RPM

RPM Package Manager is a package management system. The name RPM refers to two things: a software package file format, and software packaged in this format. RPM was intended primarily for GNU/Linux distributions; the file format *RPM* is the baseline package format of the Linux Standard Base.

This section contains an overview of principal modes using with RPM for installing, uninstalling, upgrading, querying, listing, and checking RPM packages on your Linux system. You must be familiar with these RPM commands now because we'll use them often in the continuation of this book.

To install a RPM package, use the command:

```
[root@deep] /#rpm -ivh telnet-1.0-2.i386.rpm
```

Take a note that RPM packages have a file of names like telnet-1.0-2.i386.rpm, which include the package name (telnet), version (1.0), release (2), and architecture (i386).

To uninstall a RPM package, use the command:

```
[root@deep] /#rpm -e telnet
```

Notice that we used the package name telnet, not the name of the original package file telnet-1.0-2.i386.rpm.

To upgrade a RPM package, use the command:

```
[root@deep] /#rpm -Uvh telnet-1.0-2.i386.rpm
```

With this command, RPM automatically uninstall the old version of telnet package and install the new one. Always use **rpm -Uvh** to install packages, since it works fine even when there are no previous versions of the package installed.

To query a RPM package, use the command:

```
[root@deep] /#rpm -q telnet
```

This command will print the package name, version, and release number of installed package telnet. Use this command to verify that a package is or is not installed on your system.

To display package information, use the command:

```
[root@deep] /#rpm -qi telnet
```

This command display package information; includes name, version, and description of the installed program. Use this command to get information about the installed package.

To list files in package, use the command:

```
[root@deep] /#rpm –ql telnet
```

This command will list all files in a installed RPM package. It works only when the package is already installed on your system.

To check a RPM signature package, use the command:

```
[root@deep] /#rpm  --checksig telnet
```

This command checks the PGP signature of specified package to ensure its integrity and origin. Always use this command first before installing new RPM package on your system. Also, GnuPG or Pgp software must be already installed on your system before you can use this command.

How to untar a tar file or gzip-bz2 tar file

Tar file can come compressed or uncompressed. Generally that are compressed using gzip or bzip2. The program, tar, will uncompress both types and extract the files from archive.

tar (file format)

In computing, **tar** (derived from *tape archive* and commonly referred to as "tarball") is both a file format (in the form of a type of archive bitstream) and the name of a program used to handle such files. The format was created in the early days of Unix and standardized by *POSIX.1-1988* and later *POSIX.1-2001*.

Initially developed to be written directly to sequential I/O devices for tape backup purposes, it is now commonly used to collect many files into one larger file for distribution or archiving, while preserving file system information such as user and group permissions, dates, and directory structures.

tar   cvf mybackup.tar Desktop

C The letter c means "create archive".

V he letter v means "verbose", which tells tar to print all the filenames as they are added to the archive.

F The letter f tells tar that the name of the archive appears next (right after these options).

v flag is completely optional, but I usually use it so I can see the progress of the command.

The general tar syntax of the tar command when creating an archive looks like this:

tar [flags] archive-file-name files-to-archive

Creating a compressed archive

You *can* compressed a tar archive with the gzip command after you create it, like this:

gzip Mybackup.tar

This creates the file Mybackup.tar.gz. But these days it's more common to create a compressed tar archive with one command, like this:

```
tar czvf Mybackup.tgz Desktop
```

As you can see**, I added the** z **flag there** (which means "compress this archive with gzip"), and I changed the extension of the archive to .tgz, which is the common file extension for files that have been tar'd and gzip'd in one step.

Creating a compressed archive of the current directory

Many times you will want to **create an archive** of all files in the current directory, including all subdirectories. You can easily create this archive like this:

```
tar czvf mydirectory.tgz
```

where the . refers to the current directory.

Writing an archive in a different directory

You may also want to write an archive like that previous example to a different directory, like this:

```
tar czvf /tmp/mydirectory.tgz .
```

Listing the contents of a tar archive

To *list* the contents of an *uncompressed* tar archive, just replace the c flag with the t flag, like this:

```
tar tvf my-archive.tar
```

This lists all the files in the archive, but does not extract them.

To list all the files in a *compressed* archive, add the z **flag** like before:

```
tar tzvf my-archive.tgz
```

That same command can also work on a file that was tar'd and gzip'd in two separate steps (as indicated by the .tar.gz file extension):

```
tar tzvf my-archive.tar.gz
```

I almost always list the contents of an unknown archive before I extract the contents. I think this is always good practice, especially when you're logged in as the root user.

GZIP:

gzip is a software application used for file compression. gzip is short for **GNU zip**; as the program was created a free software replacement for the compress program used in early Unix systems, intended for use by the GNU Project.

gzip was created by Jean-Loup Gailly and Mark Adler. Version 0.1 was first publicly released on October 31, 1992. Version 1.0 followed in February 1993.

OpenBSD's version of gzip is actually the compress program, to which support for the gzip format was added in OpenBSD 3.4 - the 'g' in this specific version stands for gratis.

FreeBSD and NetBSD use BSD-licensed implementation instead of the GNU version.

```
gzip mybackup.tar                  //to gzip mybackup.tar file

mybackup.tar.gz                    //after gzip command
```

The Linux Boot Sequence