-Step Installation

This section provides a basic step-by-step installation of Fedora from CD-ROM. There are many different ways to proceed with an install, and the installer can provide a graphical or text-based interface in a variety of modes.

This example installation prepares a computer for general duties as a server, perhaps to host a File Transfer Protocol (FTP) site, a web server using Apache, or Session Message Block (SMB) services using Samba.

Before you begin, you should ensure that your computer is not connected to the Internet. Although you can use the installer to set up network protection during the install, it is best to check your system settings after any install and before opening up any public services

TIP

If you are installing to a system that has an older display monitor, it is a good idea to have your monitor's manual handy during the installation. If the install does not detect your monitor settings, you might need to specify the monitor's vertical and horizontal frequencies. This does not happen often, but if it does, you will be prepared.

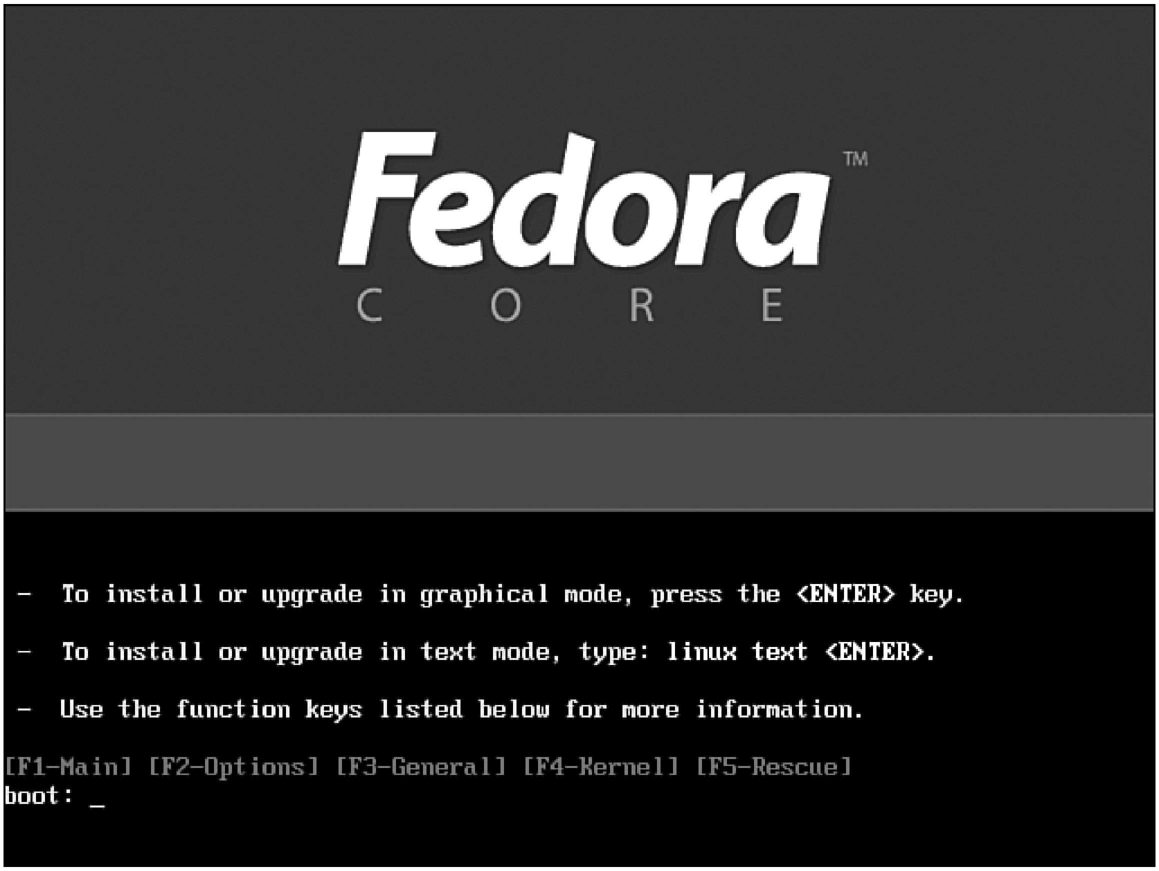
NOTE

Fedora's graphical installation dialogs are convenient and easy to use. However, you can use a text-based installation, which works with any PC. Simply specify `linux text` at the install boot prompt. Use the graphical install outlined here as a starting point for learning more about installing Fedora.

Starting the Install

To get started, insert the first Fedora disc and reboot your computer. You'll first see a boot screen that offers a variety of options for booting. Options may be passed to the Linux install kernel by typing special keywords at the boot prompt. Note that the install kernel is different from the kernel that will be installed on your system during installation!

. Select an installation option in this first Fedora Core boot screen.



```
-  To install or upgrade in graphical mode, press the <ENTER> key.

-  To install or upgrade in text mode, type: linux text <ENTER>.

-  Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _
```

The basic options most often used are

- `<ENTER>`— Starts the install using a graphical interface. The graphical interface supports a mouse and offers check boxes and text fields for choosing software, configuring options, and entering information.
- `linux text`— Starts the install using a graphical text interface.

To install using a text-based interface (used for our example), type `linux text` and press Enter; otherwise, just press Enter to start the install.

Several function keys can be used at this first boot screen to cycle through four help screens providing additional install information. Use these function keys at the boot prompt to jump to different screens describing alternative installation options and modes:

Pressing F1 returns to the initial boot screen.

Pressing F2 details some boot options.

Pressing F3 gives general installation information (described next in this chapter).

Pressing F4 describes how to pass kernel video arguments, useful for configuring video hardware to support a graphical install at a specific resolution (such as 800 x 600 pixels).

Pressing F5 describes Fedora's rescue mode.

Some of the options you can use at the boot prompt include

linux noprobe— Disables probing of the system's hardware.

linux mediacheck— Verifies the integrity of one or more install CD-ROMs.

linux rescue— Boots to single-user mode with a root operator prompt, disabling X, multitasking, and networking; this option can be used if you need to reconfigure your boot loader or to rescue data from your system.

linux dd— Uses a driver disk (a floppy image) and possibly one or more kernel arguments (such as `linux mem=512M expert`) to enable certain types of hardware, such as networking cards.

linux askmethod— Prompts for the type of install to perform, such as over a network.

linux updates— Starts an installation update.

memtest86— Starts a cyclical, intensive series of memory tests of your PC's RAM.

linux nofb— Starts a graphical installation, but does not use a framebuffer (*helpful with problematic or unsupported video).*

linux resolution=width x height— Installs using a graphical display of width-by-height pixels (such as `resolution=800x600`), which can help match older or less capable display monitors and video cards.

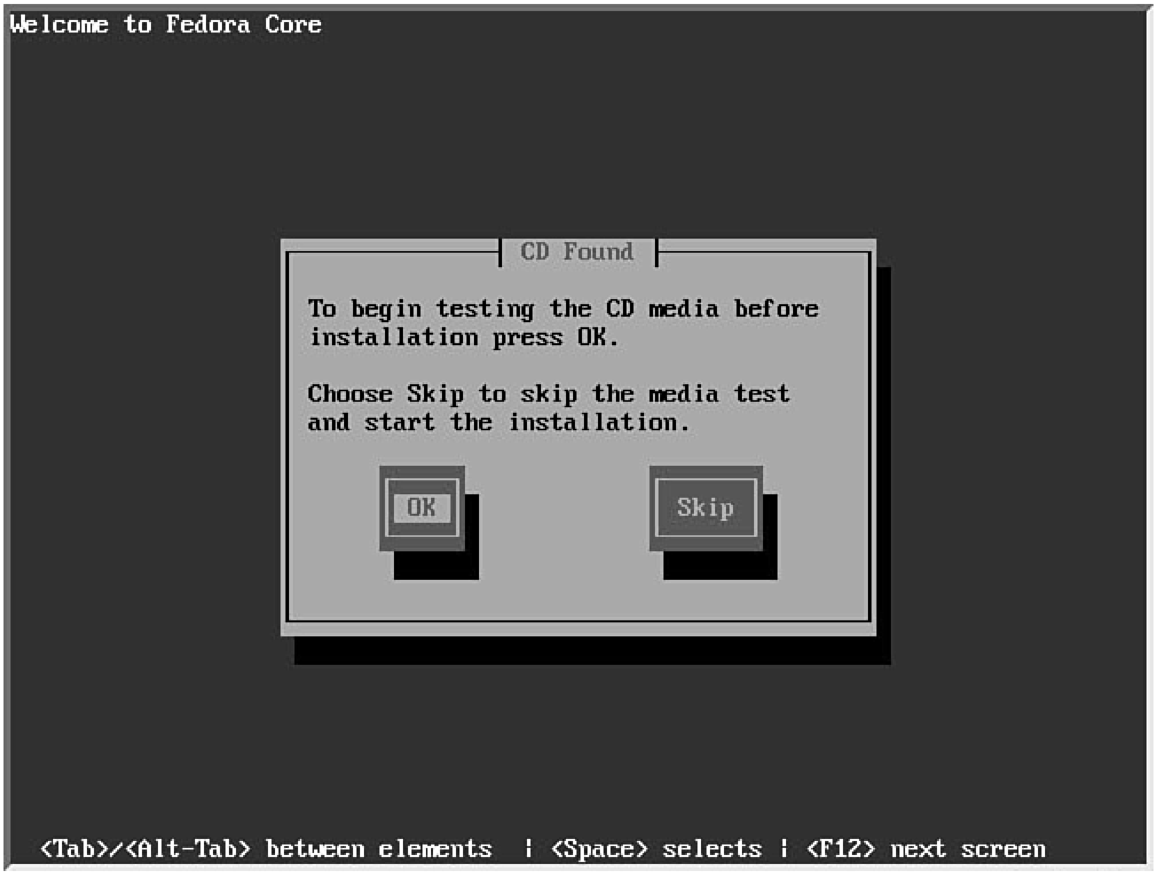
The F4 screen lists options that can be used at the boot prompt to set a specific resolution for the installation. For example, this is done by typing `linux resolution=` at the boot prompt, along with an option such as `"800x600"`. Other options, such as optional arguments for kernel modules (in order to properly configure or initialize hardware) may be passed to the install kernel if you use the noprobe option.

TIP

The installer will start automatically in 60 seconds. Press the spacebar, reboot, or turn off your PC if you need to halt the install.

After you press Enter, the installer's kernel loads, and you're asked (in a text-based screen) if you would like to perform a media check of your CD-ROM,

You can check your CD-ROM media before installing Fedora.

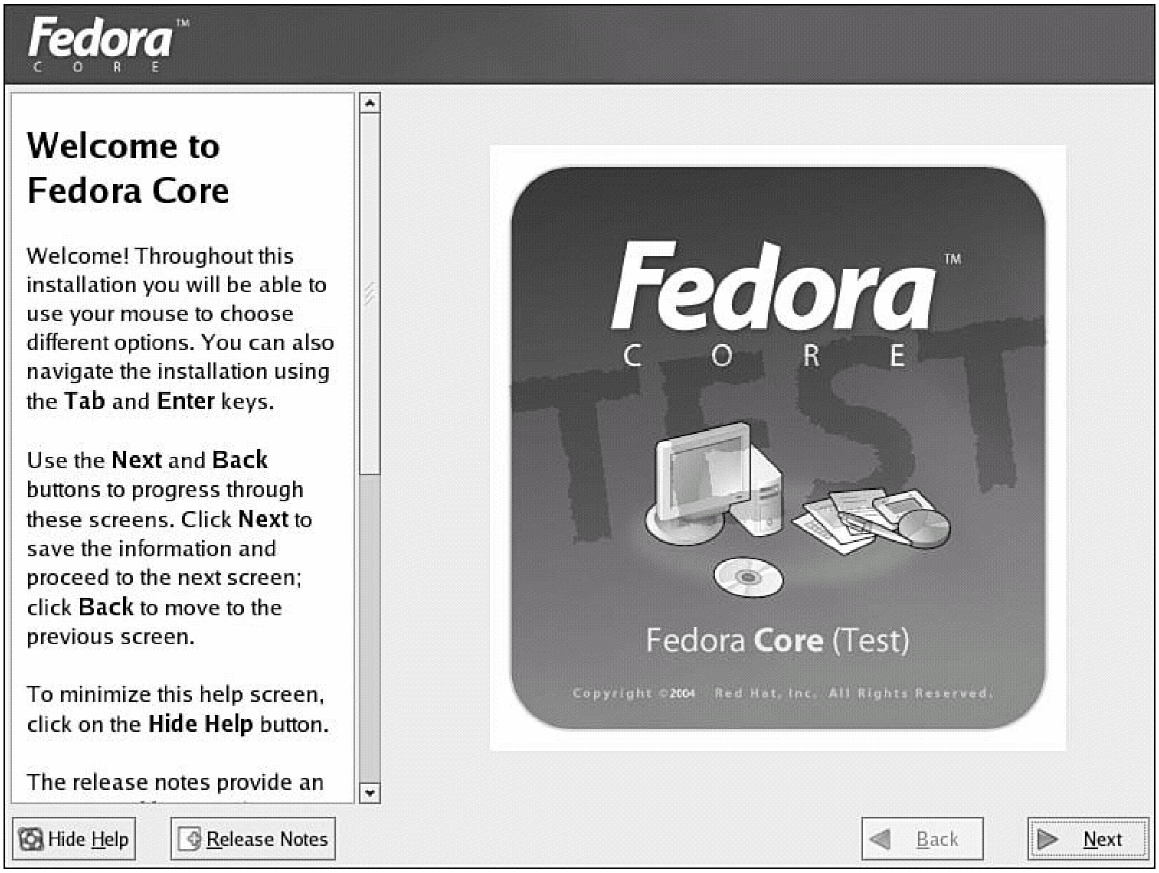


```
Welcome to Fedora Core

CD Found

To begin testing the CD media before
installation press OK.

Choose Skip to skip the media test
and start the installation.

<Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

This check can take quite some time (depending on the speed of your CD drive), but can ensure the integrity of the CD-ROM's contents, as an md5sum value is embedded on each CD-ROM. This check can help foil installation of malicious software from CD-ROMs with tampered contents. The check can also be helpful to make sure that the CD-ROM you are using will work on your PC and in your CD drive. To perform the check, choose OK; otherwise, use the Tab key to navigate to the Skip button and press Enter to choose it.

After checking your CD-ROM or skipping the check, the display will clear. The Fedora installer, Anaconda, will load, and you are presented with a graphical welcome screen as. The installer should recognize your PC's graphics hardware and mouse. You can then click on the Release Notes button to get detailed information about Fedora Core, along with tips on hardware requirements and how to perform various installs.

. Read Help or Release Notes before installing Fedora.



Welcome to Fedora Core

Welcome! Throughout this installation you will be able to use your mouse to choose different options. You can also navigate the installation using the **Tab** and **Enter** keys.

Use the **Next** and **Back** buttons to progress through these screens. Click **Next** to save the information and proceed to the next screen; click **Back** to move to the previous screen.

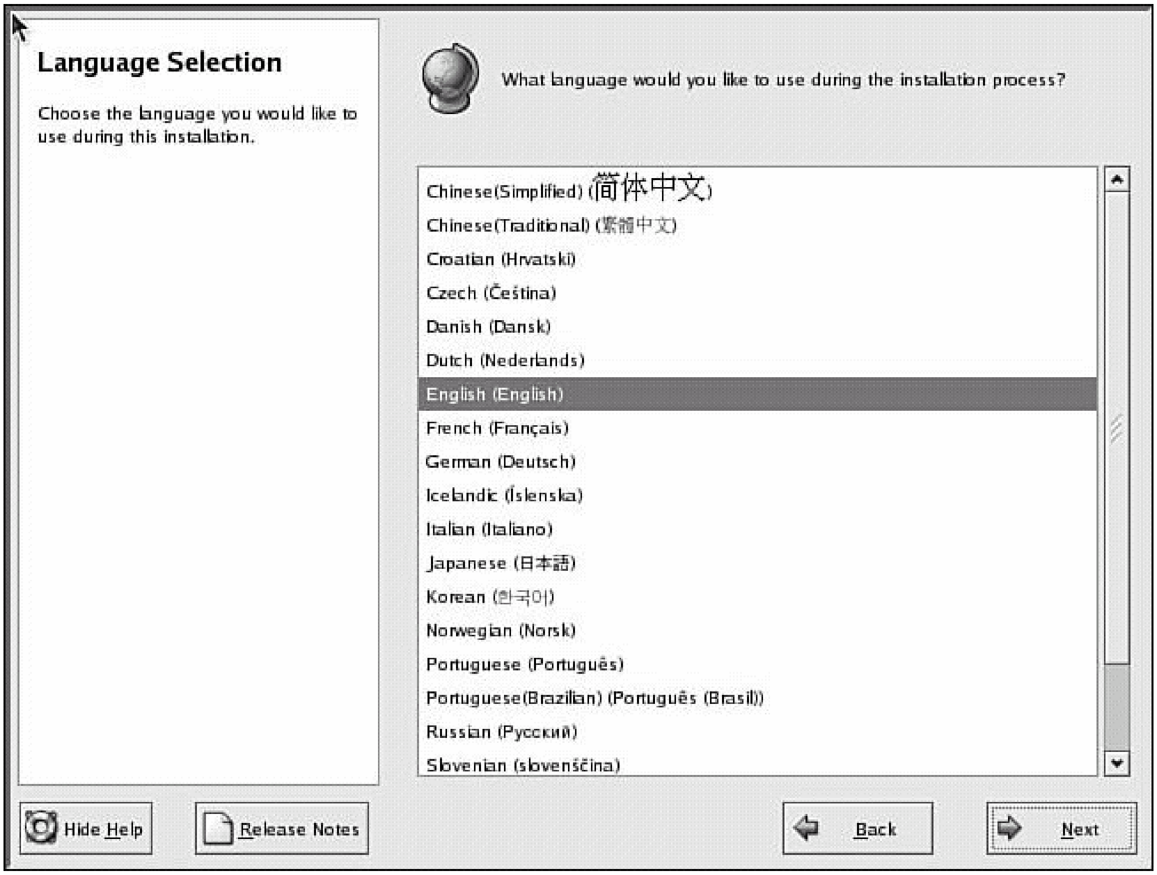
To minimize this help screen, click on the **Hide Help** button.

The release notes provide an

If your pointing device (mouse) is not recognized, you can press Alt+R to "press" the Release Notes button. Similarly, you can click Alt+H to hide text shown on the left side of the screen, but you should take a minute to read frame's contents.

Click Next (or press Alt+N) to continue, and the installer asks you to select one of 31 different languages for the installation

Select a language to use when installing Fedora.



Language Selection

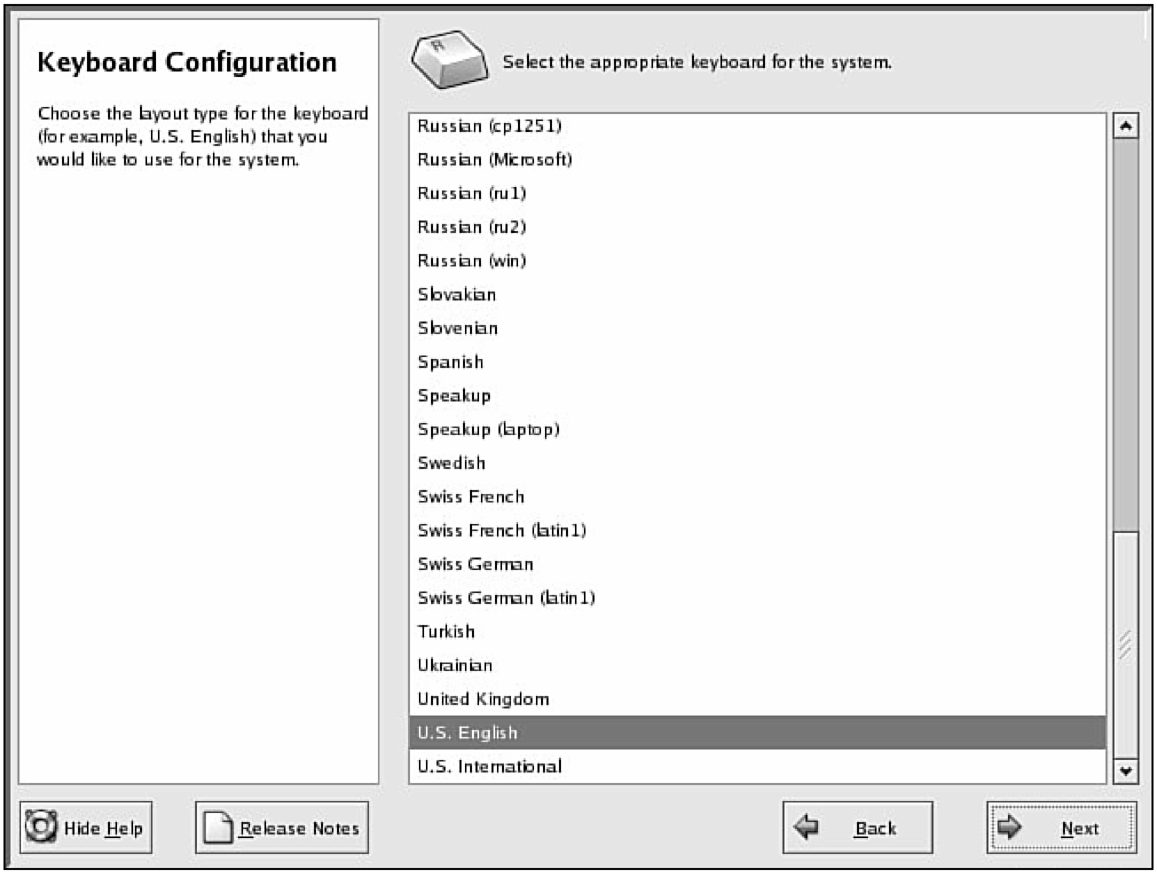
Choose the language you would like to use during this installation.

What language would you like to use during the installation process?

Chinese(Simplified) (简体中文)
Chinese(Traditional) (繁體中文)
Croatian (Hrvatski)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
English (English)
French (Français)
German (Deutsch)
Icelandic (Íslenska)
Italian (Italiano)
Japanese (日本語)
Korean (한국어)
Norwegian (Norsk)
Portuguese (Português)
Portuguese(Brazilian) (Português (Brasil))
Russian (Русский)
Slovenian (slovenščina)

You can navigate the installer's dialogs (during a text-based or graphical install) using the Tab key. You can scroll through lists using your cursor keys. Note that you can now "step backward" through the install by using a Back button. Select a language and click the Next button.

Select a default keyboard to use when installing and using Fedora



Keyboard Configuration

Choose the layout type for the keyboard (for example, U.S. English) that you would like to use for the system.

Select the appropriate keyboard for the system.

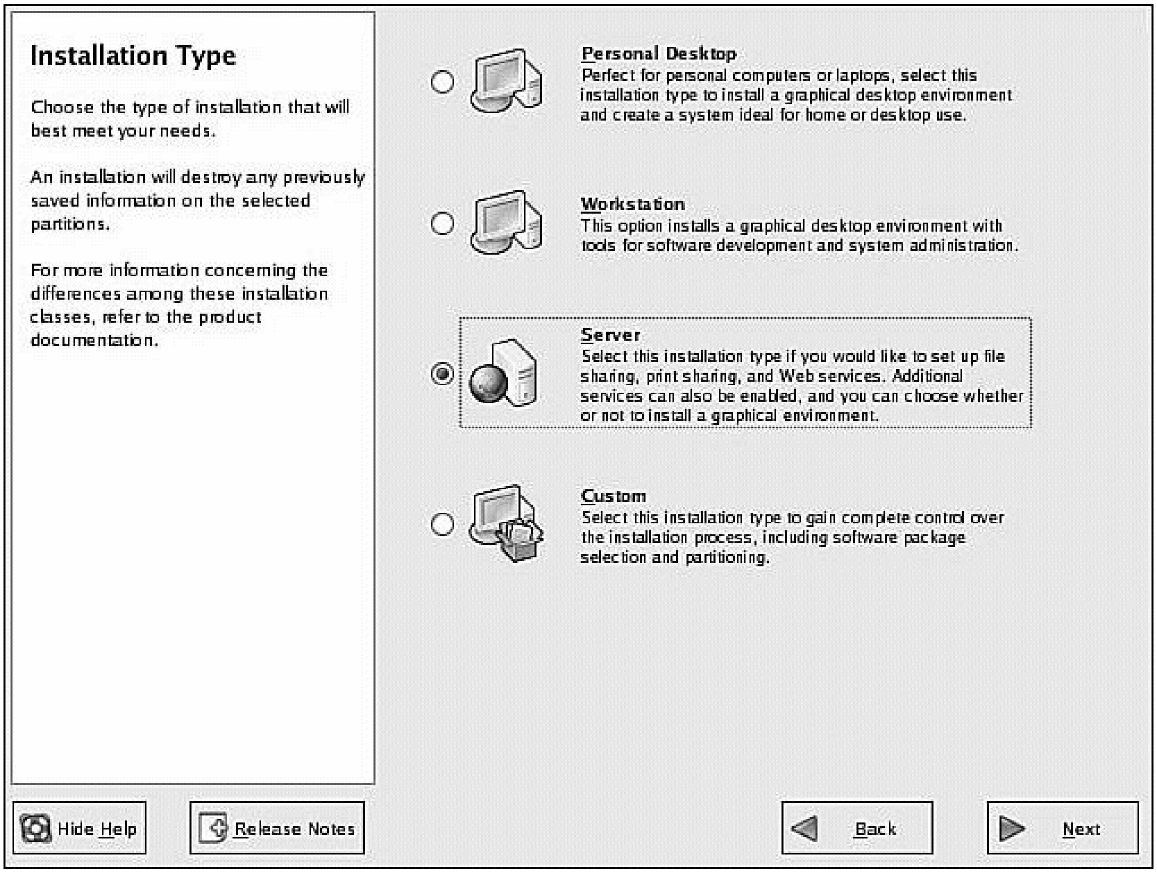
Russian (cp1251)
Russian (Microsoft)
Russian (ru1)
Russian (ru2)
Russian (win)
Slovakian
Slovenian
Spanish
Speakup
Speakup (laptop)
Swedish
Swiss French
Swiss French (latin1)
Swiss German
Swiss German (latin1)
Turkish
Ukrainian
United Kingdom
U.S. English
U.S. International

Scroll to the appropriate keyboard option. You use this option to configure the install to support one of 53 different language keyboards. Click Next after making your selection.

If your PC's monitor was not detected, you might be asked to select your model from 132 different manufacturers. In rare instances, you might have to specify your monitor's exact horizontal and vertical frequencies. This can happen with older displays.

If an existing Linux install is detected, you'll be asked if you want to upgrade and reinstall; otherwise, you're then asked to select a type of installation,.

Select a type of installation



Installation Type

Choose the type of installation that will best meet your needs.

An installation will destroy any previously saved information on the selected partitions.

For more information concerning the differences among these installation classes, refer to the product documentation.

○ **Personal Desktop**
Perfect for personal computers or laptops, select this installation type to install a graphical desktop environment and create a system ideal for home or desktop use.

○ **Workstation**
This option installs a graphical desktop environment with tools for software development and system administration.

● **Server**
Select this installation type if you would like to set up file sharing, print sharing, and Web services. Additional services can also be enabled, and you can choose whether or not to install a graphical environment.

○ **Custom**
Select this installation type to gain complete control over the installation process, including software package selection and partitioning.

Select a type of installation suitable for your intended use—we'll use a Server install for our example. As we mentioned earlier, you can use the Custom install instead to select the specific packages to be installed. This can be helpful in order to prune unnecessary software from your system and might save some time later on. After you select the installation type, click Next to continue. You will then see a screen that offers a choice of partitioning schemes and tools.

NOTE

Fedora's installer also supports the ability to monitor background and install processes running during an installation. You can watch the progress of an install and hardware information reported by the Linux install kernel by navigating to a different console display or virtual console by simultaneously pressing the Ctrl, Alt, and appropriate Fn key (such as F1–F5).

Use this approach to watch for kernel messages, monitor hardware detection, gain access to a single-user shell, and view the progress of the installer script.

When using a graphical installer, press Ctrl+Alt+F4 (then Alt+F2 or Alt+F3) to navigate to the various screens. Press Alt+F7 to jump back to the installer. When performing a text-based installation, use Alt+F2 (then Alt+F3 or Alt+F4). Use Alt+F1 to jump back to a text-based install.

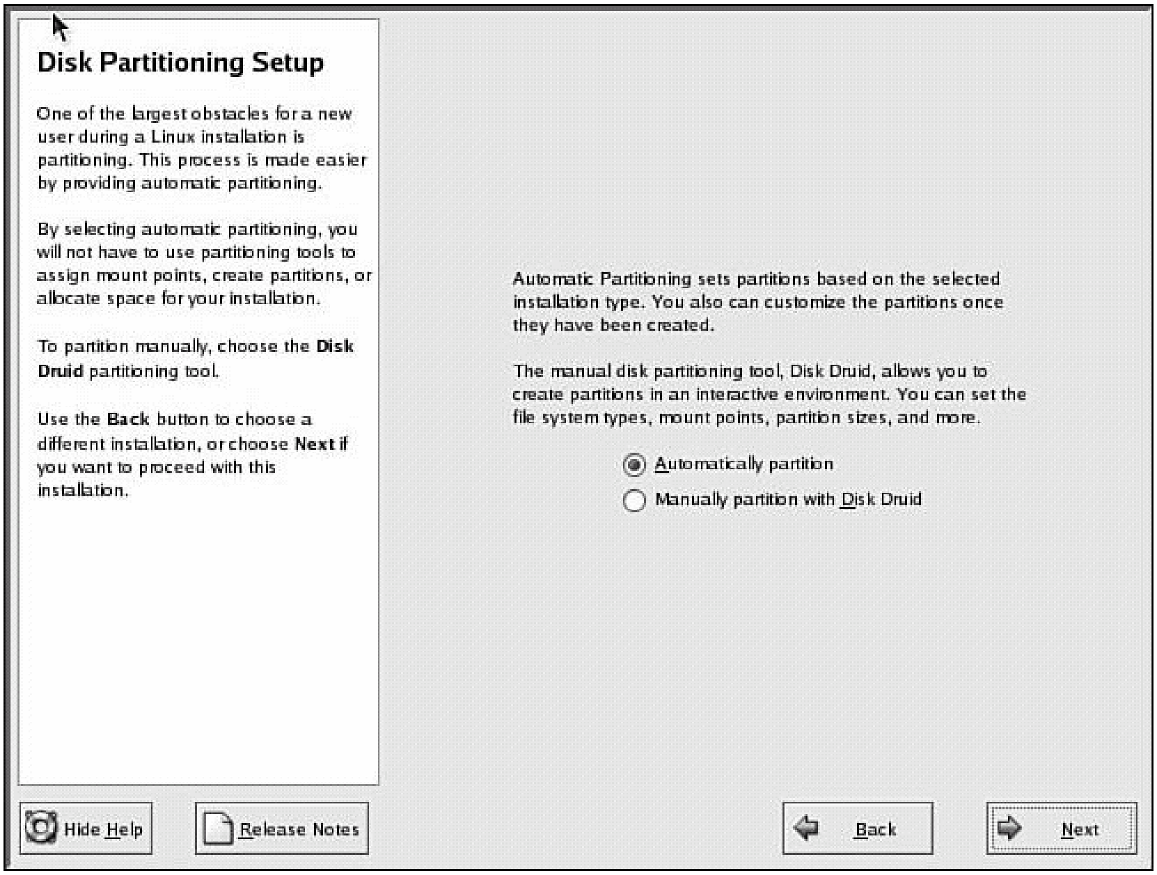
Partitioning Your Drive

You learned how to choose and plan a partitioning scheme in "Planning Partition Strategies,". The Disk Partitioning Setup screen, , offers two options for disk partitioning. Here is what the options do:

Using the Automatically Partition button conveniently partitions your hard drive according to the type of installation you selected and configures the partitions for use with Linux.

Choosing the Manually Partition with Disk Druid button launches a graphical partition editor that enables the creation of custom partition schemes.

Select a partitioning scheme or tool.



Disk Partitioning Setup

One of the largest obstacles for a new user during a Linux installation is partitioning. This process is made easier by providing automatic partitioning.

By selecting automatic partitioning, you will not have to use partitioning tools to assign mount points, create partitions, or allocate space for your installation.

To partition manually, choose the **Disk Druid** partitioning tool.

Use the **Back** button to choose a different installation, or choose **Next** if you want to proceed with this installation.

Automatic Partitioning sets partitions based on the selected installation type. You also can customize the partitions once they have been created.

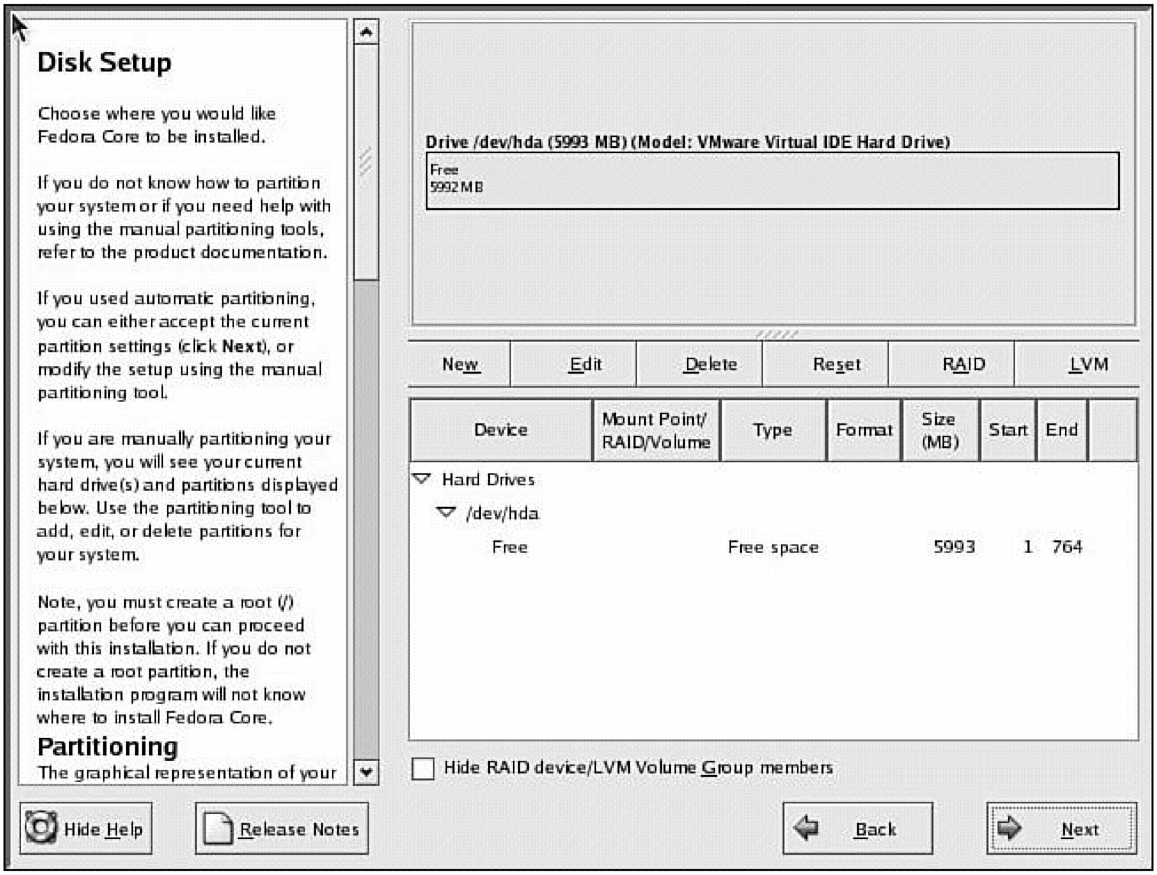
The manual disk partitioning tool, Disk Druid, allows you to create partitions in an interactive environment. You can set the file system types, mount points, partition sizes, and more.

● Automatically partition

○ Manually partition with Disk Druid

For this example, select Manually Partition with Disk Druid button and click Next. If you are using a new hard drive that hasn't previously been partitioned, you will be asked if you would like to create new partitions on the drive. Click the Yes button to initialize the drive. If you are using a hard drive that has been previously partitioned or formatted and the partitions are recognized, Disk Druid will present the partitions in its partition dialog. shows the graphical interface presented for a 6GB hard drive that hasn't been partitioned.

You can use Disk Druid to partition your drive before installing Fedora



Disk Setup

Choose where you would like Fedora Core to be installed.

If you do not know how to partition your system or if you need help with using the manual partitioning tools, refer to the product documentation.

If you used automatic partitioning, you can either accept the current partition settings (click **Next**), or modify the setup using the manual partitioning tool.

If you are manually partitioning your system, you will see your current hard drive(s) and partitions displayed below. Use the partitioning tool to add, edit, or delete partitions for your system.

Note, you must create a root (/) partition before you can proceed with this installation. If you do not create a root partition, the installation program will not know where to install Fedora Core.

Partitioning

The graphical representation of your

Drive /dev/hda (5993 MB) (Model: VMware Virtual IDE Hard Drive)

Free
5992 MB

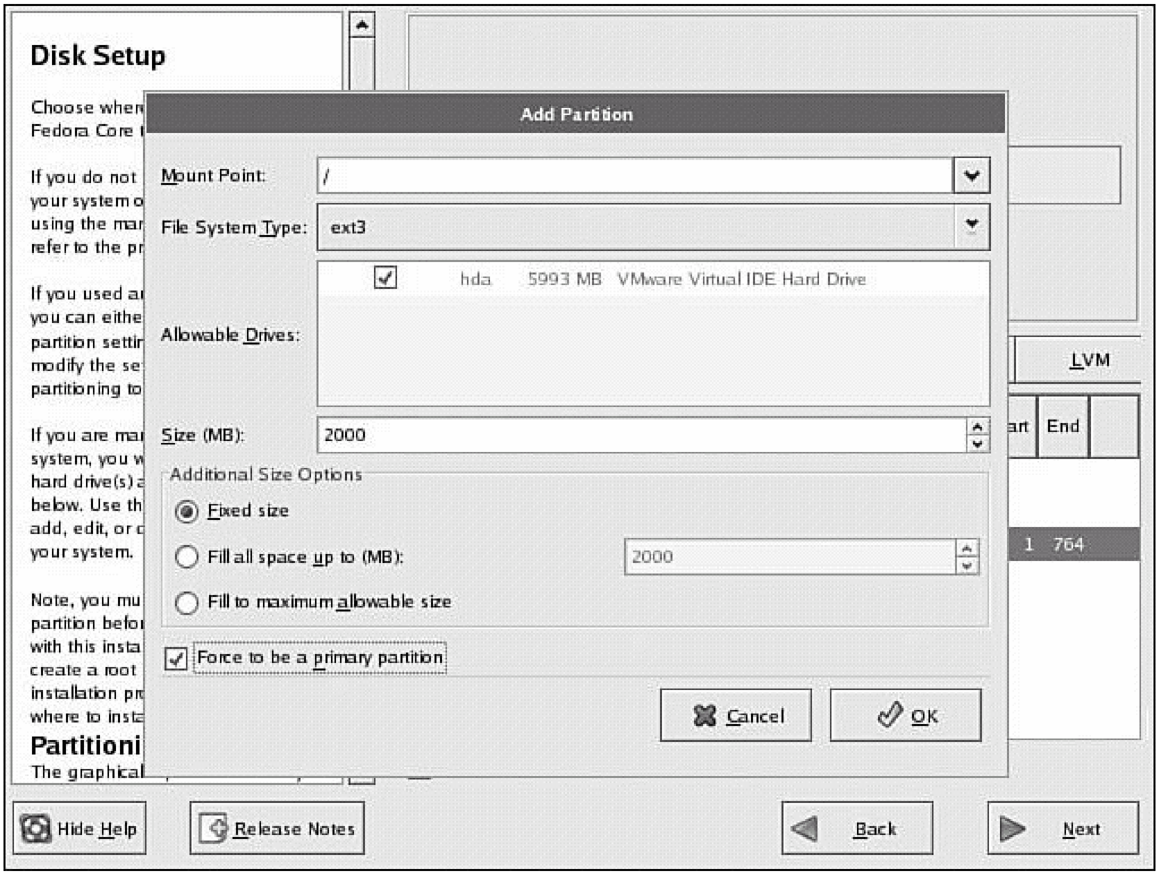
Device	Mount Point/ RAID/Volume	Type	Format	Size (MB)	Start	End
▽ Hard Drives						
▽ /dev/hda						
Free		Free space		5993	1	764

☐ Hide RAID device/LVM Volume Group members

To use Disk Druid, select any listed free space, and then click the New button (or press Alt+W) to create a new partition. Alternatively,

- To get help, see the help frame on the left.
- To create free space, scroll to an existing partition and use the Delete button to delete the partition.

Set partition information about a selected or new partition on a hard drive



Add Partition

Mount Point: /

File System Type: ext3

Allowable Drives: ☑ hda 5993 MB VMware Virtual IDE Hard Drive

Size (MB): 2000

Additional Size Options

● Fixed size

○ Fill all space up to (MB): 2000

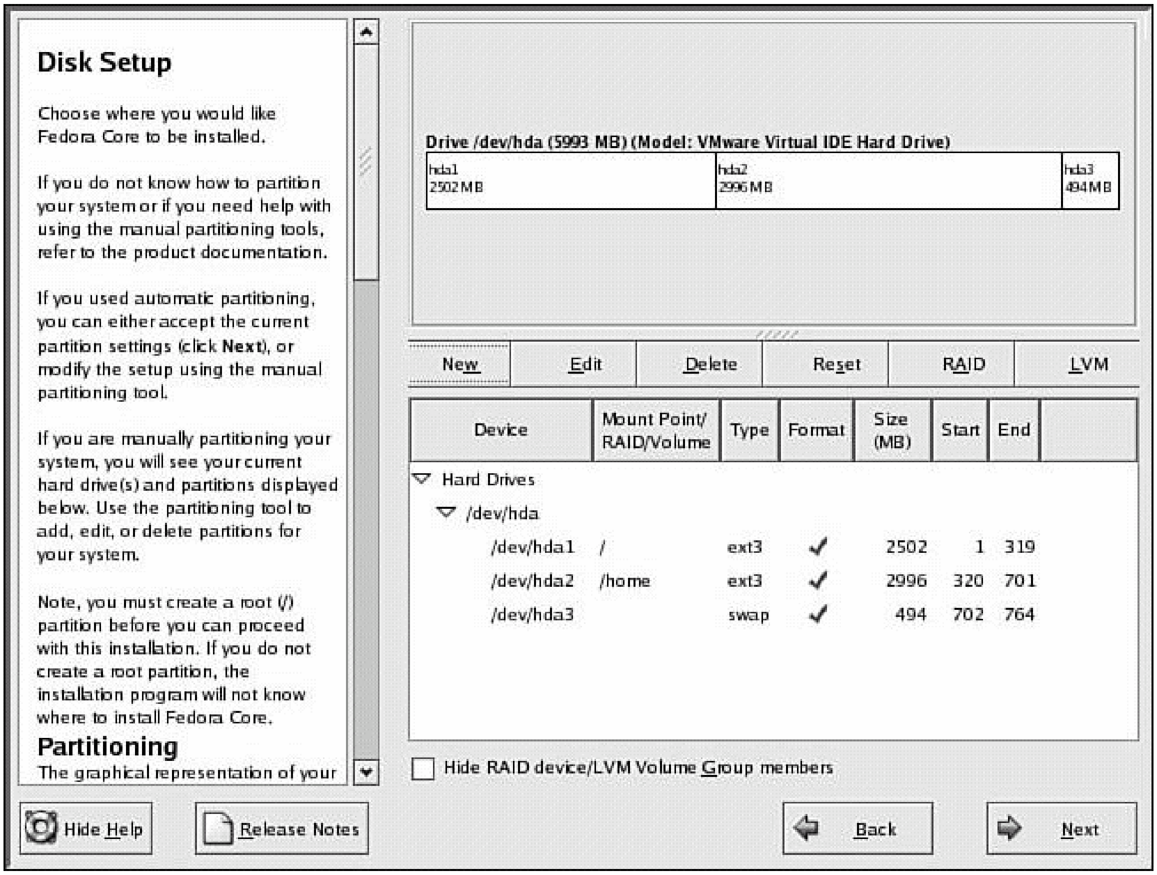
○ Fill to maximum allowable size

☑ Force to be a primary partition

You use the Add Partition dialog to assign a mount point (such as /boot or /), assign a filesystem (such as ext2, ext3, RAID, swap, or vfat) by using the drop-down menu set at ext3 by default, and assign the size of the partition. Remember that, at a minimum, your system should have a root (/) and swap partition. The ext3 filesystem is the best choice for your Linux partitions because it is the default and specifically supported by Fedora, but you can also use ext2 (and convert to ext3 later on—see Chapter 37, "Managing the File System"). The size of the partition can be fixed by entering a number (in megabytes), or if you select the Fill All Available Space field, will use all remaining free space (but not yet, as you need to create a partition for swap). Click OK to save the new partition information.

Remember: Linux requires at least a root (/) and swap partition. The swap partition should be about twice as large as the amount of installed memory (or more) in order to get the most from your computer if you run a lot of programs or host many users. After you create an initial partition for the root filesystem, repeat the steps to create a new partition, but select swap as the filesystem type using the drop-down menu..

Review your partitioning scheme for your hard drive



Disk Setup

Choose where you would like Fedora Core to be installed.

If you do not know how to partition your system or if you need help with using the manual partitioning tools, refer to the product documentation.

If you used automatic partitioning, you can either accept the current partition settings (click **Next**), or modify the setup using the manual partitioning tool.

If you are manually partitioning your system, you will see your current hard drive(s) and partitions displayed below. Use the partitioning tool to add, edit, or delete partitions for your system.

Note, you must create a root (/) partition before you can proceed with this installation. If you do not create a root partition, the installation program will not know where to install Fedora Core.

Partitioning

The graphical representation of your

Drive /dev/hda (5993 MB) (Model: VMware Virtual IDE Hard Drive)

hda1 2502 MB	hda2 2996 MB	hda3 494 MB

Device	Mount Point/ RAID/Volume	Type	Format	Size (MB)	Start	End
▽ Hard Drives						
▽ /dev/hda						
/dev/hda1	/	ext3	✓	2502	1	319
/dev/hda2	/home	ext3	✓	2996	320	701
/dev/hda3		swap	✓	494	702	764

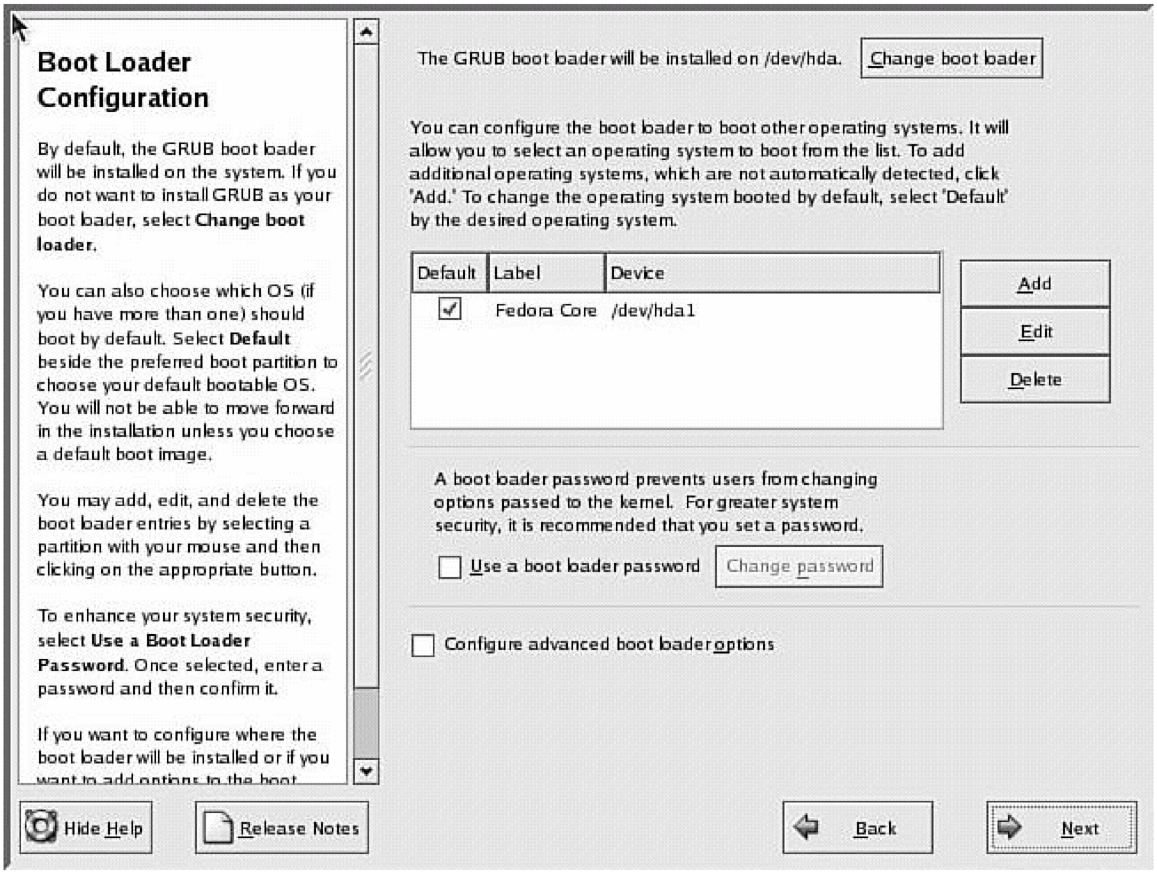
□ Hide RAID device/LVM Volume Group members

Take a moment to review your partitioning scheme. If you are not satisfied with the partitioning, you can make changes by selecting a partition and then using the Edit button to change the partition's information (such as mount point or type of filesystem). Use the Delete button to delete the partition entry and to free up partition space. You can then use the New button again to create partitions in the space that is now free. When satisfied, click Next to continue the install.

Choosing, Configuring, and Installing the Boot Loader

After you accept the partitioning scheme, a screen appears asking you to select a boot loader for booting Fedora This screen also enables you to choose not to use a boot loader (when booting from floppy, a commercial boot utility, a DOS partition, or over a network), and the ability to boot other operating systems if you have configured a dual-boot system. Review "Choosing a Boot Loader," shown previously in this chapter, for more information on making this choice.

Figure 3.11. Select whether you want to use a boot loader and configure other boot options.



Boot Loader Configuration

By default, the GRUB boot loader will be installed on the system. If you do not want to install GRUB as your boot loader, select **Change boot loader**.

You can also choose which OS (if you have more than one) should boot by default. Select **Default** beside the preferred boot partition to choose your default bootable OS. You will not be able to move forward in the installation unless you choose a default boot image.

You may add, edit, and delete the boot loader entries by selecting a partition with your mouse and then clicking on the appropriate button.

To enhance your system security, select **Use a Boot Loader Password**. Once selected, enter a password and then confirm it.

If you want to configure where the boot loader will be installed or if you want to add options to the boot

The GRUB boot loader will be installed on /dev/hda.

You can configure the boot loader to boot other operating systems. It will allow you to select an operating system to boot from the list. To add additional operating systems, which are not automatically detected, click 'Add.' To change the operating system booted by default, select 'Default' by the desired operating system.

Default	Label	Device
☑	Fedora Core	/dev/hda1

A boot loader password prevents users from changing options passed to the kernel. For greater system security, it is recommended that you set a password.

□ Use a boot loader password

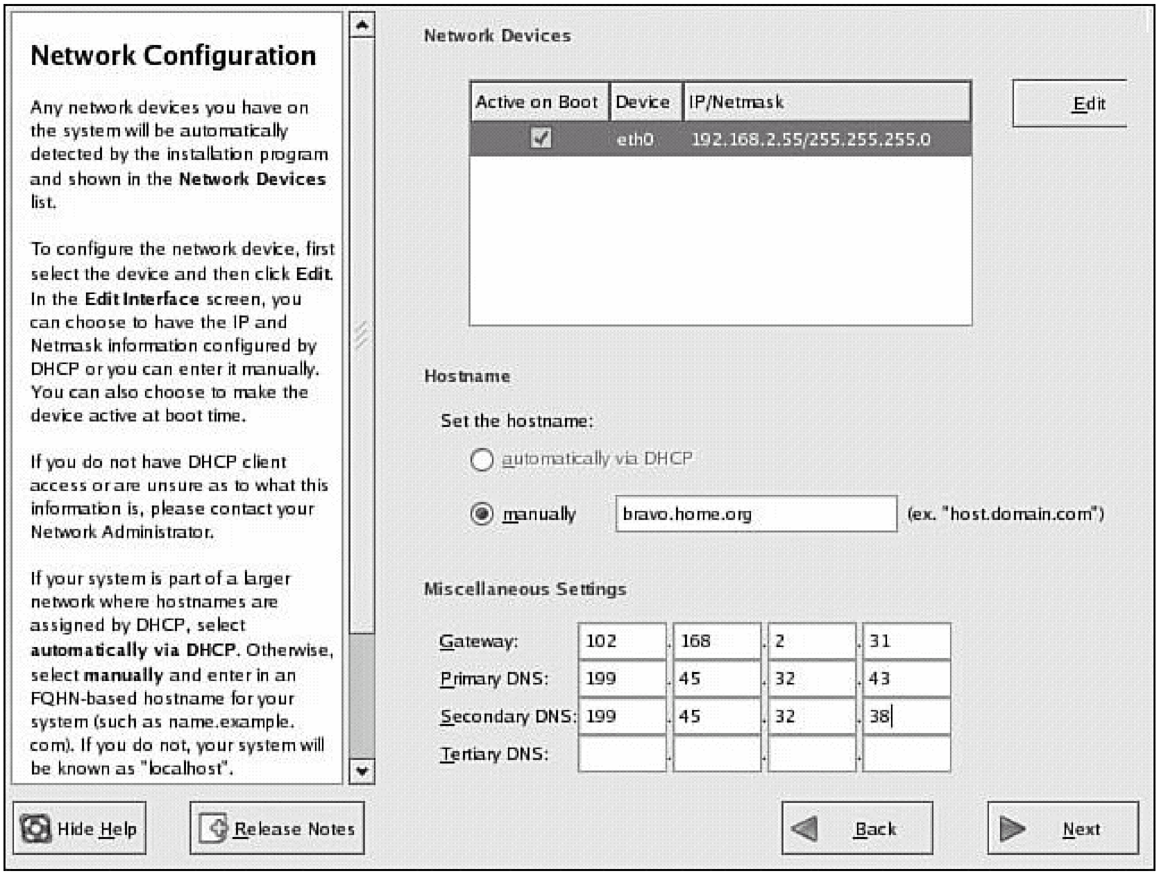
□ Configure advanced boot loader options

Select the GRUB boot loader. GRUB is typically installed in the MBR of the first IDE hard drive in a PC. However, the boot loader can also be installed in the first sector of the Linux boot partition, or even not installed on the hard drive. In this situation, you will need to create a boot floppy during the install. Note that you can also backtrack through the install process to change any settings.

Note that you can assign a password for the boot loader. If you choose to use this option, you will need to enter a password at the GRUB boot screen (see the section "Login and Shutdown" at the end of this chapter for information on graphical logins). Carefully note the password! It does not have to be the same password used to log in, but if you password protect booting through your computer's BIOS and use a boot loader password here, you will subsequently need to enter three passwords (BIOS, boot loader, and login) in order to access Linux. Type in a password of at least eight characters twice (once on each line); then click OK or Cancel to exit the dialog.

If you click the Configure Advanced Boot Loader Options button, you're asked for arguments to pass to the Linux kernel before booting. Kernel arguments are used to enable or disable various features of Linux at boot time. If you install the source to the Linux kernel, you'll find documentation about the more than 200 different kernel arguments in the file kernel-parameters.txt under the /usr/src/linux/Documentation directory.Click Next to set your boot loader configuration.

. **Select or enter networking configuration information**



Network Configuration

Any network devices you have on the system will be automatically detected by the installation program and shown in the **Network Devices** list.

To configure the network device, first select the device and then click **Edit**. In the **Edit Interface** screen, you can choose to have the IP and Netmask information configured by DHCP or you can enter it manually. You can also choose to make the device active at boot time.

If you do not have DHCP client access or are unsure as to what this information is, please contact your Network Administrator.

If your system is part of a larger network where hostnames are assigned by DHCP, select **automatically via DHCP**. Otherwise, select **manually** and enter in an FQHN-based hostname for your system (such as name.example.com). If you do not, your system will be known as "localhost".

Network Devices

Active on Boot	Device	IP/Netmask
☑	eth0	192.168.2.55/255.255.255.0

Hostname

Set the hostname:

○ automatically via DHCP

● manually bravo.home.org (ex. "host.domain.com")

Miscellaneous Settings

Gateway:	102	168	2	31
Primary DNS:	199	45	32	43
Secondary DNS:	199	45	32	38
Tertiary DNS:				

NETWORK CONFIGURATION

If you have an installed network adapter, you are asked for network configuration details,. Fedora can be set to automatically configure networking upon booting. Note that you can also configure networking following installation using Fedora's system-config-network graphical network administration tool .

NOTE

If the Linux kernel finds more than one network interface installed on your computer, you might be asked to configure a second Ethernet device. This might be the case, for example, if you are installing Fedora on a computer that will serve as a gateway or firewall. If you configure more than one Ethernet device, the device named eth0 will be the first active interface when you start Fedora.

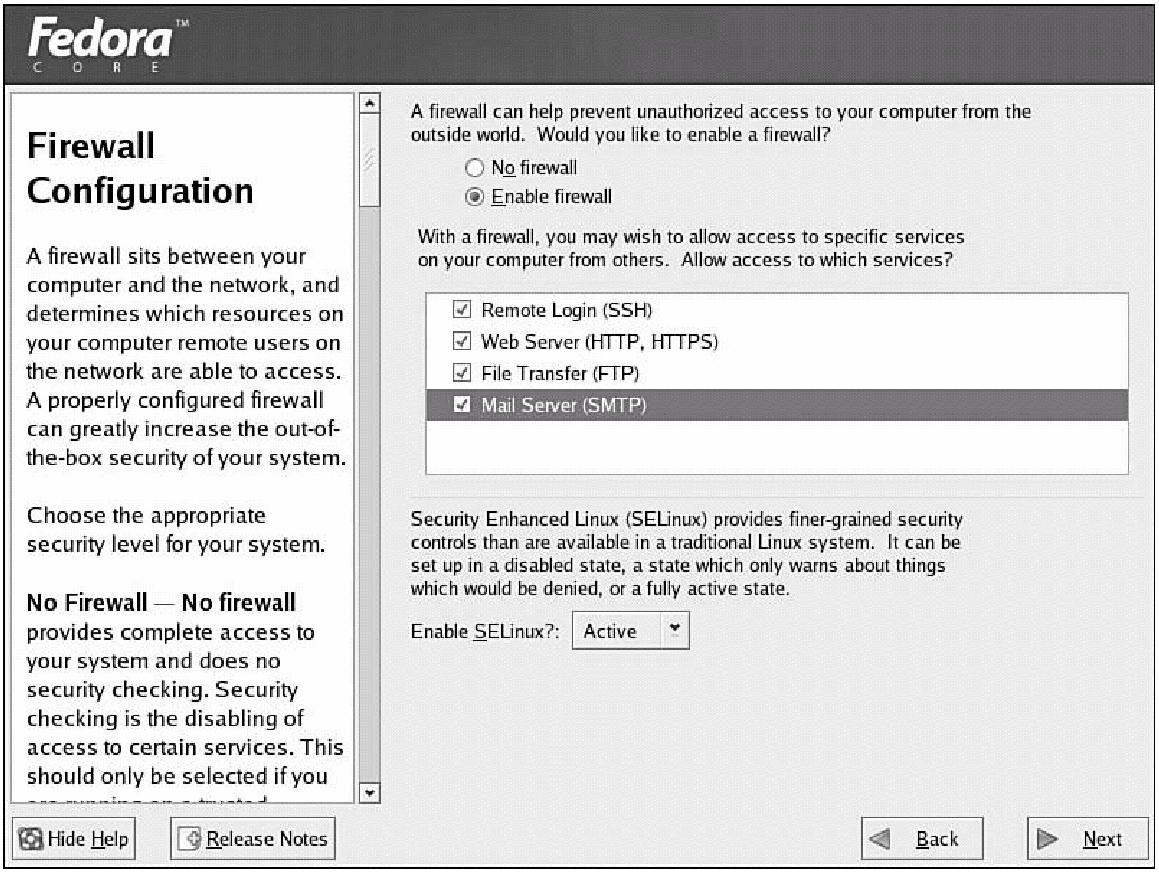
You can choose to have your interface information automatically set using DHCP. Otherwise, especially if you are configuring a DHCP server, manually enter an IP address, hostname, or gateway address (such as for a router), along with DNS information if you click the Edit button listed by the interface (such as eth0 in the example).

After making your selection, click Next to continue. You'll be asked to select a firewall configuration.

FIREWALL AND SECURITY CONFIGURATION

Figure shows the Fedora installer Firewall Configuration dialog, which offers an opportunity to set default security policies for the new server. Protecting your system using a firewall is especially important if your server is connected to a network (although it is best to first install Linux, set security policies, and then connect to a network). These settings in this installation screen determine how remote computers or users will be able to access your server. You can change these policies after finishing the install and logging in. Also on this screen is the option to either enable or disable SELinux, the more secure version of Fedora. If you have not come across SELinux before, you should consider setting it to either warn or disable because it will enable you to learn how SELinux could potentially impact your installation.

Select a desired security level and allowed services



Firewall Configuration

A firewall sits between your computer and the network, and determines which resources on your computer remote users on the network are able to access. A properly configured firewall can greatly increase the out-of-the-box security of your system.

Choose the appropriate security level for your system.

No Firewall — No firewall provides complete access to your system and does no security checking. Security checking is the disabling of access to certain services. This should only be selected if you

A firewall can help prevent unauthorized access to your computer from the outside world. Would you like to enable a firewall?

○ No firewall
● Enable firewall

With a firewall, you may wish to allow access to specific services on your computer from others. Allow access to which services?

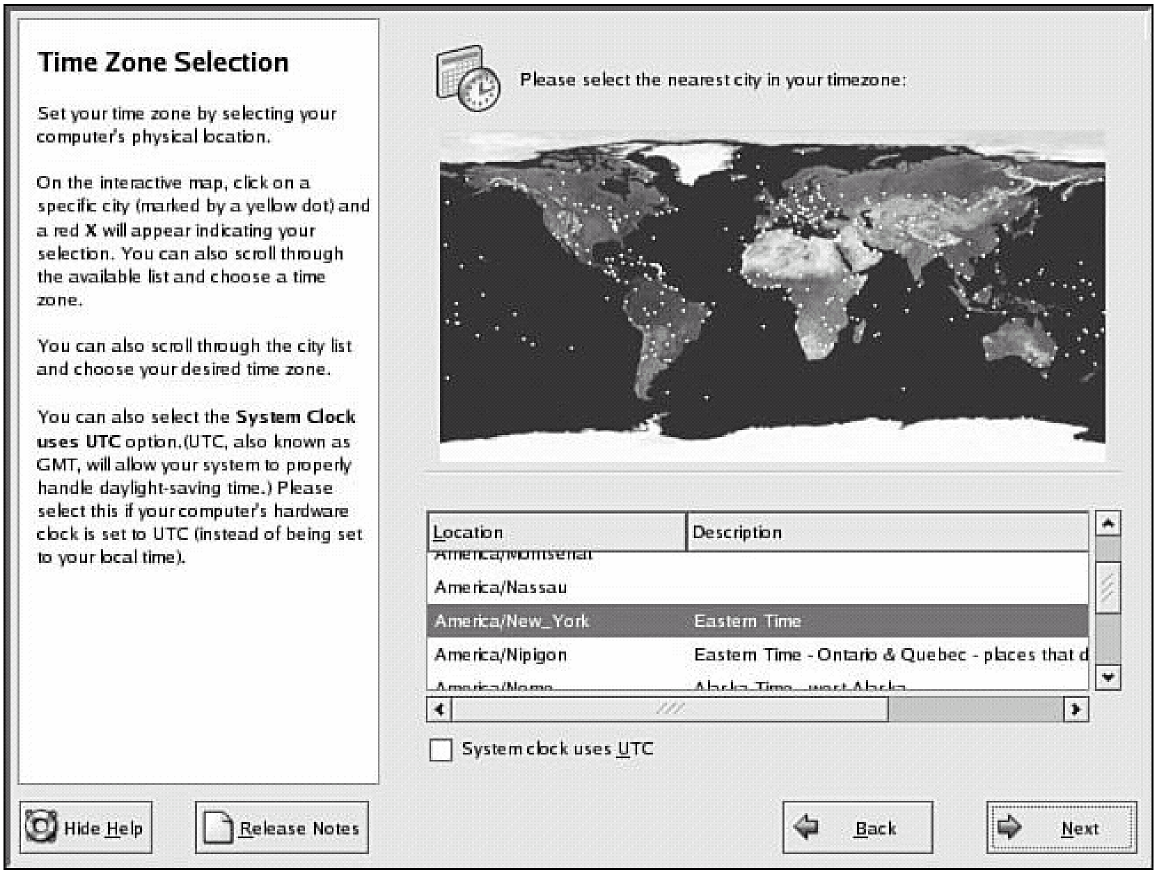
☑ Remote Login (SSH)
☑ Web Server (HTTP, HTTPS)
☑ File Transfer (FTP)
☑ Mail Server (SMTP)

Security Enhanced Linux (SELinux) provides finer-grained security controls than are available in a traditional Linux system. It can be set up in a disabled state, a state which only warns about things which would be denied, or a fully active state.

Enable SELinux?: Active

If you have a general idea of how you want to protect your computer, use the dialog shown in Figure to turn on firewalling.

Select your time zone



Time Zone Selection

Set your time zone by selecting your computer's physical location.

On the interactive map, click on a specific city (marked by a yellow dot) and a red **X** will appear indicating your selection. You can also scroll through the available list and choose a time zone.

You can also scroll through the city list and choose your desired time zone.

You can also select the **System Clock uses UTC** option.(UTC, also known as GMT, will allow your system to properly handle daylight-saving time.) Please select this if your computer's hardware clock is set to UTC (instead of being set to your local time).

Please select the nearest city in your timezone:

Location	Description
America/Montserrat	
America/Nassau	
America/New_York	Eastern Time
America/Nipigon	Eastern Time - Ontario & Quebec - places that d
America/Nome	Alaska Time - west Alaska

□ System clock uses UTC

Choosing the No Firewall setting is not recommended; use this setting only if Fedora will be used as a non-networked workstation.

NOTE

Note that you can also manually configure security settings after installation using the text-based lokkit command, system-config-securitylevel client, or graphical gnome-lokkit client. "Securing Your Machines," for details on how to protect your system using these clients and various security level settings.

Click any allowable services, as shown in Figure 3.14. For some servers, HTTP, FTP, and Simple Mail Transport Protocol (SMTP) requests are acceptable and reasonable. Do not select or use the Telnet service, which is used to allow remote network logins. For security reasons, the Secure SHell (SSH) service is a much better choice "First Steps with Fedora," on how to use the ssh client).

Click Next to install the firewall security settings. You will then be asked to select additional language support on your server. Again click Next when finished.

SETTING THE TIME ZONE

You are next shown a Time Zone Selection dialog There are two "clocks," or times, when using a PC: the hardware clock, maintained by hardware in the computer and a backup battery; and the system time, set upon booting and used by the Linux kernel. It is important to keep the two times accurate and in synchronization because automated system administration might need to take place at critical times. Many computer installations use computers with hardware clocks set to GMT, which stands for Greenwich Mean Time. The more modern designation is UTC or Coordinated Universal Time. The Linux system time is then set relative to this time and the default time zone, such as Eastern Standard Time, which is –5 hours of UTC.

Setting the computer's hardware clock to UTC (GMT) has the advantage of allowing the Linux system time to be easily set relative to the geographic position of the computer and resident time zone (such as a Linux laptop user who would like to create files or send electronic mail with correct time stamps, and who has traveled from New York to Tokyo). "Post-Installation Configuration," for details on setting the date and time for Linux.

TIP

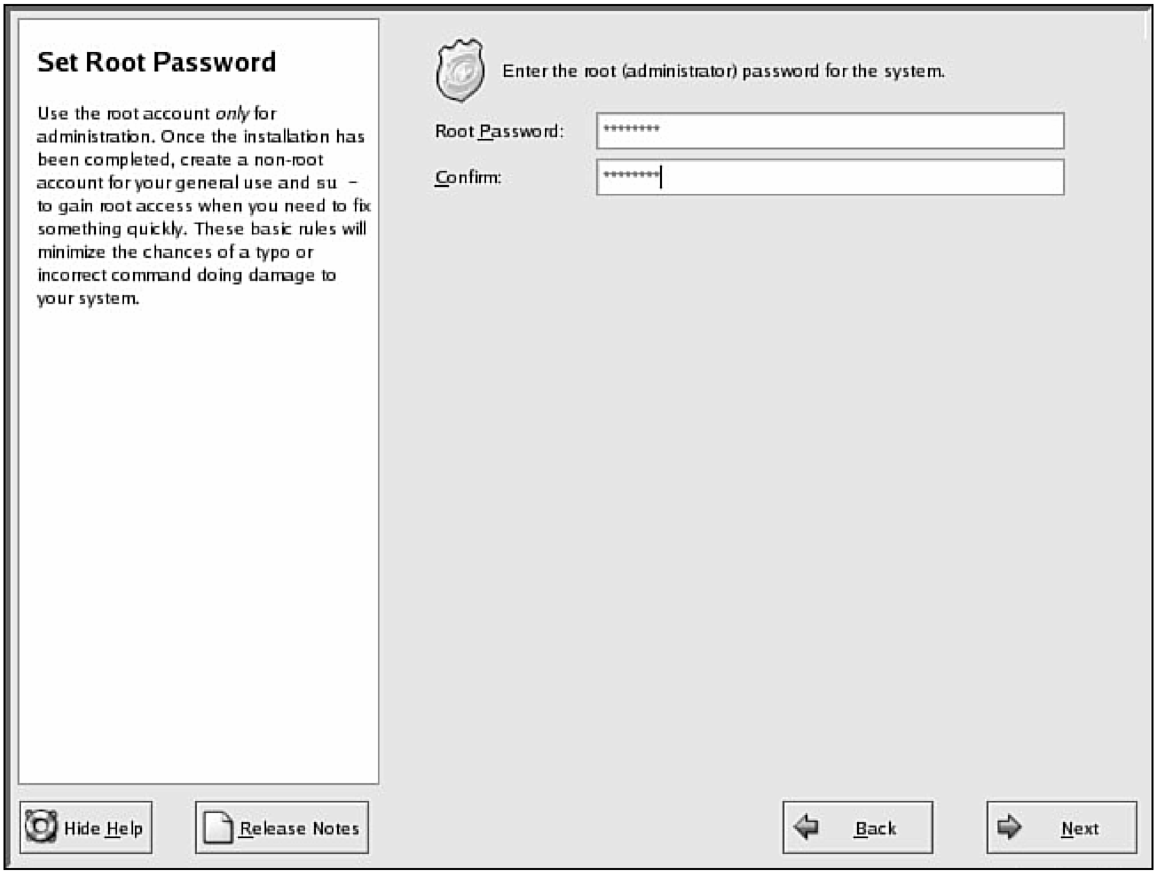
Read the manual page for the hwclock command to learn how to keep a running Linux system synchronized with a PC's hardware clock. for more details on using the hwclock command and Linux time-related software.

Choose your time configuration, and then click Next.

Creating a Root Password and User Accounts

You are next asked to enter a root operator password, as shown in Figure Type in a password, press Tab or Enter, and then type it again to make sure that it is verified. The password, which is case sensitive, should be at least eight characters (or more) and consist of letters and numbers. Note that the password is not echoed back to the display. Your root password is important because you will need it to perform any system administration or user management with Fedora.

Type in, and do not forget, your root password



Set Root Password

Use the root account *only* for administration. Once the installation has been completed, create a non-root account for your general use and su – to gain root access when you need to fix something quickly. These basic rules will minimize the chances of a typo or incorrect command doing damage to your system.

Enter the root (administrator) password for the system.

Root Password: *********

Confirm: *********

.

When finished, click Next to continue on to software package selection for your new server.

NOTE

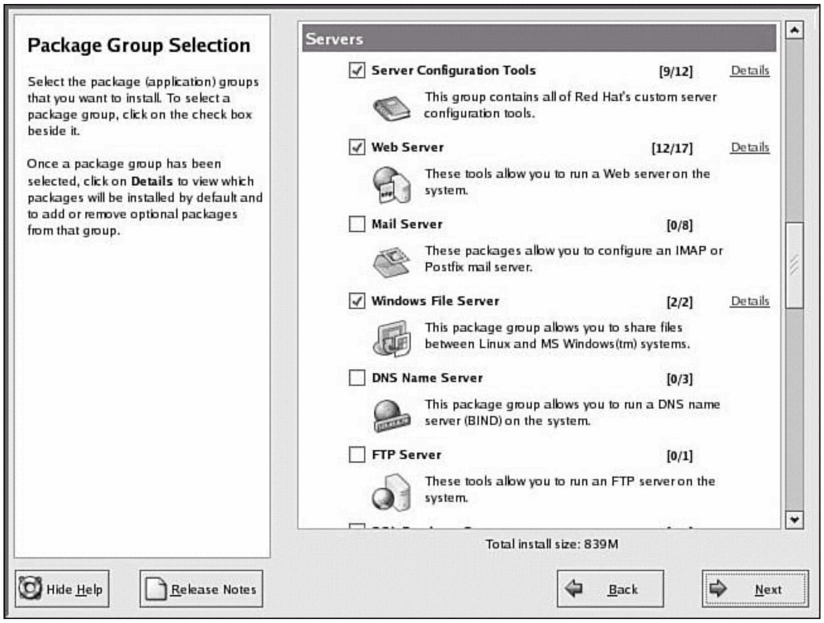
You can only create a root account during a Fedora install. You will have to create user accounts later on after booting, using command-line programs (such as adduser) or the graphical system-config-users client. Create an account for yourself and any additional users. Usernames traditionally consist of the first letter of a person's first name and the last name. For example, Cathy Taulbee would have a username of ctaulbee. Do not forget to enter a password for any new user! If you create a user without a creating a password, the new user will not be able to log in.

You should create at least one user for your server besides the root operator. This is for security purposes and to avoid logging in as root, either through the keyboard at the server or remotely over the network. The default shell and home directory settings should remain set at the defaults, which are the Bourne Again SHell (bash) and the /home directory.

SOFTWARE SELECTION AND INSTALLATION

The Package Group Selection dialog shown in Figure displays the installer's suggested software for your class of installation (a server in our example).

select software package groups for installation.



Package Group Selection

Select the package (application) groups that you want to install. To select a package group, click on the check box beside it.

Once a package group has been selected, click on **Details** to view which packages will be installed by default and to add or remove optional packages from that group.

Servers

☑ **Server Configuration Tools** [9/12] Details
This group contains all of Red Hat's custom server configuration tools.

☑ **Web Server** [12/17] Details
These tools allow you to run a Web server on the system.

□ **Mail Server** [0/8]
These packages allow you to configure an IMAP or Postfix mail server.

☑ **Windows File Server** [2/2] Details
This package group allows you to share files between Linux and MS Windows(tm) systems.

□ **DNS Name Server** [0/3]
This package group allows you to run a DNS name server (BIND) on the system.

□ **FTP Server** [0/1]
These tools allow you to run an FTP server on the system.

Total install size: 839M

If you choose to install a personal desktop, workstation, or other installation type, the software packages appropriate for that installation will be automatically selected for you. Each package (actually a Group) provides many different individual software packages

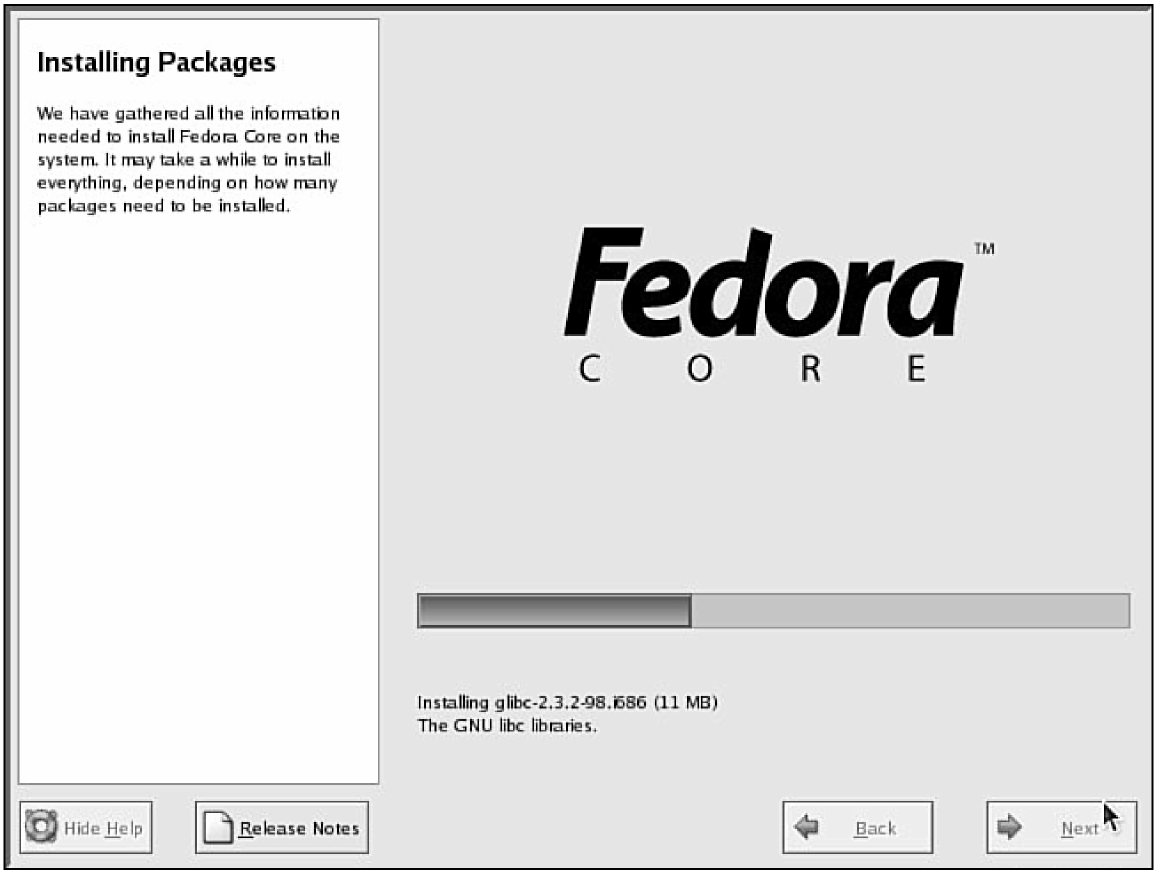
Scroll through the list of package groups, and then click a software package check box to select or deselect software to be installed. Note that the entire size (drive space requirements) of the installed software will be dynamically reflected by your choices.
Click the Next button when finished to start installing Linux and the Fedora Core software.

The installer will then perform a quick dependency check and present a dialog informing you that a log of the install will be saved under the /root directory in the file named install.log. Press the Enter key to begin the installation of the software on your system. Be certain that you are ready when you confirm the process, as you cannot step back from this point on!

The installer will then format and prepare your new Linux partitions.

Next, the installer will prepare for the install by gathering a list of the RPM files and will start placing the software on the newly formatted partitions. This process can take anywhere from several minutes to two or more hours, depending on your PC and the amount of software you have chosen to be installed. The installer reports on the name of the current package being installed and the remaining time, as shown in Figure

The Fedora installer formats your drive, and then installs selected software package groups.



Installing Packages

We have gathered all the information needed to install Fedora Core on the system. It may take a while to install everything, depending on how many packages need to be installed.

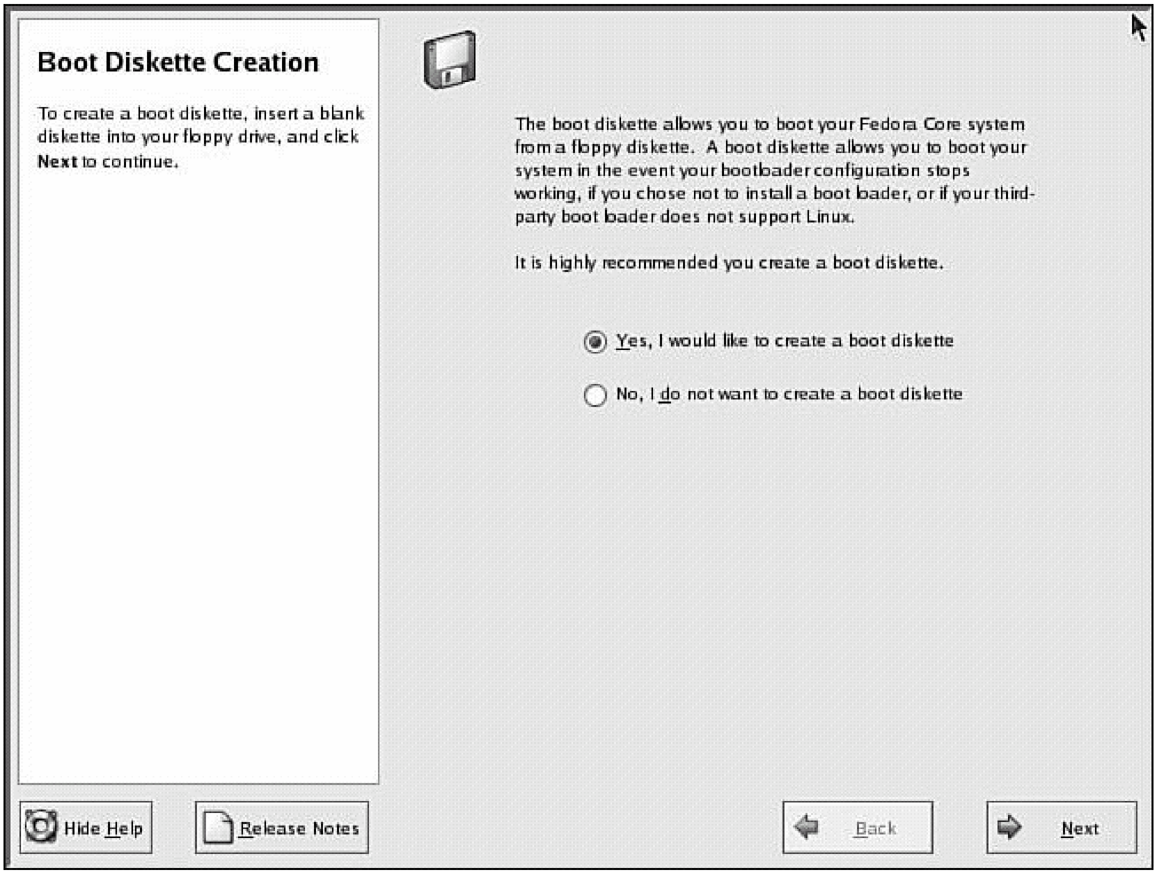
Installing glibc-2.3.2-98.i686 (11 MB)
The GNU libc libraries.

If you are installing over a network, go take a break because the install will proceed unattended through the software installation. If you are using this book's CD-ROMs, you might be prompted to remove the first CD-ROM and insert another. You might also be asked to repeat this operation using the third CD-ROM at some point.

Creating a Boot Disk

When the software installation finishes, the installer will perform some temporary file cleanup, install the boot loader, and then ask if you would like to create a boot disk for possible use later on, as shown in figure

Create a boot disk for use with Fedora



Boot Diskette Creation

To create a boot diskette, insert a blank diskette into your floppy drive, and click **Next** to continue.

The boot diskette allows you to boot your Fedora Core system from a floppy diskette. A boot diskette allows you to boot your system in the event your bootloader configuration stops working, if you chose not to install a boot loader, or if your third-party boot loader does not support Linux.

It is highly recommended you create a boot diskette.

● Yes, I would like to create a boot diskette

○ No, I do not want to create a boot diskette

You can create this boot disk now, or, as mentioned earlier, you can use Fedora's `mkbootdisk` command later on while using Fedora. Select Yes or No. Having a boot disk can be handy, especially if an error was made during the install and the boot loader fails to boot Linux.

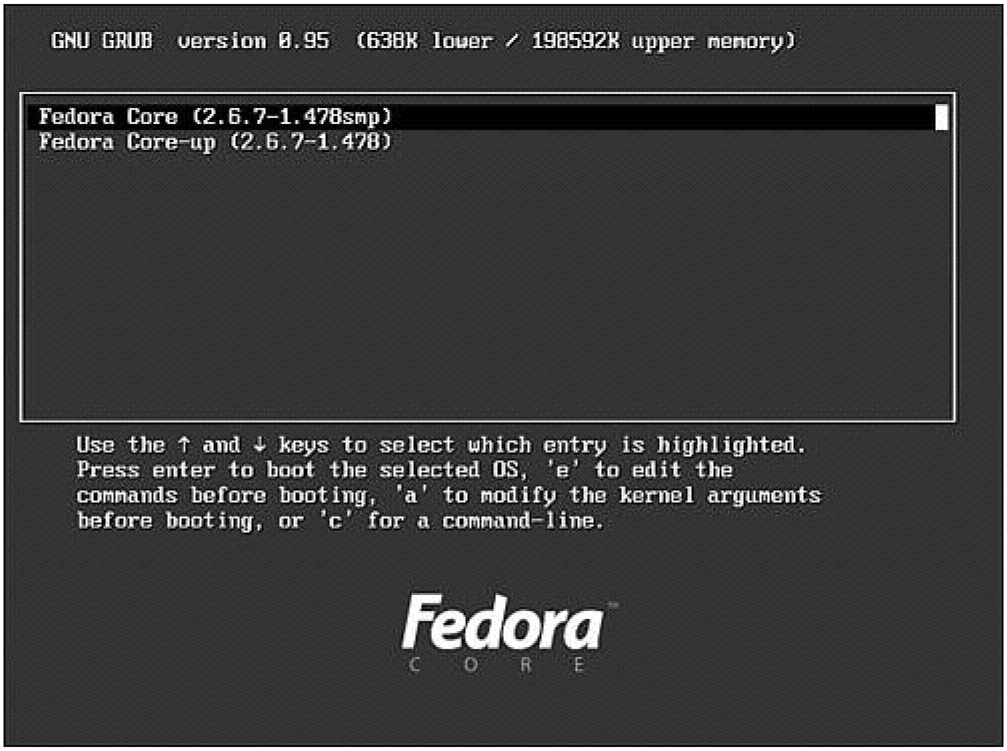
If you choose to create a boot disk, you will need to have a blank disk on hand. Select Yes, insert a blank disk when prompted, create the boot disk, and continue the install.

If you chose the X Window System, you can skip X configuration during the install and configure X after installation. This might be a better approach if the install fails to accurately probe your hardware or cannot configure X during the install, but you still desire to have X software installed.

Finishing the Install

You are done! Press the Exit button, and the installer will eject any inserted CD-ROM and reboot. The GRUB boot loader will present a boot prompt as shown in Figure

Boot Fedora with GRUB by pressing the Enter key or waiting 10 seconds



```
  GNU GRUB  version 0.95  (638K lower / 198592K upper memory)

 Fedora Core (2.6.7-1.478smp)
 Fedora Core-up (2.6.7-1.478)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, 'a' to modify the kernel arguments
    before booting, or 'c' for a command-line.
```

If you have set a GRUB password, press the p key, type your password, and press Enter. If you do nothing for 10 seconds or press Enter, either boot loader will boot Linux.

NOTE

After installation, you can edit the file /boot/grub/grub.conf and change the timeout= setting to change the boot time to a value other than 10 seconds.

Logging In and Shutting Down

After rebooting your PC, you will be able to log in to a Linux session. If you did not choose to use X11 software during the installation, you will log in at a text-based login prompt. If you configured X and enabled a graphical login, the screen will clear after your system boots, and you will be presented with a graphical login screen, as shown previously in Figure.

To log in at the text-based prompt, type your username and press Enter. You will then be prompted for your password. After you press Enter, you will be at the Linux command line. If you use a graphical login, you can use the shutdown or reboot menus in the screen's dialog to shut down or reboot your system. To immediately shut down your system from the command line of a text-based session, use the su command and its -c option to run the halt command, like this:

```
$ su - c halt
```

You can also use the `reboot` command to restart your computer like this:

```
$ su -c reboot
```

For new users, installing Fedora is just the beginning of a new and highly rewarding journey on the path to learning Linux. For Fedora system administrators, the task ahead is to fine-tune the installation and to customize the server or user environment.

3. GETTING STARTED WITH THE DESKTOP

GETTING FAMILIAR WITH THE DESKTOP

Desktop refers to the presentation of windows ,menus, panels, icons, and other graphical elements on user computer screen. Originally, computer systems such as Linux operated purely in text mode – no mouse , no colours, just commands typed on the screen. Desktops provide a more intuitive way of using user computer.

Like most things in linux, the desktop is built from a set of interchangeable building blocks. The building blocks of user desktop , to use a car analogy, are:

- The X window system.
- The KDE or GNOME desktop environment .
- The Metacity window manager
- The bluecurve desktop theme.

Once linux is installed and user has logged in ,user see either the GNOME or KDE desktop .GNOME is the default desktop for Fedora.

TOURING THE DESKTOP

Step1 : *checking out the home folder*

Double click the user's Home icon on the desktop . the window that appears show the filemanager window as it displays the contents of user home folder.the location of home folder is usually /home/user. Where user is replaced by user name.here are something to try out with home folder:

1. folders : create folders and subfolders to store the work.

2. Open location : To open another folder on user's computer , click file then open location and type a directory name .

3. Open with   : Click any object in a folder with the right mouse button ,then select open with. User should able to see several programs user can use to open the object.

4. Side pane : Right click any folder in the Nautilius file manager window, then select Browse Folder to open the new folder with a Side pane displayed. From the drop-down box at the top of the side pane ,choose information to show to show information about the selected folder or file. Next choose History to see files and folders previously viewed.

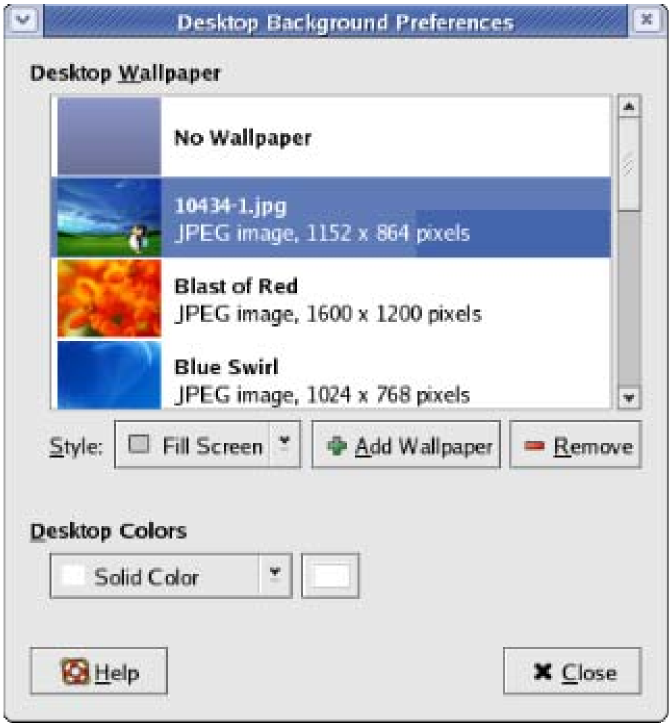
5. Backgrounds : Click Edit then Backgrounds and Emblems . Drag and drop patterns or colors user like into the pane on user's folder window.Click Emblems ,then drag and drop an emblem on a file or folder .

6. Organize the work : As user can create documents, add music, or download images from user camera, organize them into user home folder or any subfolder .

step 2: *Change some preferences***:**

More than 20 preferences categories are available from the GNOME desktop. There are few preference user might want to modify when he start out.

- *Change background* – Select Desktop Background . the Desktop Background preference window appears. Select one of the Desktop wallpaper images.



Desktop Background Preferences

Desktop Wallpaper

No Wallpaper

10434-1.jpg
JPEG image, 1152 x 864 pixels

Blast of Red
JPEG image, 1600 x 1200 pixels

Blue Swirl
JPEG image, 1024 x 768 pixels

Style: Fill Screen

Desktop Colors

Solid Color

- *Add screensaver* - Select screensaver. Try out a few screensavers. Click the only one screen saver check box in the mode box.
- *Change the theme* - Select theme. User can change the entire theme for his desktop.click theme details to mix and match attributes from different themes.

Step 3 : *Configure panels :*

Most people manage their desktop from panels that appear at the top and bottom of the screen. These panels provide an intuitive way to:

- Launch applications
- Change workspaces
- Add useful information (clocks , news tickets , CD players and so on)

Step through the following procedure to learn about the desktop(GNOME) panels:

1. *Application Menu* – Click applications in the top panel . Most useful GUI applications and system tools that come with Fedora and RHEL are available from the Menus and submenus of this Applications menu.
2. *Desktop Menu* – Click Desktop in the top panel . we can change settings or log out or shut down from this menu.
3. *Places Menu* – Click places in the top panel. From the menu that appears, user can open his home folder, his Desktop files, and his computer in a nautlius manager window.
4. *Select desktop applications* – Red Hat places icons for popular desktop applications right on the panel. Click any of the icons shown to launch a web browser,an e-mail reader, a word processor ,a presentation creator, and spreadsheet application, respectively.
5. *Use workspaces* – Click different panels in the workspace Switcher . Open an application ,then click another workspace panel. Workspace is a great way to have multiple windows and still keep user's desktop uncluttered .

USING THE GNOME DESKTOP

GNOME provides the desktop environment that user get by default when he install Fedora or RHEL.This desktop environment provides the software that is between user
X window system framework and look and feel provided by the window manager. GNOME is stable and reliable desktop environment, with a few cool features in it.
To use GNOE desktop user should be familiar with the following components:

- *Metacity (window manager*) – The default window manager for GNOME in Fedora is Metacity .the window manager provides such things as themes, window borders, and window controls.
- *Nautilus (file manager/ graphical shell)* – When user open folder ,the Nautilus window opens and displays the contents of the selected folder. Nautilus can also display other types of content, such as shared folders from windows computers on the network.
- *GNOME panels (application/task launcher*) – These panels , which line the top and bottom of user screen ,are designed to make it convenient for user to launch the applications he use, manage running applications, and work with multiple virtual desktops.
- *Desktop area* – The windows and icons user use are arranged on the desktop area . it supports such things as drag and drop actions between applications , a desktop menu and icons for launching applications.

The following section provide details on using the GNOME desktop.

USING THE METACITY WINDOW MANAGER

The metacity window manager seems to have been chosen as the default window manager for GNOME in RED HAT LINUX because of its simplicity .there isn’t much user can do with metacity except that user work can be done efficiently . Assigning new themes to metacity and changing colors and window decorations is done through the GNOME preferences

USING THE GNOME PANELS

Red Hat places panels on the top and bottom of the GNOME desktop . From those panels user can start applications ,see what programs are active ,check for software updates ,adjust user’s audio volume , and switch workspaces . There are also many ways to change the top or bottom panel – by adding applications or monitors ,or by changing the placement or behavior of the panel.

From the Gnome panel menu ,user can perform a variety of functions ,including:

- *Use the application menu* – displayed on the applications menu are most of the applications and system tools user will use from the desktop.
- *Add to panel* – user can add an applet ,menu,launcher, drawer, or button.
- *Delete this panel* – user can delete the current panel.
- *Properties* – Change position,size, and background of the panel.
- *New panel* – User can add panels to his desktop in different styles ,and locations

CHANGING GNOME PREFERENCES

There are many ways to change the behavior , look, and feel of user’s GNOME desktop. Most GNOME preferences can be modified from windows user can launch from the Desktop menu .

The following items highlight some of the preference user might want to change:

- Accessibility – If user have difficulty operating a mouse or keyboard, the keyboard accessibility preferences window let user adapt mouse and keyboard settings to make those devices more accessible.add figure 110
- Desktop Background – From Desktop background preferences ,user can choose a solid color or an image to use as wallpaper.If user choose to use a solid color ,click the color box, choose fro the palette, and select OK.
- Screen saver – User can choose from dozens of screensavers the screensaver window. User can also choose to require a password or to enable power management to shut down the monitor after a set number of minutes.
- Theme Selector – User can choose to have an entire theme of elements be used on user desktop. A desktop theme affects not only the background, but also the way that many buttons and menu selections appear.

Checking network from GNOME

The GNOME network tools window brings together several tools user would normally run the command line to monitor network resources from a graphical window on user GNOME desktop .To open the network tools window ,select applications then system tools then network tools.Eight tabs on that window let user perform different operations on his network.

The devices tab displays information about each of user's network interfaces. It makes it easy to find the names and address associated with each of user network interfaces as well as information on data transmissions and collisions.on the other tabs user can run graphical versions of : the *ping* **command** ,netset command and traceroute command.

Exiting GNOME

When user complete his work ,user can either log out fro his current session or shut down his computer completely. To exit from GNOME ,do the following:

click Desktop.

Select Log Out from the menu. A pop up window appears , asking if user want to log out.

Select OK from the pop-up menu . This will log user out and return user to either the graphical login screen or to user shell login prompt.

Select OK to finish exiting from GNOME.

4. LINUX COMMANDS

THE SHELL INTERFACE

User should use shell to run commands . to get in the shell depends on the configuration i.e. either GUI or CUI .with the desktop GUI running user can open the terminal window to start a shell. User can begin typing commands into the terminal window. After getting in, in the shell interface user should see the shell prompt. The default prompt for the normal user is a dollar sign $. The default prompt for the root user is a pound sign #.

CHECKING THE LOGIN SESSION

To find information about user identity , use the *id* command as follows :

```
$ id
uid=501(chris) gid=105(sales) groups=105 (sales), 4(adm) ,7(lp)
```

this shows that the user name is chris, which is represented by the numeric user ID(uid) 501.which has a group id (gid) of 105.

User can see information about his current login session by using the *who* command .

```
$ who
chris
```

Checking Directories And Permissions

to find out user current directory , type the *pwd* command ,

```
$ pwd
/usr/bin
```

to find out the name of user home directory , type the *echo* command.

```
$ echo $ HOME
/home/chris
```

user can exit the shell by typing *exit* or pressing *ctrl + D*

CREATING FILES AND DIRECTORIES

1. Cat command is used to create a new file,

```
   $ cat  > file name
```

2. *mkdir* command is used to create a new directory

```
$ mkdir  directory name
```

3. *cd* command is used to change to another directory

```
$ cd  directory name
```

4. *chmod* command is used to change the permission on a file or directory

5. *ls* command is used to list the contents of a directory

6. *ls –a* command is used to list all hidden contents of a directory

7. *cp* command is used to copy a file

8. *rm* command is used to remove a file.

9.*mv* command is used to change the location of a file

10. *head* command is used to displays the top of the file,when used without an option, it displays the first ten lines of the file

```
$ head emp1.lst
```

user can use –n option to specify a line cont and display.

11. *tail* command is used to displays the end of the file.

12. *cut* command is used to extract specific coloumns and fields from the file.

Ex-

```
$ head –n 5 emp.lst | tee shortlist
 2233|a.k.shukla | g.m. | sales | 12/12/52|6000
 9876| jai Sharma | director | production | 03/12/50|7000
 5678| sumit chakraborty |d.g.m| marketing | 04/19/43| 6000
  2365|barun gupta | director |personnel | 05/11/47| 7800
 5423 | n.k. gupta | chairman | admin| 08/30/56 |5400
```

to extract specific coloumns ,user need to follow the –c option with a list of coloumn numbers, delimited by a comma.

```
$ cut –c 6-22,24-32 shortlist
 a.k.shukla                  g.m.
  jai Sharma                 director
  sumit chakraborty           d.g.m
  barun gupta                 director
  n.k.gupta                    chairman
```

13. whatever user cut can be pasted back by using *paste* command.

```
 $ paste –d “ |” cutlist1
```

14. *grep* commands scan its input for a pattern, and can display the selected pattern , the line numbers or the filenames where the pattern occurs. The command uses the following syntax:

```
    grep options pattern filename(s)
     $grep “sales” emp.lst
     2233| a.k.shukla |g.m.        | sales     |12/12/52     | 6000
     1006| l.d.Sharma|d.g.m.     |  sales     | 12/03/76    |6700
     1256| n.k.jain      |manager | sales     | 30/04/56     |5700
      2476|s.chand      |manager | sales     | 01/05/64     | 5800
```

when *grep* is used with multiple filenames, it displays the filenames along with the output.

When user look for a name,but is not sure for the case,*grep* offers the –i option Which ignores case for pattern matching:

```
 $grep –I ‘sharma’ emp.lst
 1006 |l.d.Sharma|d.g.m | sales |12/03/76 | 6700
```

15. *groupadd* command is used to create a new group with a GID .

syntax

```
 $ groupadd –g GID groupname
  $groupadd –g GID  nikhil
```

16. *useradd* command is used to add new user to the system . all parameters related to the user have to be provided in the command line itself:

```
# useradd –u 210 –g nikhil –d /home/oracle –s/bin/ksh
```

17. *shutdown* command shut down the machine

```
# shutdown –g2                          shut down the machine after 2 minutes
#shutdown  -y –g0                       shutdown the machine immediately
#shutdown   -y –g0 –i6                  shutdown and reboot the machine.
```

5. UNDERSTANDING SYSTEM ADMINISTRATION

This section describes the general principle of Fedora and RHEL system administration. In general ,this section covers some of the basic tools user need to administer his Linux system . It also helps user learn how to work with his file system and monitor the setup and performance of his Linux system. User Accounts

Three kinds of users are at work in the typical Fedora system environment: the superuser, the regular user, and the system user. All three have important roles and must work cooperatively to accomplish their tasks.

All users have accounts. Fedora Core uses the `/etc/passwd` file to hold user account information. Each user, regardless of type, will have a one-line entry of account information stored in the `/etc/passwd` text file. Each account entry contains a username (used for logging in), a password field containing an `x` (as passwords are actually contained in `/etc/shadow`), a User ID (UID), and a Group ID (GID). The fifth field contains optional human ID information, such as real name, office location, phone number, and so on. The last two fields are the location of the user's home directory and the user's default login shell. See the section "The Password File" later in this chapter for more information.

Fedora uses the traditional form of Unix file ownership and permissions. Each file (which includes directories and devices) can be assigned read, write, and/or execution permission to an owner, a member of a group, or anyone on the system. This information can be viewed with the `ls` command, using `-l` for files or `-ld` for directories. Fedora's file security is derived by combining ownerships and permissions. It is the superuser's responsibility to make sure that all users have proper filename, UIDs, and GIDs and that sensitive system files are protected from improperly permissive write permission assignment.

Although many system administrators might exist on a large system, only one `root` user has (and grants) all privileges on the system. The root user is defined as having a User ID of zero and a Group ID of zero. (We will discuss those `ID`s later in the chapter, but you can see how that `ID` is unique to `root`.)

The `root` user can use any program, manipulate any file, go anywhere in the file system, and do anything within the Fedora Core Linux system. For reasons of security, that kind of raw power should only be given to a single trusted individual.

It is often practical for that power to be delegated by the `root` user to other users. This delegation is referred to as an elevation of privileges, and these individuals are known as superusers because they enjoy the same powers that `root` enjoys. This approach is normally only used on large systems in which one person cannot effectively act as the system administrator.

The system user is not a person, but a process running on the computer. The system user requires ownership of files and processes so that it can do its job in a secure manner. (Fedora calls these users logical users.) For example, the system user named `apache` owns the web server (assuming that you are using Apache) and all the associated files. No one else (except `root`) may have access to those files in a way that Apache does not permit. Unlike regular users, system users do not have a home directory or password and cannot log in like a regular user.

You will find a list of all the users on a system in the `/etc/passwd` file. Fedora refers to these users as the standard users because they will be found on every Fedora computer as the default set of system (or logical) users provided during the initial installation. This "standard" set differs between Linux distributions.

USING THE ROOT USER ACCOUNT

The traditional role of the root user in Linux system is to have complete control of the operation of user ‘s Fedora system. That user can open any file or run any program .The

Root user also installs software packages and adds accounts for other people who use the system.

During the Fedora OR Rhel installation process ,user required to add a password for the root user. User need to remember and protect this password. User will need it to log in as root or to obtain root permission while user logged in as some other user.

The home directory for root user is /root .the home directory and other information associated with root user account is located in /etc/passwd file. The root entry looks like in the /etc/passwd file as :

```
Root: x:0:0:root:/root:/bin/bash
```

This shows that for the user named root ,the user id is set to 0(root user) ,the group ID is set to0 (root group),the home directory is /root ,and the shell for that user is /bin/bash.User can change the home directory or the shell used by changing the values in this file.

BECOMING SUPER USER(THE SU COMMAND)

Though one way to become the super user is to log in as root,sometimes that is not convenient. For example, user may logged into a regular user account and just want to make a quick administrative change to user system without having to log out and log back in.Or user ay need to log in over the network to make a change to a Linux system but find that the system doesn’t allow root users in from over the network.

The answer is that user can use the *su* command.from any terminal window or shell ,user can simply type:

```
$ su
password : *****
#
```

when you are prompted, type in the root user’s password. The prompt for the regular user ($) will be changed to the super user prompt(#)

user can also use the su command to become another user then root

for ex to have the permissions of user named *chum.*

```
$su -  chum
```

even if user was root user before user typed this command, user would only have the permissions to open files and run programs that are available to chum. As root user ,however, after user type su command to become another user, user don't need a password to continue. If user type that command as a regular user, user must type the new user's password. When user finished using super user permissions, return to the previous shell by exiting the current shell. Do this by pressing the Ctrl+D or by typing exit.

GRANTING SYSTEM ADMINISTRATOR PRIVILEGES TO REGULAR USERS

On occasion, it is necessary for regular users to run a command as if they were the root user. They usually do not need these powers, but they might on occasion—for example, to temporarily access certain devices or run a command for testing purposes.

There are two ways to run commands with root privileges: The first is useful if you are the superuser and the user; the second if you are not the regular user (as on a large, multiuser network).

Temporarily Changing User Identity with the su Command

What if you are also root, but are logged on as a regular user because you are performing non-administrative tasks and you need to do something that only the superuser can do? The `su` command is available for this purpose

Granting Root Privileges on Occasion—The sudo Command

Often it is necessary to delegate some of the authority that `root` wields on a system. For a large system, this makes sense because no single individual will always be available to perform superuser functions. The problem is that Unix permissions come with an "all or nothing" authority. Enter `sudo`, an application that permits the assignment of one, several, or all of the root-only system commands.

Once configured, using `sudo` is simple. An authorized user merely precedes the superuser-authority–needed command with the `sudo` command, like so

```
$ sudo command
```

LEARNING ABOUT ADMINISTRATIVE GUI TOOLS, COMMANDS, CONFIGURATION FILES,AND LOG FILES

Fedora and RHEL have advanced enough in recent releases that user can now do most system administration from user desktop GUI ,bypassing the shell altogether. Whether user administer Linux fro the GUI or from a shell, however , underlying user activities are many administrative commands,configuration files,and log files.
Understanding where GUI administrative tools, commands, and files are located and how they are used will help user effectively maintain user Linux system . Although most administrative features are intended for the root user ,other administrative sers have limited administrative capabilities .

USING GRAPHICAL ADMINISTRATIVE TOOLS

The trend over the past few versions of Fedora and RHEL distributions has been to steer clear of the massive administrative interfaces and instead to offer graphical windows that perform individual administrative tasks . Instead of sharing one monolithic interface , they share common menus.individual graphical windows for configuring a network,adding users or setting up printers can be launched from those menus. To administer user 's Fedora or RHEL system through the GNOME or KDE desktops ,Red Hat ,Inc.has provided a common set of menus under the applications and Desktop buttons on the panel . selections for starting most graphical administration windows are available by selecting one of these two menus:

- *System settings* – Select desktop – system settings from the desktop panel to select tools for configuring user's system . These include tools for adding users, setting date and time , configuring user network,setting up printers , and getting sound cards and printers to work.

- *System tools* – Select Applications – System Tools from the desktop panel to select tools to monitor and work with user's system .these include tools for doing backups , monitoring the system ,and checking network activity.

Because these administrative tasks require root permission ,if you are logged in as a regular user you must enter the root password before the GUI application's window opens. For example ,if you launch the system logs window from the desktop panel as a regular user .
After user have entered the root password , most of the system configuration tools will open without requiring user to retype the password during this login session .

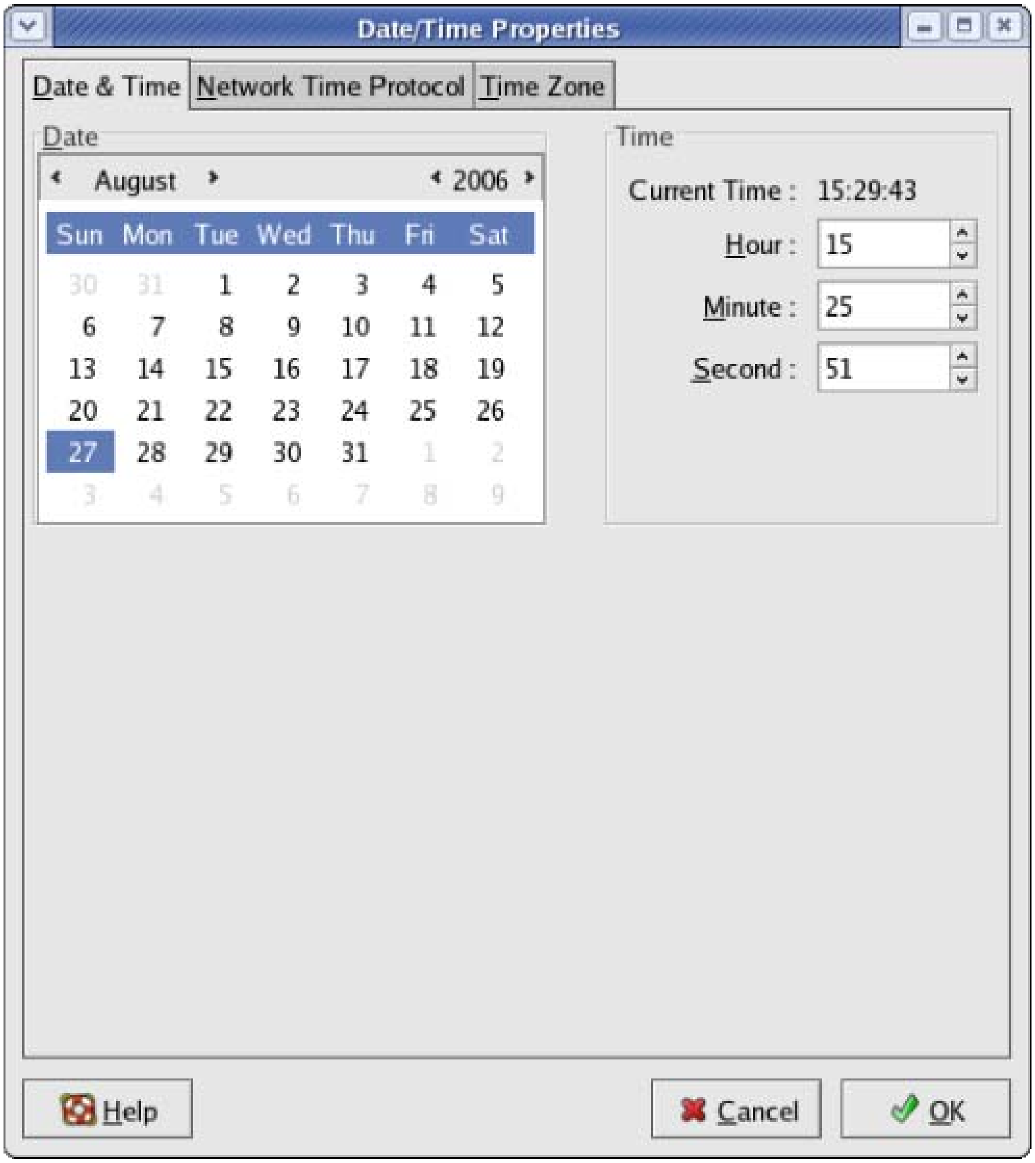
The following lists describes the administrative tools user can start from the System settings menu(desktop-system settings):

- ❖ *Server Settings*--- This submenu accesses the following server configuration windows:
    1. Domain name system- Create and configure zones if user computer is acting as a DNS server.
    2. HTTP – configure user computer as an Apache Web server.
    3. NFS – set up directories from user system to be shared with other computers on user network using the NFS service .
    4. Samba- configure windows file sharing .
    5. Services – display and change which services are running on user Fedora or RHEL system at different run levels.

Add/Remove Applications ---

Manage software packages in the fedora and RHEL distributions.

- *Authentication* –Change how users are authenticated on user system.
- Date & Time – Set the date & time or chose to have an NTP server keep system time in sync.



Date

August 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Time

Current Time : 15:29:43

Hour : 15

Minute : 25

Second : 51

6. *Display* – Change the settings for user X desktop,including color depth and resolution for user display.

7. *Network* – Manage user current network interfaces,as well as add interfaces.
8. *Red Hat Network Configuration* – configure user system to use the up to date facility to get software updates for Fedora or RHEL.

ADMINISTRATIVE COAMMANDS

Many commands are intended only for root. When user log in as root, user $PATH variable is set to include some directories that contain commands for the root user. These include the following directories:

1. /sbin- This contains commands for modifying user disk partitions ,changing boot procedures(grub), and changing system states(init).
2. /usr/sbin – This contains commands for managing user accounts(such as user add) and configuring user mouse. Commands that run as daemon are also contained in this directory.

ADMINISTRATIVE CONFIGURATION FILES

Configuration files are another mainstay of Linux Administration. Configuration files are needed to setup the different features that make up Fedora and RHEL systems. There are several locations in a Fedora file system where configuration files are stored. Some of major locations are:

$HOME – All users store information in their home directories that directs how their login accounts behave.Most configuration files in $HOME begin with a dot(.), so they don't appear as a user's directory when user use a standard *ls* command .There are dot files that define how each user's shell behaves, the desktop look and feel, and options used with user text editor. There are even files that configure network permissions for each user.

/etc – This directory contains most of the basic Linux system-configuration files. The following /etc configuration files are of interest :

aliases – Can contain distribution lists used by the Linux mail service.
Exports - Contains a list of local directories that are available to be shared by remote computers using the Network file system(NFS)
Fstab – Identifies the devices for common storage media and locations where they are mounted in the Linux system. This is used by the mount command to choose which files systems to mount.
Host.conf – Sets the locations in which domain names are searched for om TCP/IP networks .By default ,the local hosts file is searched, then any namesaver entries in resolv.conf.
Hosts – contains IP address and hostnames that user can reach from his computer.
Hosts.allow – Lists host computer that are allowed to use certain TCP/IP services from the local computer.
Protocols – sets protocol numbers and names for a variety of internet services.
Resolv.conf – identifies the location of DNS name server computers that are used by TCP/IP to translate internet host.domain names into IP addresses.
Services – Defines TCP/IP services and their port assignments.
Shells – lists the shell command line interpreters that are available on the system, as well as their locations.
/etc/cups – contains files that are used to configure the CUPS printing service.
/etc/init.d – contains the permanent copies of run-level scripts .

- /etc/squid – contains configuration files for the Squid proxy caching server.
- /etc/sysconfig – contains important system configuration files that are created and maintained by various system services.

ADMINISTRATIVE LOG FILES

One of the things that Linux does well is keep track of itself. This is a good thing, when user consider how much can go wrong with a complex operating system. Sometimes user is trying to get a new facility to work and it fails without giving user the foggiest reason why. Other times user want to monitor his system to see if people are trying to access his computer illegally. In any of those cases ,user can use log files to help track down the problem.

The main utilities for logging error and debugging messages for Linux are the syslogd and klogd daemons .general system logging is done by syslogd. Logging that is specific to kernel activity is done by klogd.

USING THE MOUNT COMMAND TO MOUNT THE FILE SYSTEMS

User fedora system automatically runs ‘mount –a’ each time user boot. The average user or administrator uses mount command in two ways:

1. to display the disks,partitions, and remote file systems that are currently mounted.
2. to temporarily mount a file system.

Any user can type the mount command to see what files systems are currently mounted on the local Linux system . the most common devices to mount by hand are the floppy disk and CD-ROM .however depending on the type of desktop user is using , CD-ROMs and floppy disk may be mounted for user automatically when user insert them.

USING THE UMOUNT COMMAND TO UNMOUNT A FILE SYSTEM

When user want to unmount a permanent file system temporarily, user can use the umount command .this command detaches the file system from its mount point in user Linux file system.. the umount command will fail if the device is mounted in more than one location.

6. CONNECTING TO THE INTERNET

SETTING UP DIAL-UP PPP

Point to point protocol is used to create Internet Protocol (IP) connections over serial lines . Most often ,the serial connection is established over a modem,however ,it will also work over serial cables or digital lines.

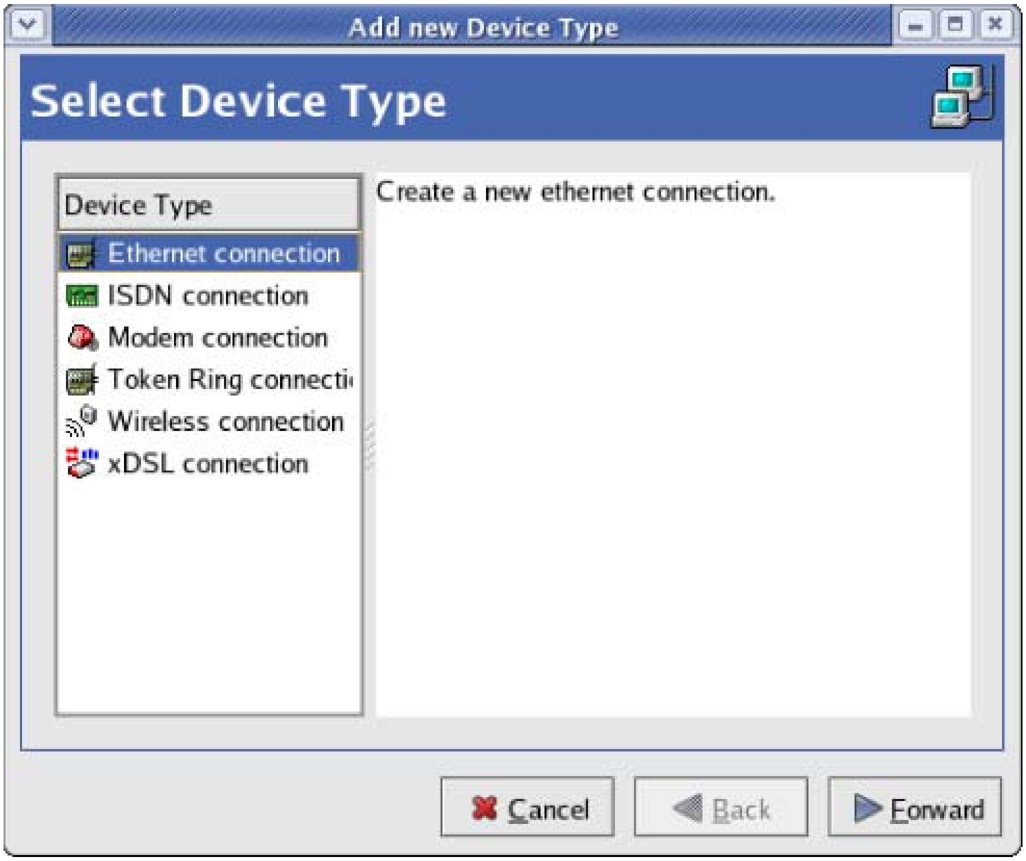
Although one side must dial out while other side must receive the call to create a PPP connection over a modem, after the connection is established, inforation can flow in both directions.

Dial-up can be configure by using either the Internet Configuration Wizard or through KPPP window .

- Internet configuration wizard – From the applications menu,choose system tools then internet configuration wizard. The select device type window that appears lets user configure and test his dial-up PPP connections.
- KPPP window – From the KDE desktop ,select internet then KPPP, or from a terminal window run the ‘kppp’ command. From the KPPP window user can set up a PPP dial –up connections and launch it.

CREATING A DIAL –UP CONNECTION WITH THE INTERNET CONFIGURATION WIZARD

User can use the Internet configuration wizard to set up dial-up networking. To start it, choose application then system tools then internet configuration wizard from the desktop panel.A selected Device type window appears to help user select the device for user internet connection.



Create a new ethernet connection.

Follow the procedure from the first select device type window.

1. from the select Device type window that appears,select mode connection and click forward. The wizard searches for a modem and the select modem window appears.
2. select the following modem properties :
   - *modem device* – if the modem is connected to user first serial port user can select /dev/ttyS0; for the second serial port choose /dev/ttyS1.
   - *Use touch tone dialing* – Leave this check box on in most cases. If for some reason user phone system doesn't support touch-tone dialing ,user can turn it off.

   Click Forward . The select provider window appears.
3. Enter the following provider information :
   - *Internet provider* – if user is using internet service in any of the countries shown in the internet provider window ,select the plus sign next to that

country name.if the internet provider appears under national list ,select it . Information is automatically filled in for that provider. Otherwise ,user will need to fill in the rest of the dialog window.click forward .

- phone number – Enter the telephone number of the ISP user want to dial into.
- Provider name – the name of the internet service provider .user could use ppp0 here as the provider name, to identify the interface.
- *Login name* – the login name assigned to user from the ISP . the ISP may have called the login name a login ID or something similar.
- *Password* – the password associated with the login name .

Click forward,and the IP settings window appears

with a dial –up connection ,user would typically select automatically obtain IP address settings. However , if the ISP has assigned a static IP address check box, and then enter user IP address, subnet mask, Default gateway address. Then click forward to continue.

4. click the ppp device name and click the Activate button. The Internet dialer starts up and dials user ISP. If everything is working properly ,user should see his login and password accepted and the ppp connection completed.

LAUNCHING PPP CONNECTION

Although the dial- up connection should now configured ,it is not set automatically. One way to start the connection is to set it up to launch from the desktop panel.

From the GNOME desktop :

1. right click the panel and then choose add to panel then application launcher then system settings then network. An icon appears on the panel that user click to open the network configuration window.
2. select the new icon from the panel . a network configuration window appears.
3. select the dial-up interface user added and click Activate to connect .

here is an example of settings user can add to his dial-up configuration file to configure on –demand dialing :

```
ONBOOT = yes
DEMAND = yes
IDLETIMEOUT = 600
RETRYTIMEOUT =30
```

The ONBOOT=yes starts the pppd daemon. Also,because DEMAND=yes , a dial-up connection attempt is made any time traffic tries to use user dial-up connection. With IDLETIMEOUT set to 600 ,the connection is dropped after 600 seconds with no traffic on the connection . With RETRYTIMEOUT set to 30 ,a dropped connection is retried after 30 seconds.

SETTING UP LINUX AS A PROXY SERVER

One way to provide Web –browsing services to the computers on the LAN without setting up routing is to configure Linux as a proxy server.

The squid proxy caching server software package comes with Fedora . the basic proxy services available with squid are :

1. *HTTP* – allowing HTTP proxy services is the primary reason to use squid. This is what lets client computers access Web pages on the internet from their browsers .
2. *FTP* – this represents represents File Transfer Protocol proxy services. When user enable HTTP for a client, user enable FTP automatically .
3. *Gopher* – the gopher protocol proxy service was one of the first mechanisms for organizing and searching for documents on the internet.

STARTING THE SQUID DAEMON

When user install Fedora ,user have an opportunity to install Squid ,I f user is not sure whether Squid was installed or not type the following :

```
# rpm –q squid
```

```
squid-2.5.STABLE8-2
```

user can check whether squid is configured or not by

```
#chkconfig - - list squid
squid  0: off 1:off 2:off 3:off  4:off 5 :off 6: off
```

if the squid service is off for run levels 3,4,5 ,user can set it to start automatically at boot time .to set up the squid daemon to start at boot time,

```
#chkconfig squid on
```

at this point squid daemon should start automatically when system boots. By default squid daemon will run with the –D option . The –D option enables squid to start without having an active Internet option.

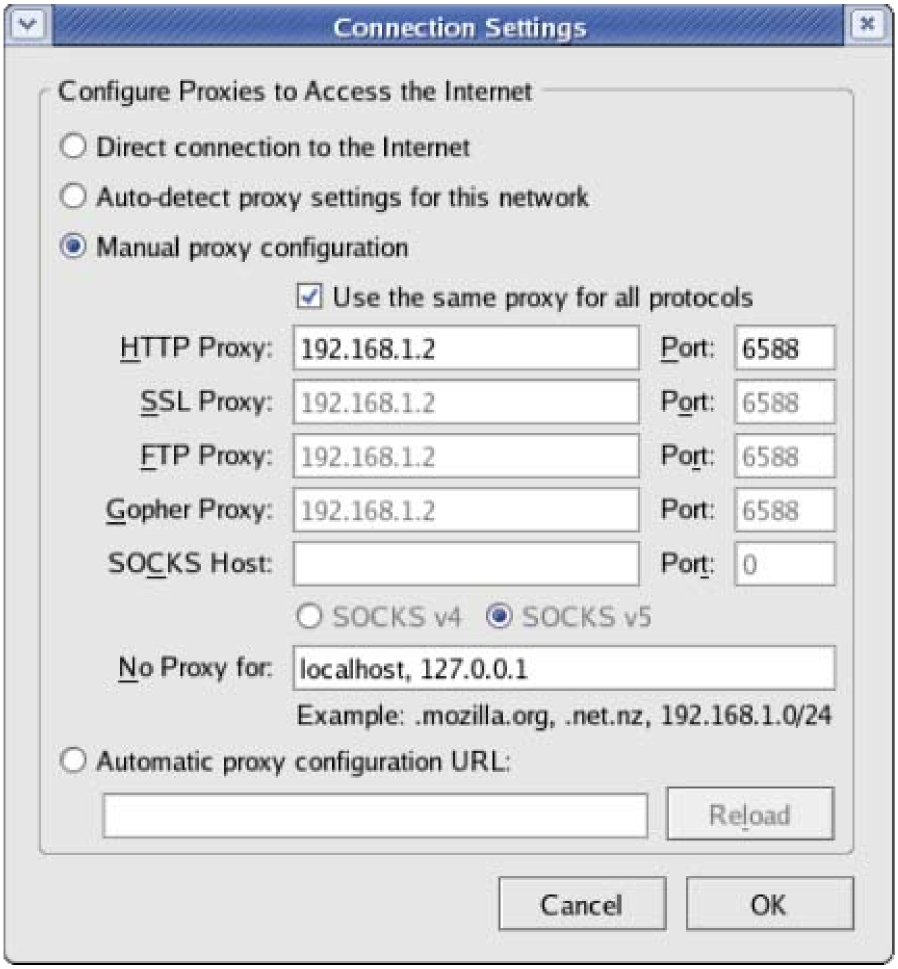
User can restart the squid service by /etc/init.d/ squid restart.

With the squid daemon ready to run ,user need to set up the squid .conf configuration file.

Configuring Mozilla or Firefox to use a proxy

Normally user would set up Mozilla to browse the Web directly over a TCP/IP connection to the Internet. Follow this procedure to change Mozilla to access the Web through user proxy server:

1. open Mozilla or Firefox.
2. choose Edit then Preferences . the Preferences window appears.
3. in Mozilla, next to advanced category , click the plus sign and select Proxies. In Firefox ,select the general category and click connection settings.
4. click Manual proxy configuration to open the Proxies window
5. type the proxy server’s name or IP address in the address boxes for HTTP,FTP and Gopher services.
6. Type the port number for HTTP services on user proxy server in the port boxes for HTTP ,FTP,and Gopher services
7. click ok.



Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet

○ Auto-detect proxy settings for this network

● Manual proxy configuration

☑ Use the same proxy for all protocols

HTTP Proxy:	192.168.1.2	Port:	6588
SSL Proxy:	192.168.1.2	Port:	6588
FTP Proxy:	192.168.1.2	Port:	6588
Gopher Proxy:	192.168.1.2	Port:	6588
SOCKS Host:		Port:	0

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Understanding local area networks

Connecting the computers in user organization via a LAN can save a lot of time and money . with a LAN ,user begin to open the greatest potential of Linux – its ability to act as a server on a network . Because Fedora and RHEL are more robust and feature rich than other computing systems, adding it to user’s LAN can provide a focal point to workstations that could use Linux as a file server, a mail server , a print server, a web server or a boot server.

Creating and configuring a LAN consists of these steps:

1. *Setting up LAN hardware* – this entails choosing a network topology ,purchasing the equipment user need, and installing it

2. *Configuring TCP/IP*- To use most of the networking applications and tools that come with Linux ,user must have TCP/IP configured. TCP/IP lets user communicate not only with computers on user’s own LAN but also with any computer that user can reach on his LAN, modem, or other network connection.

7. SETTING UP LOCAL AREA NETWORK

SETTING UP LAN HARDWARE

LAN TOPOLOGIES

Most small office and home LANs connect computers together in one of the following topologies :

- *Star topology* – The star topology is by far the most popular LAN topology .In this arrangement ,each computer contains a Network Interface Card (NIC) that connects with a cable to a central hub. Other equipment such as printers and fax machines ,can also be connected to the hub in a star topology.
- *Bus topology* – Instead of using hubs, the bus topology connects computers in a chain from one to the next. The cabling usually used is referred to as coaxial,or Thin Ethernet cable. A “T” connector attaches to each computer’s NIC, then to two adjacent computers in the chain . At the two ends of the chain, the T connectors are terminated.
- *Ring Topology* – This is a less popular topology than star and bus topologies. In a ring topology ,computers connect to a ring of wires on which tokens are taken and passed by computers that want to send information on the network.This type of topology typically uses IBM’s token ring protocols.

LAN EQUIPMENT

The equipment that user need to connect user LAN can include some of the following:

- o *Network interface card(NIC)* – Typically ,one of these cards goes into a slot in each computer. For wired Ethernet networks,the cards can transmit data at 10 Mbps or 100 Mbps.Gigabit(1000 Mbps) NIC’s are also available, but are quite a bit more expensive.

- *Cables* – For star topology ,cables are referred to as twisted pair. Category 5e wiring , which contains four twisted –pair sets per wire, is the most common type of wiring used for LANs today.These cables plug into the computer’s NIC at one end and the hub at the other.
- *Hubs* – With the star toplology ,a hub is typically used to connect the computers. Sometimes hubs are also referred to as repeaters because they receive signals from the nodes connected to them and send the signals on to other nodes.
- *Switches* – A switch can be used instead of a hub. It lets user divide a LAN that is getting too large into segments that are more manageable . A switch can reduce network traffic by directing messages intended fir a specific computer directly to that computer. This is as opposed to a hub ,which broadcasts all the data to all nodes.

LAN EQUIPMENT SETUP

With an Ethernet card, appropriate cables, hub, user is ready to set up his wired Ethernet LAN. The steps for setting up an Ethernet LAN are:

1. Power down each computer and physically install the NIC card
2. Using cables appropriate for NIC cards and hub ,connect each NIC to the hub.
3. Power up each computer.
4. If Fedora is not install yet,install the software and reboot.
5. If Fedora is already installed, configure the Ethernet cards.
6. When the system comes up,Ethernet card and interface should be ready to use.

NETWORKING WITH TCP/IP

The basic building block for any network based on Unix hosts is the Transport Control Protocol/Internet Protocol (TCP/IP) suite of three protocols. The suite consists of the Internet Protocol (IP), Transport Control Protocol (TCP), and Universal Datagram Protocol (UDP). IP is the base protocol. The TCP/IP suite is packet-based, which means that data is broken into little chunks on the transmit end for transmission to the receiving end. Breaking data up into manageable packets allows for faster and more accurate transfers. In TCP/IP, all data travels via IP packets, which is why addresses are referred to as IP addresses. It is the lowest level of the suite.

TCP is a connection-based protocol. Before data is transmitted between two machines, a connection is established between them. When a connection is made, a stream of data is sent to the IP to be broken into the packets that are then transmitted. At the receiving end, the packets are put back in order and sent to the proper application port.

On the other hand, UDP is a connectionless protocol. Applications using this protocol just choose their destination and start sending. UDP is normally used for small amounts of data or on fast and reliable networks.

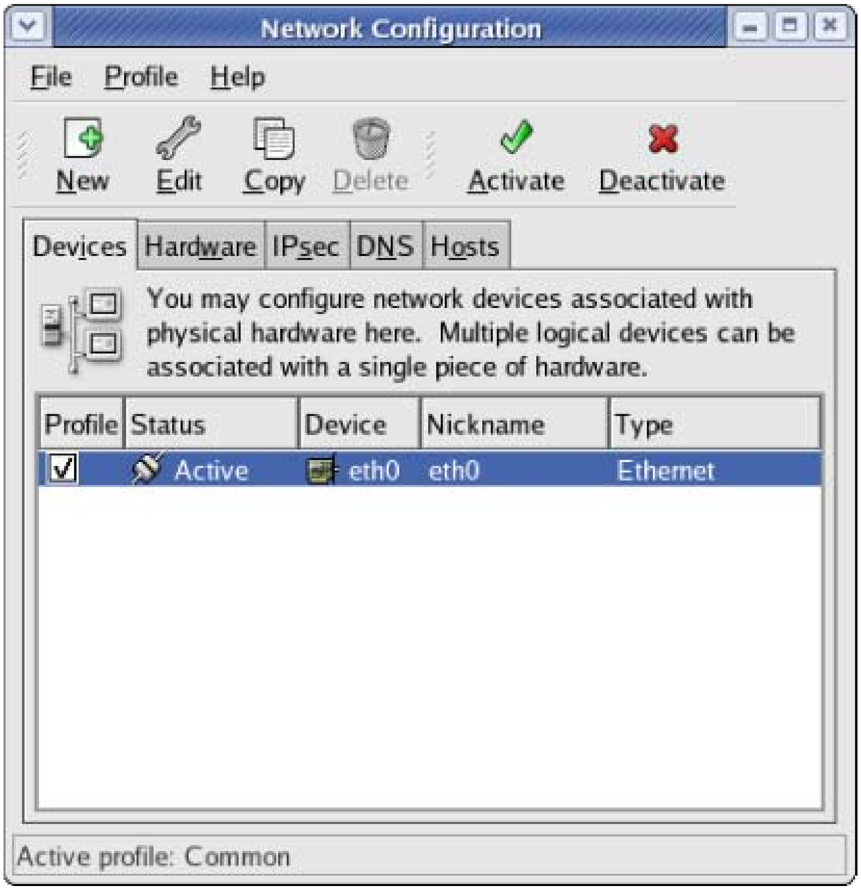
CONFIGURING TCP/IP FOR USER'S LAN

When we install Fedora , we have given the opportunity to add user TCP/IP host nae and address, as well as some other information ,to user computer or choose to have that information automatically provided using DHCP, or dynamic host configuration protocol. User can also set up a way to reach other computer on his LAN by name . that's typically done by adding computer names and IP address to user /etc/hosts file or using a DNS server.

To define user's IP address for user's Ethernet interface, follow this procedure:

1. Start Network configuration .From the desktop menu ,click system settings then network or, as root user from a terminal window, type *neat* . The Network configuration window appears.

2. Click the Devices tab. A listing of USER existing network interfaces .
3. Double click the eth0 interface. A pop up window appears, enabling user to configure his eth0 interface .



You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Active	eth0	eth0	Ethernet

Active profile: Common

4. On the Ethernet Devices window that appears, user can enter the following information:
    - Activate device when computer starts: Check here to have eth0 start at boot time.
    - Allow all users to enable and disable the device: Check to let non root users enable and disable the network interface.
    - Enable Ipv6 configuration for this interface: Check here if user is connected to an Ipv6 network.

5. On the same window, user must choose whether to get user IP address from another computer at boot time or enter the address himself .

- Automatically obtain IP address settings with:select this check box if user have a DHCP or BOOTP server network from which user can obtain user's IP address, net mask, and gateway.DHCP is the most common way to connect to user ISP.
- *Statically set IP address :* If there is no DHCP ,or other boot server,on LAN,user can add necessary IP address information statically by selecting this option and adding the following information:

  Address: Type the IP address of this computer into the Address box. This no. must be unique on user network . For user private LAN ,user can use private IP address.

  Subnet mask : Enter the net mask to indicate what part of the IP address represents the network.

  Default Gateway Address: If a computer connected to user LAN is providing routing functions to the internet or other network, type the IP address of the computer into this box.

6. click ok in the Ethernet Device window to save the configuration and close the window.
7. Click File then Save to save the information entered.
8. Click Activate in the Network Configuration Window to start user connection to the LAN.

NETWORK ORGANIZATION

Properly organizing your network addressing process grows more difficult as the size of your network grows. Setting up network addressing for a Class C network with fewer than 254 devices is simple. Setting up addressing for a large, worldwide company with a Class A network and many different users can be extremely complex. If your company has fewer than 254 hosts (meaning any device that requires an IP address, including computers, printers, routers, switches, and other devices) and all your workgroups can share information, a single Class C network will be sufficient.

Subnetting

Within Class A and B networks, there can be separate networks called subnets. Subnets are considered part of the host portion of an address for network class definitions. For example, in the 128. Class B network, you can have one computer with an address of 128.10.10.10 and another with an address of 128.10.200.20; these computers are on the same network (128.10.), but they have different subnets (128.10.10. and 128.10.200.). Because of this, communication between the two computers requires either a router or a switch. Subnets can be helpful for separating workgroups within your company.

Often subnets can be used to separate workgroups that have no real need to interact with or to shield from other groups information passing among members of a specific workgroup. For example, if your company is large enough to have its own HR department and payroll section, you could put those departments' hosts on their own subnet and use your router configuration to limit the hosts that can connect to this subnet. This configuration prevents networked workers who are not members of the designated departments from being able to view some of the confidential information the HR and payroll personnel work with.

Subnet use also enables your network to grow beyond 254 hosts and share IP addresses. With proper routing configuration, users might not even know they are on a different subnet from their co-workers. Another common use for subnetting is with networks that cover a wide geographic area. It is not practical for a company with offices in Chicago and London to have both offices on the same subnet, so using a separate subnet for each office is the best solution

Subnet Masks

Subnet masks are used by TCP/IP to show which part of an IP address is the network portion and which part is the host. Subnet masks are usually referred to as netmasks. For a pure Class A network, the netmask would be 255.0.0.0; for a Class B network, the netmask would be 255.255.0.0; and for a Class C network, the netmask would be 255.255.255.0. Netmasks can also be used to deviate from the standard classes.

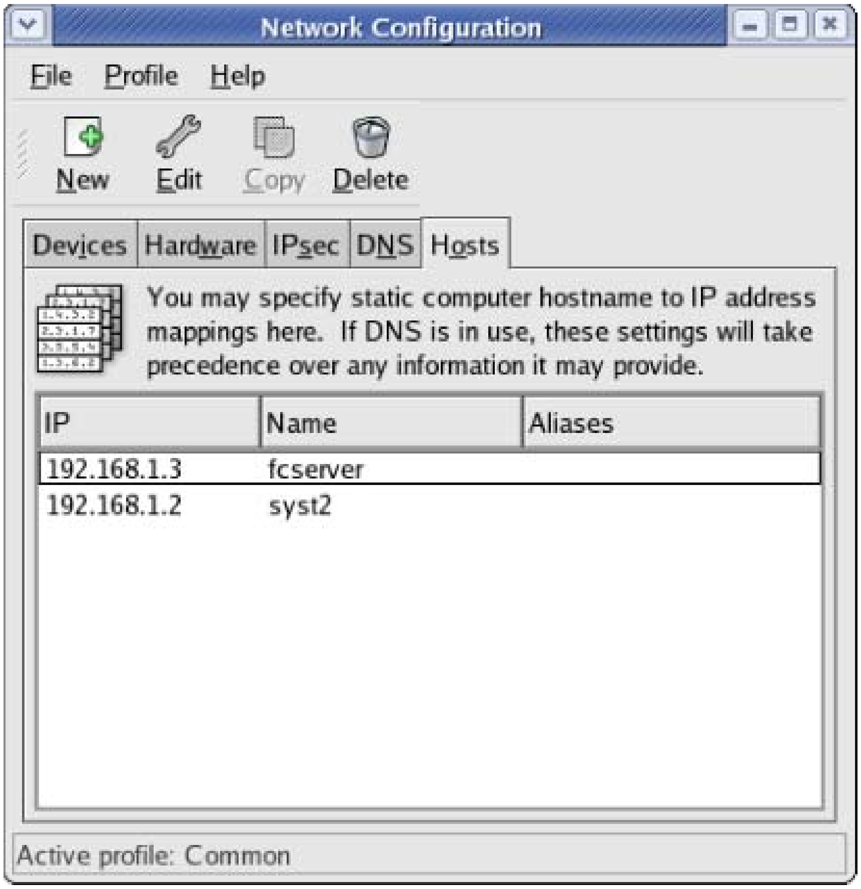
By using customized netmasks, you can subnet your network to fit your needs. For example, your network has a single Class C address. You have a need to subnet your network. Although this isn't possible with a normal Class C subnet mask, you can change the mask to break your network into subnets. By changing the last octet to a number greater than zero, you can break the network into as many subnets as you need.

IDENTIFYING OTHER COMPUTERS (HOSTS AND DNS)

Each tie user use a name to identify a computer, as when browsing the Web or using an E-mail address, the computer name must be translated into an IP address. User can use the Network configuration window to add:

- *Host name and IP address*: User might do this to identify hosts on his LAN that are not configured on a DNS server.
- *DNS search path* : By adding domain names to a search path ,user can browse to a site by its host name and have Linux search the domains user added to search path to find the host user is looking for.
- *DNS name servers* : A DNS server can resolve addresses for the domains it serves and contact other DNS servers to get addresses for all other DNS domains.

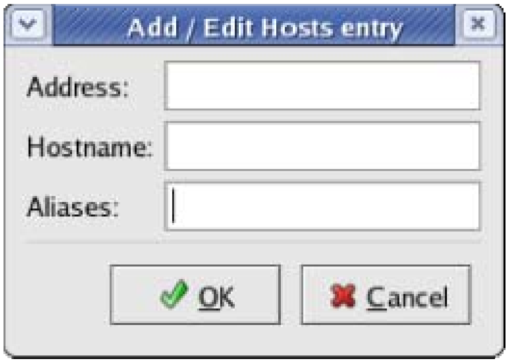
To add host names ,IP address, search paths, and DNS servers do the following:



You may specify static computer hostname to IP address mappings here. If DNS is in use, these settings will take precedence over any information it may provide.

IP	Name	Aliases
192.168.1.3	fcserver	
192.168.1.2	syst2	

Active profile: Common



1. Start the network configuration. As root user from a Terminal window, type neat or fro the desktop menu, click system settings then network .The network configuration window appears.
2. Click the Hosts tab. A list of IP addresses, hostnames ,and aliases appears.
3. Click New. A pop up window appears asking user to add the IP address, hostname, and aliases for a host that user can reach on his network.

4. Type in the IP address number , hostname , and optionally the host alias.
5. Click ok.
6. Repeat this process until user have added every computer on his LAN.
7. Click the DNS tab.
8. Type the IP address of the computers that serve as user’s primary and secondary DNS server . User get these IP addresses from user’s ISP or, if user created user’s own DNS server, user can enter that server’s IP address.
9. Type the name of the domain to be searched for hostnames into the DNS search path box.
10. Select File then save to save the changes.
11. select file then quit to exit.

Now ,when user use programs such as ftp, ssh or other TCP/IP utilities, user can use any hostname that is identified on user local computer, exists in user search path domain, or can be resolved from the Public Internet DNS servers.

ADDING WINDOWS COMPUTERS TO USER’S LAN

It is likely that user have other types of computers on his LAN in addition to those running Linux systems. If there is a DHCP server available on user LAN windows and the most other computer systems can simply start up and begin using the network . in cases where user network card is not properly detected, or user want to set static IP addresses, user need to do some extra configuration.

The following are general steps for doing some manual steps to add user windows computers to the Ethernet LAN user just created:

1. Power down user computer and install an Ethernet card .
2. connect an Ethernet cable from the card to user hub.
3. Reboot the computer . If user card is detected , windows will either automatically install a driver or ask user to insert a disk that comes with the card to install the driver.
4. Open the window to configure networking . a window to change network properties appears.
5. What user do next depends on version of windows user is running.

For windows 98:

- Find the Ethernet card user has just installed in the list and select it.
- Click Add. The select network component type pop up window appears.
- Double click Protocol. The select network Protocol window appears.
- Click Microsoft, and then double click TCP/IP . a new entry should appear in user network window that looks similar to the following , depending on user card: TCP/IP-> 3Com Etherlink III ISA
- Double click on that new entry. The TCP/IP properties window should appear, similar to the one in figure .

For windows 2000 or XP :

- Click Switch to classic view.
- Double click the network connections.
- Double click Local Area connection. The Local Area Connection status window appears.
- Click properties . the Local Area Connection properties window appears.
- Select Internet Protocol (TCP/IP) and click the properties button .the Internet protocol properties window appears

6. Click use the following IP address to configure user IP address manually.
7. Add the IP address, subnet mask, and default Gateway for this computer.
8. Add the IP address of up to two DNS servers.
9. Click ok . user may need to reboot Windows for the settings to take effect.

At this point ,user window computer knows to listen on the network for messages addressed to the IP address user just entered.

UNDERSTANDING INTERNET PROTOCOL ADDRESSES

Each computer user communicate must have an unique address on the network . In TCP/IP ,each computer must be assigned an internet protocol address.

There are two basic ways to assign a hostname and IP address to a network interface in Linux:

1. Static addresses – with static IP addresses, each computer has an IP address that doesn’t change each time the computer reboots or restarts its network interface. Its IP address can be entered manually.

dynamic addresses – With dynamic addresses, a client computer gets it IP address assigned from a server on the network when the client boots. The most popular protocol for providing dynamic addresses is called Dynamic host configuration protocol(DHCP). With this method , a client computer may not have the same IP address each time it boots.

An IP address is a four port number, with each part represented by a number from 0 to 255 . ex- 192.168.34.121

IP ADDRESS CLASSES

There are originally three basic classes of IP addresses, each class representing a different size network.

Class A— Consists of networks with the first octet ranging from 1 to 126. There are only 126 Class A networks—each composed of up to 16,777,214 hosts. (If you are doing the math, there are potentially 16,777,216 addresses, but no host portion of an address can be all zeros or 255s.) The "10." network is reserved for local network use, and the "127." network is reserved for the loopback address of 127.0.0.1. Loopback addressing is used by TCP/IP to enable Linux network-related client and server programs to communicate on the same host. This address will not appear and is not accessible on your LAN.

.*Class B*— Consists of networks defined by the first two octets with the first ranging from 128 to 191. The "128." network is also reserved for local network use. There are 16,382 Class B networks—each with 65,534 possible hosts.

Class C— Consists of a network defined by the first three octets with the first ranging from 192 to 223. The "192." network is another that is reserved for local network use. There are a possible 2,097,150 Class C networks of up to 254 hosts each.

No host portion of an IP address can be all zeros or 255s. These addresses are reserved for broadcast addresses. IP addresses with all zeros in the host portion are reserved for network-to-network broadcast addresses. IP addresses with all 255s in the host portion are reserved for local network broadcasts. Broadcast messages are not typically seen by users.

These classes are the standard, but a netmask also determines what class your network is in. The netmask determines what part of an IP address represents the network and what part represents the host. Common netmasks for the different classes are

Class A— 255.0.0.0

Class B— 255.255.0.0

Class C— 255.255.255.0

Because of the allocation of IP addresses for Internet hosts, it is now impossible to get a Class A network. It is also nearly impossible to get a Class B network (all the addresses have been given out, but some companies are said to be willing to sell theirs), and Class C network availability is dropping rapidly with the current growth of Internet use worldwide.

TROUBLE SHOOTING USER LAN

After user LAN has been set up ,user Ethernet cards installed, and hostnames and addresses added , there are several methods user can use to check that everything is up and working. Some troubleshooting techniques are :

Did Linux find user Ethernet driver at boot time ?

After user boot his computer to verify whether Linux found user card and installed the Ethernet interface properly , type

```
 dmesg  | grep eth
```

the dmesg command lists all the messages that were output by Linux at boot time . The grep eth command causes only those lines that contain the word eth to be printed. The message shown below appeared on computer with the NETGEAR card.

```
Eth0: NE2000 Compatible: port 0x300 , irq3 , hw_addr 00: 80: C8:8C :8E:49
```

The message in the example shows that a card was found at IRQ3 with a port address of 0x300 and an Ethernet hardware address of 00:80:C8:8C:8E:49.

Can user reach another computer on the LAN?

The ping command can be used to send a packet to another computer and to ask for a packet in rerturn. User could give ping either a host name or an IP address.for ex- to ping a computer at IP address 10.0.0.10 on the network, type the following command :

```
# ping 10.0.0.10
```

if that works try again, but this time use the hostname :

```
# ping pine
```

if the computer can reach , the output will look similar to the following:

```
PING pine (10.0.0.10): 56(84) data bytes
64 bytes from pine (10.0.0.10) :icmp_seq=1 ttl =255 time =0.351ms
----ping pine statistics-----
10 packets transmitted, 10 packets received ,0% packet loss, time 9011 ms
rtt min/avg/max/mdev= 0.351/0.402/0.457/0.042 ms
```

A line of output is printed each time a packet is sent and received in return. It shows how much data was sent and how long it took for each package to be received. type Ctrl +C to stop ping.

Is the Ethernet connection up?

Using the *if config* command , user can determine whether the Ethernet are up and running. Type the following command:

```
# ifconfig
```

the output looks like :

```
eth0 Link encap: Ethernet Hwaddr 00: 90: 27 : 4E : 67 : 35
inet addr:10.0.0.10 Bcast: 10.0.0.255 Mask :255.255.255.0
UP broad cast running multicast MTU : 1500 metric:1
RX packets :  156 errors:0 dropped: 0 overruns : 0 frame :0
TX packets :104 errors :0 dropped :0 overruns: 0 carriers : 0
Collisions :0 txqueuelen:100
RX bytes :20179 (19.7 kb) TX bytes : 19960 (19.4 kb)
```

8. SERVER SETUP & CONFIGURATION

GOALS OF SETTING UP A FILE SERVER

Centralized distribution – user can add documents or applications to one location and make them accessible to any authorized computer or user. In this way ,user By centralizing data and applications on a *file server*, user can accomplish several goals:

- don't have to be responsible for placing necessary files on every computer.
- transparency – Using protocols such as NFS ,clients of user file server can connect user's file systems to their local file systems as if user file system existed locally.

SETTING UP AN NFS FILE SERVER

The Network File System (NFS) facility lets user extend his Linux file system to connect file system on other computers to his local directory structure as well.

Creating an NFS file server is an easy way to share large amounts of data among the users and computers in an organization . an administrator of a Linux system that is configured to share its file system using NFS has to perform the following tasks to set up NFS :

1. *Set up the network* – If a LAN or other network connection is already connecting the computers on which user want to use NFS ,user already has the network he need.
2. *On the server, choose what to share* – decide which file systems on user's Linux NFS server to make available to other computers. User can choose any point in the file system to make all files and directories below that point accessible to other computers.
3. *On the server, set up security* – User can use several different security features to suit the level of security with which user is comfortable. there are any type of securities like Mount level security, user level security etc.

4. *On the client ,mount the file system* – Each client computer that is allowed access to the server's NFS shared file system can mount it anywhere the client chooses.

SHARING NFS FILE SYSTEMS

To share an NFS file system from user's Linux system, user need to export it from the server system. Exporting is done in Fedora by adding entries into the /etc/export files. Each entry identifies the directory in user local file system that can share the resource and includes other options that reflect permissions associated with the directory.

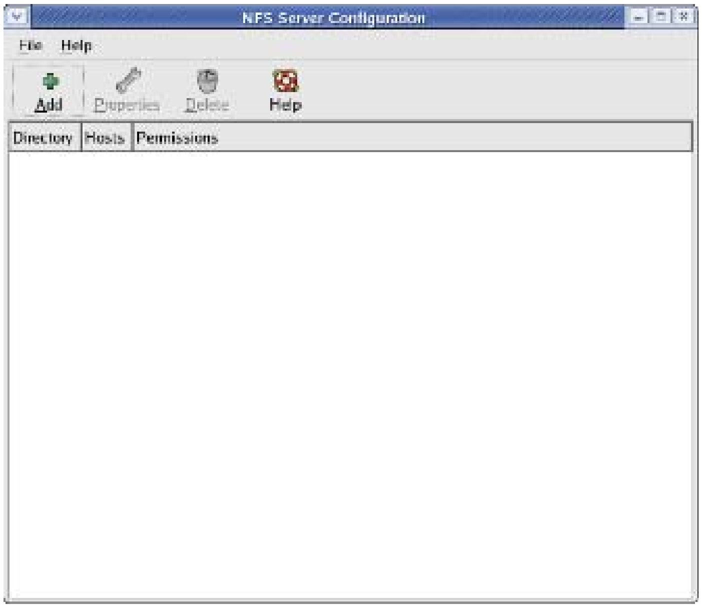
The following section explains how to use NFS Server Configuration window to share directories with other computer

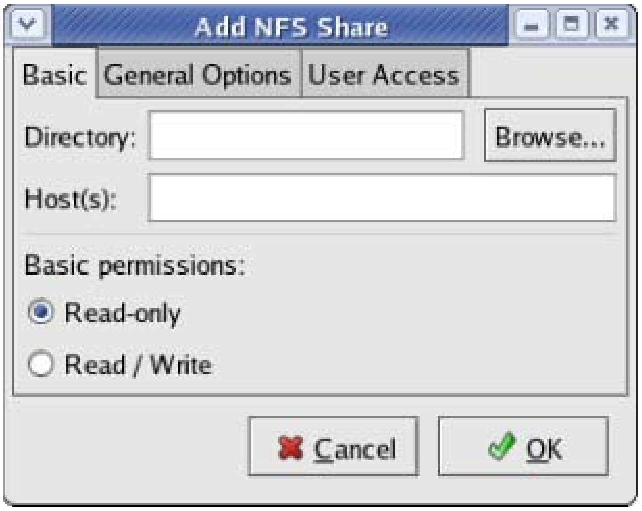
USING THE NFS SERVER CONFIGURATION WINDOW

The NFS Server Configuration Window allows user to share his NFS directories using a graphical interface. Start this window from the desktop menu by clicking system settings then server settings then NFS .

To share a directory with the NFS server configuration window, do the following :

1. from the NFS Server configuration window,click File then Add share. the Add NFS share window appears.




Add NFS Share

Basic | General Options | User Access

Directory:

Host(s):

Basic permissions:

● Read-only

○ Read / Write

2. In the add NFS share window basic tab, enter the following information:

   - *Directory* – Type the name of the directory user want to share.
   - *Hosts* - enter one or more hostnames to indicate which hosts can access the shared directory. Hostnames,domain names and IP address are allowed here.
   - *Basic permissions* – click Read only or Read/write to let remote computers mount the shared directory with read access only or read/write accessm,respectively.

3. click the General Options tab. This tab lets user add options that define how the shared directory behaves when a remote host connects to it

   - Allow connections fro ports 1024 and higher – Normally, an NFS client will request the NFS service from a port number under 1024. Select this option if user need to allow a client to connect to user from a higher port number.
   - Allow insecure file locking – if checked , NFS will not authenticate any locking requests from remote users of this shared directory.
   - Disable subtree checking – By selection this option, NFS won't verify that the requested file is actually in the shared directory
   - Sync write operations on request – This is on by default , which forces a write operation from a remote client to be synced on user local disk when the client request it.

5. click the User Access Tab , then select any of the following options :

- treat the remote root user as local root – If this option is on, it enables the remote root user host accessing user shared directory to save and modify files as through he was the local root user. Having this on is a security risk, since the remote user can potentially modify critical files.
- Treat all client users as anonymous users – When this option is on, user can indicate that particular user and group Ids be assigned to every user accessing the shared directory from a remote computer. Enter the user ID and group ID user want assigned to all remote users.

6. CLICK OK.

The new shared directory appears in the NFS server configuration window.

MANUALLY MOUNTING AN NFS FILE SYSTEM

If user know that the directory from a computer on user network has been exported , user can mount that directory manually using the mount command.here is an example of mounting /tmp directory from a computer named maple on user local computer:

```
# mkdir /media/maple
#mount maple:/tmp/media/maple
```

the mkdir command creates the mount point directory .the mount command then identifies the remote computer and shared file system separated by colon.

To ensure that the mount occurred, type ‘mount’. This command lists all mounted disks and NFS file systems.the output from the mount command shows user mounted disk partitions, special file systems, and NFS file systems.

User can also add options to the mount command line for NFS mounts:

- -a – mount all file system in /etc/fstab
- -f – this goes through the motions of mounting the file systems on the command line .used with the –v option ,-f is useful for seeing whwt mount would do before it actually does it.
- -r – mounts the file system as read only.

- -w – mounts the file system as read/write.

Setting up a Samba file server

Samba is a software package that comes with Fedora . samba enables user to share file systems and printers on a network with computers that use the Server Message Block(SMB) protocol.

SMB is the protocol that is delivered with windows operating systems for sharing files and printers.

On Fedora ,the samba software package contains a variety of daemon processes,administrative tools, user tools.and configuration files. To do basic samba configuration ,user can start with samba server configuration window. This window
Provides a graphical interface for configuring the server and settings directories to share.

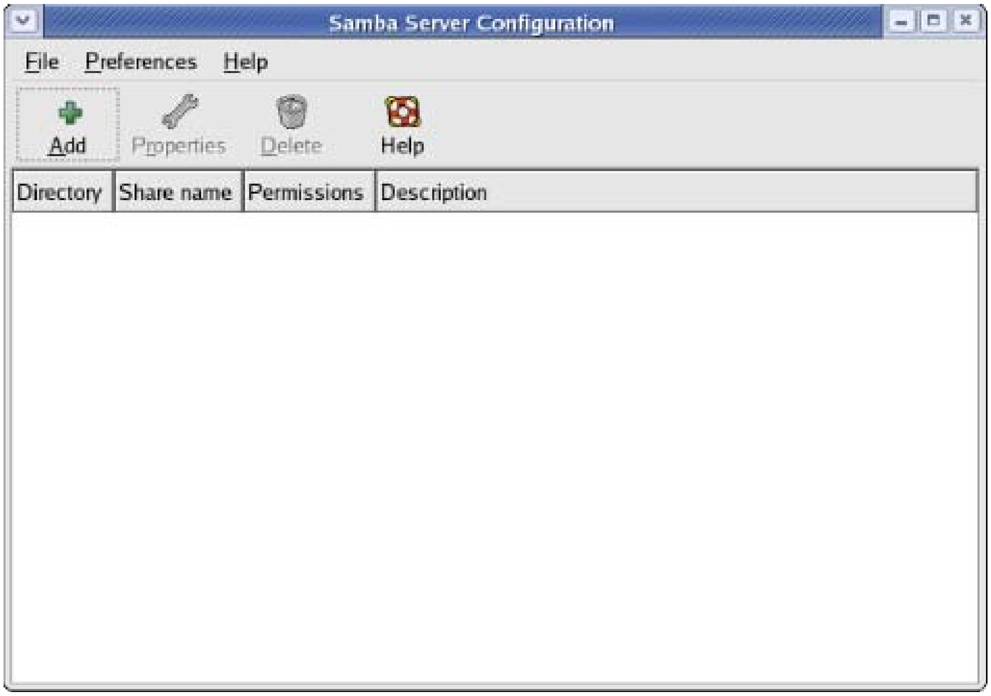
To see if Samba is installed on user Fedora ,type:

```
# rpm –qa | grep samba
```

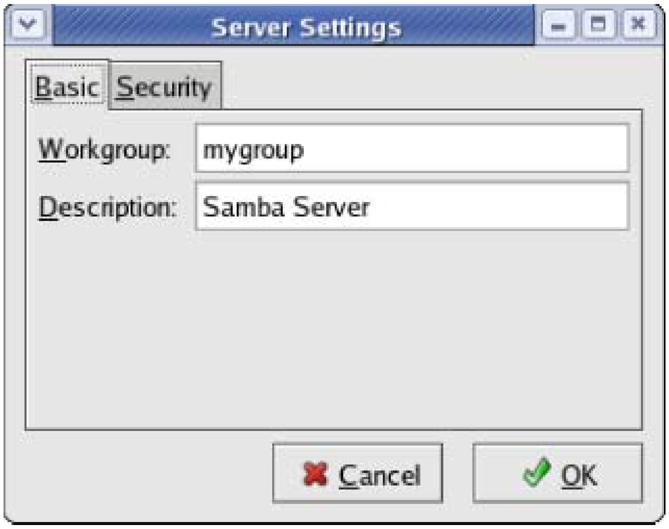
configuring a simple Samba server

The samba server configuration window enables user to do a basic Samba configuration and identify which directories user want to share.the following procedure describes how to configure Samba and create a shared directory in Samba:

1. To open the Samba server configuration window ,click settings then server settings then samba. The samba server configuration window appears.
2. click preferences then server settings .the server settings window appears .



3. type the workgroup name and a short description.
4. click the security tab. A window appears .



Workgroup: mygroup

Description: Samba Server

5. provide the following information for the fields on the security tab and click ok:
   - *authentication mode* – select user ,share, server ,ADS ,or domain.
   - *Authentication server* – this field is only valid if user samba server is configured to use server or domain security. It identifies the server that will be used to authenticate the user name and password the Samba client enters to gain access to this samba server.

- *Kerberos realm* – if user network uses Kerberos for user authentication ,enter the name of user kerberos realm here.
- *Encrypt passwords* – select yes or no .
- *Guest account*- set this field to a user name that user assigned to requests from anonymous users. Even with user mode security set globally ,user can assign guest access to a particular Samba shares.
- With user mode security ,any user who wants to access a samba share must have a regular user account on the linux system.

6. to add a user as a samba user ,select preferences then samba users, the samba users window appears.
7. click add user. The create new samba user window appears.
8. provide information for the following fields in the create new samba user window and click ok:
   - *unix username* – click this check box, then select the Linux user name to which user want to the Samba server.
   - *Windows username* – This is the user name provided by the user when he requests the shared directory .
   - *Samba password* – type the samba password ,then retype it into the confirm samba password field.
9. repeat the previous step for each user to access the samba shared directory .
10. now that user have configured the default values for user samba server,add a directory to share by clicking file then add share . the create samba share window appears.
11. fill in the following fields shown in the create samba share window:
    1. *directory* – type the name of the directory user want to share.
    2. *description* – type any description user like of the shared directory.
    3. *basic permissions* – select either Read only or read/write .
12. click the access tab ,select one of the following choices for access to the share and then click ok:

1. *only allow access to specific users* – click here ,then choose which userwill be allowedto access the shared directory .
2. *allow access to everyone* – choose this option if user want to allow anyone to access this directory.

After user click ok,samba is started and the new directory is immediately available.

INTRODUCTION TO WEB SERVER

The web server usually has a simpler job to accept Hyper Text Transfer Protocol requests and send a response to the client . however this job can get much more complex ,executing functions such as :

1. performing access control based on file permissions , user name / password pairs, and host name / IP address restrictions .
2. parsing a document before sending it to client.
3. sending a java applet to the client.
4. logging any successful accesses, failures and errors.

THE APACHE WEB SERVER

The apache web server is the base for several other web servers, most of which use Apache’s freely available source code and add improved security features such as Secure Sockets Layer(SSL) for encrypted data transfer or advanced authentication modules .

The main features of the Apache Web Server include:

1.the stability and rapid development cycle associated with a large group of cooperative volunteer programmers.

2. full source code , downloadable at no charge.

3. ease of configuration using plain text files.

4. access control based on client host name / IP address or user name / password combinations .

QUICK START THE APACHE WEB SERVER

Quick way to start the apache web server going are:

1.make sure that Apache is installed by typing the following from a terminal window:

```
  $ rpm  -qa | grep httpd
system-config-httpd-1.3.1-2
httpd-devel-2.0.53-6
httpd-2.0.53-6
httpd-manual-2.0.53-6
```

the version no. user see may be different . user need only the httpd package to get started. The httpd-devel package includes the apxs tool for building and installing extension modules. The system config httpd package contains a GUI based Apache configuration tool.

2. A valid host name is recommended for Apache server. If user don't have a real , fully qualified domain name, user can edit the /etc /httpd /conf/ httpd.conf file and define the server name as user computer's IP address.

3. add an administrative E-mail address where someone can contact user in case an error is encountered with user server.

4. start the httpd server. As root user , type the following:

```
# service httpd start
```

this message will appear Starting httpd: [ok].

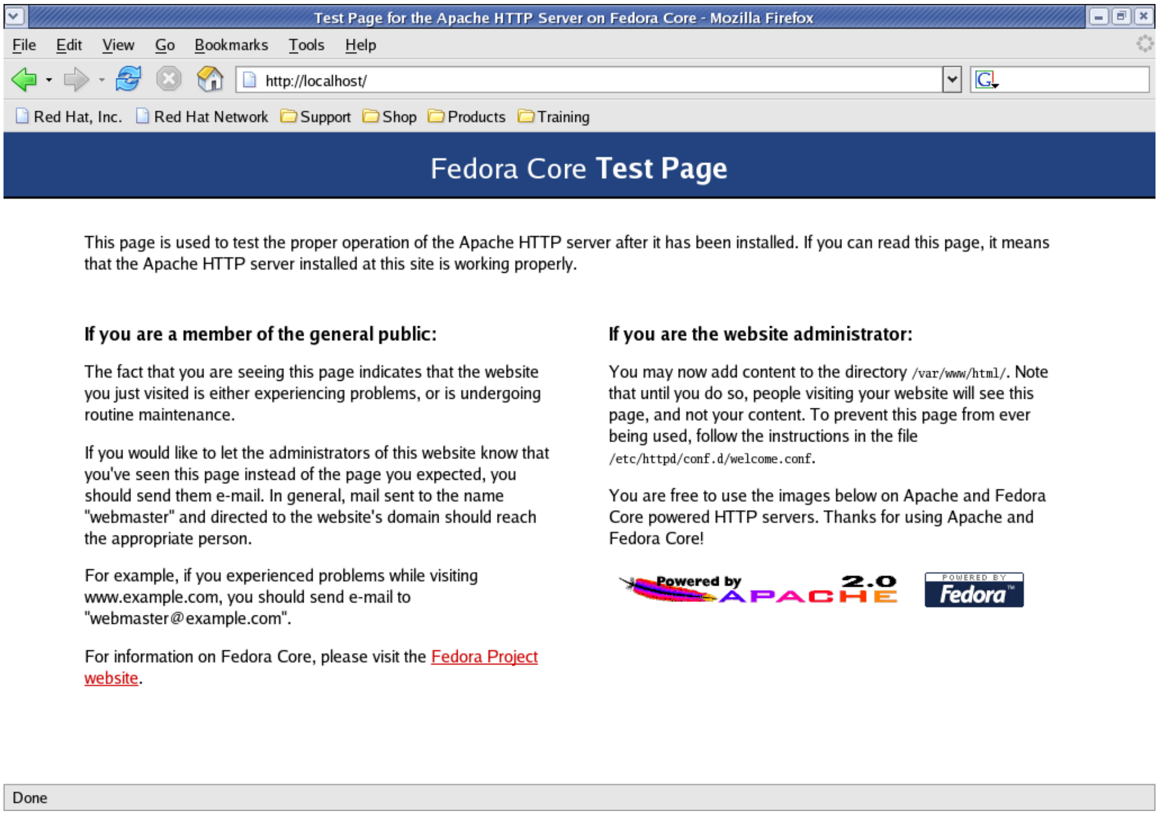
5. user.

```
# chkconfig httpd on
```

6. to make sure that web server is working, open firefox and type the following into the location box and press enter:

http://localhost/

7. user should see the test page for the Apache web server. To access this page from another computer, user will need to enter his Apache server's host name or IP address



Fedora Core **Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Fedora Core, please visit the Fedora Project website.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and Fedora Core powered HTTP servers. Thanks for using Apache and Fedora Core!

8. the test page is actually an error condition, indicating that user haven’t added any content to user web site yet. To get started,user can add an index.html file that contains user own home page content in the /var /www/html directory. That user can continue to add his own content to the directory structure.

CONFIGURING THE APACHE SERVER

The primary file for configuring user Apache web server is httpd.conf. All Apache configuration files are plain text files and can be edited with user favourite text editor . some individual modules, scripts and other services related to Apache , such as perl,php, ssl,webalizer, have individual configuration files that may interest user, those files are contained in the /etc/httpd/conf.d directory.

SETTING UP AN FTP SERVER

On the FTP server files were organized in a directory structures users could connect to the server over the network , move up and down the directory structure to find the files that interested them , and download files from the server. One drawback of FTP server is that when user looked for a file or a document on the internet they had to know which FTP server sever held the file they were looking for.

QUICK STARTING VERY SECURED FTP SERVER

The following is a quick procedure for getting the vsFTPd server up and running.
to use the vsFTPD server , user must make sure that the vsFTPd software package is installed.

```
# rpm –q vsftpd
```

enable the vsftpd server by typing the following line(as a root user):

```
# chkconfig vsftpd on
```

start the vsFTPd server as follows:

```
 # service vsftpd start
```

try to log in to the FTP server as anonymous:

```
 $ ftp local host
connected to yourhost
220(vsFTPD 2.0.3)
530 please login with USER and PASS
name:anonymous
331 please specify the password.
Password:******
230 login successful.
```

Now user vsFTPd server is running.

CONFIGURING VSFTPD

Most of the configuration of vsFTPd is done in the /etc/vsftpd/vsftpd.conf file .

Users who can access your vsFTPd server are, by default, the anonymous user and any users with real- accounts on your system.

The following line set these user access features:

```
Anonymous_enable=yes
Local_enable=yes
```

The first line lets users log in anonymously. second line lets any user with local account can log in.

9.COMPUTER SECURITY ISSUES

LINUX SECURITY CHECKLIST

While Linux Offers ALL the tools user need to secure user computer,if user is careless someone can harm user system or try to steal user's data. The following the checklist covers a range of security measures to protect user's Linux desktop or server.

- *Add users and passwords* – creating separate user accounts is user first line of defense in keeping user data secure.Users are protected from each other,as well as from an outsider who takes over one user account. Setting up group accounts can extend the concept of ownership to multiple users.
- *Read ,write, and execute permissions* – Every item in a linux system can be restricted by read,write, and execute permissions for that item's owner group,as well as by all others. In this way , for example ,user can let other users run a command or open a file,without being able to change it.
- *Protect root* – In standard Linux systems, the root users have special abilities to use and change user's Linux system. Protect the root account's password and don't use the root account when you don't need to an open shell or desktop owned by the root user can be a target for attack
- *Use trusted software* – while there are no guarantees with any open source software, user have a better chance of avoiding compromised software by using an established Linux distribution Software depositories where user get add on packages or updates should likewise be srutinized .Using valid GPG public keys can help ensure that the software user install comes from a valid vendor. And ,of course, always be sure of the source of data files user receive before opening them in a Linux applications.
- *Get software updates* – As vulnerabilities and bugs are discovered in a software packages,every major Linux distributionsoffers tools for getting and installing those updates. Be sure to get those updates,especially if user is using Linux as a server.
- *Use secure applications* – Even with software that is valid and working,some applications offer better protection from attack or invasion than others.

- *Use restrictive firewalls* – A primary job of a firewall is to accept requests for services from a network that user want to allow and turn away requests that user don’t . A desktop system should refuse requests that come in on most ports. A server system should allow requests for a controlled setof ports.
- *Enable only services user need* – To offer services in Linux ,a daemon process will listen on a particular port no. don’t enable services user don’t need.
- *Limit access to services* – user can restrict access for a service user want to have on to a particular host computer,domain,or network interface.For example , a computer with interface to both the Internet and a local LAN might limit access to a service such as NFS to computers on LAN, but not offer those same services to the internet.
- *Check user system* – Linux has tons of tools available for checking the security of user’s system. After user install Linux, user can check access to its ports using nmap or watch network traffic using ethernal. User can add popular security tools such as Nessus, to get a more complete view of user ‘s system security.
- *Monitor user’s system* – User can log almost every type of activity on his Linux system . System log files,using the syslogd and klogd facilities,can be configured to track as much or as little of user system activity as user choose. The logwatch facility provides an easy way to have the potential problem message forwarded to user administrative e-mail account .

USING PASSWORD PROTECTION

Passwords are the most fundamental security tool of any modem operating system and consequently ,the most common attacked security feature . It is natural to want to choose a password that is easy to remember ,but very often this means choosing password that is also easy to guess. Crackers know that on any system with more than a few users ,at least one person is likely to have an easily guessed password.

By using the “brute force” method of attempting to login to every account on the system and trying the most common passwords on each of these accounts ,a persistent cracker has a good shot of finding a way in. remember that a cracker will automate this attack ,so thousands of login attempts are not out of this question obviously ,choosing good passwords is the first and most important step to having a secure system.

Here are somethings to avoid while choosing a password:

do not use any variation of user login name or user full name. Even if user use varied case, append, or prepend numbers or puncuation, or type it backwards,this will still be an easily guessed password.

do not use a dictionary word,even if user add numbers or punctuation to it.

do not use proper names of any kind.

do not use any contiguous line of letters or numbers on the keyboard.

SECURING LINUX WITH IP TABLES FIREWALLS

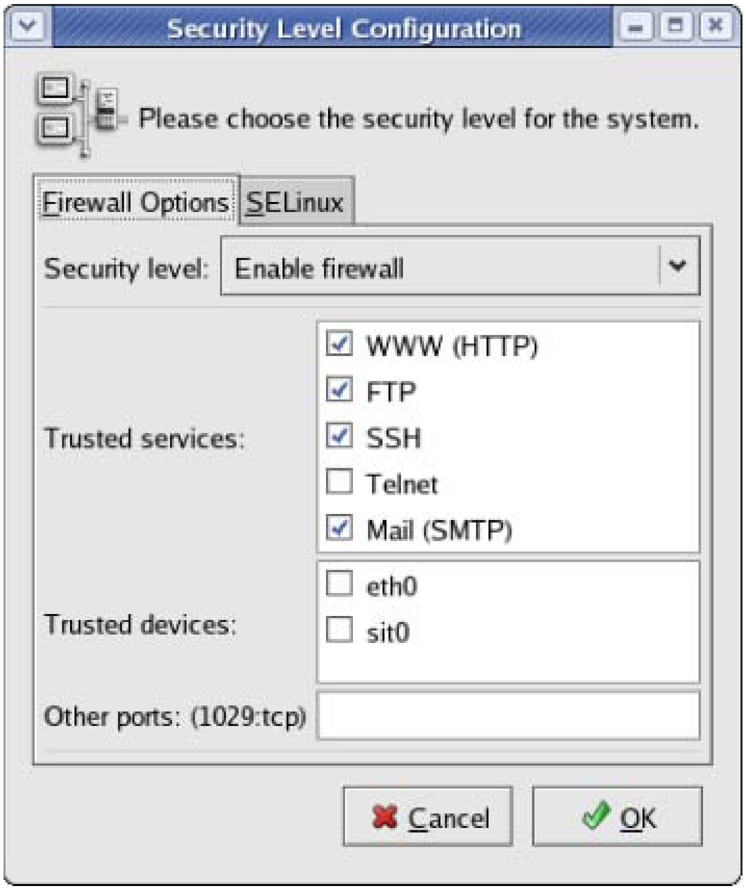
Computer firewalls serve a important purpose to block attacks from crackers on the internet. A firewall also known as a packet filter, is a physical piece of hardware that sits between user network and the internet ,regulating and controlling the flow of information.

The most common types of firewall used today are filtering firewalls. A filtering firewall filters the traffic flowing between user network and the internet , blocking certain things tat may put user network at risk. It can limit access to and from the internet to specific computers on user network . it can also limit the type of communication, selectively permitting or denying various internet services.

For Fedora to act as a firewall ,user can use the iptables features.

STARTING WITH IPTABLES IN FEDORA

Using the security level configuration user can create iptables firewall for the system. To open the security level configuration window ,from the desktop menu select system settings then security level and firewall .



Please choose the security level for the system.

Security level: Enable firewall

Trusted services:
☑ WWW (HTTP)
☑ FTP
☑ SSH
□ Telnet
☑ Mail (SMTP)

Trusted devices:
□ eth0
□ sit0

Other ports: (1029:tcp)

For making selections in security level configuration window :

1. *security level* – select enable firewall.
2. *trusted services* – User can open access to secure web services ,FTP, telnet , HTTP, and secure shell(SSH) by simply clicking the box next to that service. This action opens the common port associated with that service in user firewall , but does not configure the service itself.
3. *trusted devices* – user can identify an entire interface as trusted i.e. requests for any port numbers from computers on that interface will not be blocked.
4. *other ports* – user can allow access to any other port numbers by adding them as a comma separated list in this box. User can identify the protocol along with the port number.

CONFIGURING AN IPTABLE FIREWALL

TURNING ON IPTABLES

The iptable firewall feature is the default firewall software .iptables are complex,powerful, flexible.

The following procedure describes how to get iptables going on user Fedora system.

1. set the iptables script to start automatically at boot time:
   #chkconfig iptables on
2. before user can start iptables user must have a working set of rules that has been placed in user */etc/sysconfig/iptables file.*
3. if user is doing NAT or IP masquerading, turn on ip packet forwarding. This is allowed by opening /etc/sysct1.conf file as a root user and change the line as:
   net.ipv4.ip_forward=1
4. restart the network interfaces to have IP packet forwarding take effect.
   #/etc/init.d/network restart
5. once the rules file is in place,start up iptables:
   # /etc/init.d /iptables start
6. at this point ,iptables is installed as firewall.user can check to see that the modules used by iptables are loaded by using the ‘ lsmod’ command,as follows:
   # lsmod |grep ip
7. if user want to allow passive FTP or IRC connections on LAN, user may need to load those modules by adding the to /etc/modrobe.conf file.

If the iptable service didn’t start ,make sure that:

The /etc/sysconfig/iptables file exists.

Creating iptables firewall rules

One way to configure iptables is to start by adding and deleting rules to user kernel from the command line. Then when user get a set of rules that are currently running on the system. The tools use to create firewalls rules and then make them permanent are as follows:

- *iptables* – Use this command to append (-A),delete(-D),replace(-R) or insert (-I) a rule . use the –L option to all current rules.

- *Service iptables save* – use this command to save the rules from the kernel and install them in the configuration file.
- /*etc/sysconfig/iptables -config* – this is the configuration files that contains the rules that were saved from the service iptables save command.
- */etc/init.d/iptables* – This is the ip tables start-up script that must run automatically each time Fedora reboots . When it starts ,it clears all iptables rules and counters and installs the new rules from the /etc/sysconfig/iptables file .

FIREWALL FOR SHARED INTERNET CONNECTION(PLUS SERVERS)

This is to show how a small-office LAN with a Fedora system acting as an iptables firewall betweenthe LAN and the INTERNET.the firewall computer also acts as a web server,FTP server, and DNS server.

If user want to use the sample firewall script that follows, user must change the following information to match his configuration:

Firewall computer-the firewall computer is set up as follows:

- *local host* – 127.0.0.1(IP address) and lo(interface). User shouldn't need to change these.
- *Connection to the internet* – 123.45.67.89(IP address) and eth0(interface).replace the with the static IP address and the interface name associated with user connection to the internet.
- *Connection to the LAN* – 10.0.0.1(IP address) and eth1(interface). Replace 10.0.0.1 and eth1 with the static IP address and the interface name associated with user connection to user LAN.
- *Computers on the LAN* – Each computer on the LAN has an IP address from 10.0.0.2 to 10.0.0.254 .change 10.0.0.255 to a number that matches user LAN's range of addresses.

Commands used :

1. policies – the iptables –P commands set as the default policies for INPUT,OUTPUT,AND FORWARD chains.by assigning each of those policies to DROP ,any packet that isn't matched is discarded.
2. user –defined chain – A user defined chain is created to do a few more checks on packets requesting certain TCP services.
3. INPUT chain rules – the bulk of the packet filtering is done in the INPUT chain. The first set of input rules indicates to iptables when to always accept packets from the INTERNET and from the LAN.
    - *Packets from LAN* – because user want the users on his LAN and the firewall computer itself to be able to use the Internet, this set of rules lets through packets that are initiated fro those computers. The first line tells iptables to accept packets for all protocols for which the source is an acceptable address on user's LAN. The next three lines allow packets that come from all valid IP addresses on the firewall computer itself. The last line accepts broadcast packets on the LAN.
    - *Packets from internet(already connected)* – it accepts packets that are both associated with connections that are already established and are requested directly to the firewall's IP address
    - *TCP rules* – in these lines user opens ports for FTP service ,secure shell service, web service and IDENTD authentication, the last of which might be necessary for protocols such as IRC.
    - *UDP rules* – these lines define the ports where connection packets are accepted from the internet for UDP services.
    - ICMP rules – ICMP messages are really more for reporting conditions of the server than for actually providing services.
4. *FORWARD chain rules* – because this firewall is also acting as a router, FORWARD rules are needed to limit what the firewall will and will not pass between the two networks. The first line forwards

everything from the LAN .the second line forwards anything from the internet that is associated with an established connection.

5. *OUTPUT chain rules* – These rules basically exist to prevent anyone from user local computer from *spoofing* IP address .according to these rules, each packet output from the firewall must have as its source address one of the addresses from the firewall computer'sinterfaces.
6. *POSTROUTING chain rules* – the postrouting chain defines rules for packets that have been accepted ,but need additional processing.this is where the actual network –address translation work takes place.

UNDERSTANDING IPTABLES

The IP table feature works by having IP packets that enter or leave the firewall computer, traverse a set of chains that define what is done with the packet.each rule user add essentially does both of the following:

- Checks whether a particular criterion is met.
- Takes an action such as dropping ,accepting ,or further processing a packet.

Enhancing iptables firewall

User can modify or expand on the iptables .iptable is tremendously flexible.
When user actually create his own iptables firewall,user should refer to the iptablesman page(type man iptables) for detailed descriptions of options,ways of matching,ways of entering addresses and other details.
For using iptables :

- *Reduce rules* - try to improve performance by reducing the number of rules.
- *Opposite* – to make a rule its opposite,use an exclamation mark (!)
- *All interfaces* – to match all interfaces of a type, use an plus sign (+),as in eth+.
- *Dos attacks* – user can - -limit option to reduce the impact of DOS attacks, but it still won't stop them together.as long as the traffic is directed at user server,user

network bandwidth is being leeched away,and the machine still utilizes resources to ignore the data.

CHECKING LOG FILES

User must recognize a cracker attack when it is occurring, understanding the various log files in which Fedora record important events is critical to this goal.the log files can be found in the /var/log directory.

SECURING LINUX FEATURES

Understanding attack techniques –

Attacks on computer systems take on different forms,depending on the goal and resources of the attacker,some attacker want to be disruptive, while others want to infiltrate user machines and utilize the resources for their own nefarious purposes. Here are three major categories of attacks :

- *Denial of service(DOS)* – The easiest attacks to perpetrate are denial of service attacks. The primary purpose of these attacks is to disrupt the activities of a remote site by overloading it with irrelevant data. DOS attacks can be as simple as sending thousand of page requests per second at a website. These type of attack are easy perpetrate and easy to protect against . once user handle on where the attack is coming from, a simple phone call to the perpetrator's ISP will get the problem solved.
- *Distribution denial of service (DDOS)* – more advanced DOS attacks are called Distribution denial of service attacks. DDOS attacks are nearly impossible to stop. In this form of attack, an attacker takes control of hundreds or even thousands of weakly secured Internet connected computers. The attacker then directs them in unison to send a stream of irrelevant data to a single Internet host . the result is that the power of one attacker is magnified thousand of times. The best defense

against a DDOS attack is to contact ISP to see if it can filter traffic at its border routers.

- *Intrusion attacks* – to remotely use the resources of a target machine ,attackers must first look for an opening exploit. In absence of inside inforation such as passwords,they must scan the target machine to see what services are offered. Perhaps one of the services is weakly secured and the attacker can use some known exploit to finagle his or her way in.

  A tool called nmap is generally considered the best way to scan a host for services.once the attacker has a list of the available services running on his target,he needs to find a way to trick one of those services into letting him have privileged access to the system.usually this is done with a program called exploit.

PROTECTING AGAINST DENIAL OF SERVICE ATTACKS

Some common attacks and their defenses are:

1. *Mail Bombing* – mail bombing is the practice of sending so much e-mail to a particular user or system that the computer's hard drive becomes full. There are several ways to protect from mail bombing.

Blocking mail with Procmail

The procmail e-mail filtering tool is installed by default with Fedora and is tightly integrated with the sendmail e-mail daemon,thus it can be used to selectively block or filter out specific types of e-mail.

Blocking mail with send mail

The procmail tool works quite well when only user is being mailbombed. If.,however ,the mailbombing affects many user , user should probably configure his sendmail daemon to block all e-mail from the mail bomber .

2. *Spam relaying*

Spam refers to the unsolicited junk e-mail that has become a common occurrence on the internet. Through this user cant see the unwanted e-mail.spammers often deliever their annoying messages from a normal dial-up internet account. They need some kind of high capacity e-mail to accept and buffer the payload of messages. They deliver the spam to the server all in one huge batch and then log off, letting the server do the work of delivering the messages to the victims. Having user mailserver highjacked to act as a spam relay can have a devastating effect on user system. Fortunately , open mail relaying is deactivated by default on fedora.

PROTECTING AGAINST INTRUSION ATTACKS

Crackers have a wide variety of tools and techniques to assist them in breaking into user computer. Intrusion attacks focus on exploiting weakness in user security , so the crackers can take more control of user system than they could from the outside.

There are many tools and techniques for combating intrusion attacks.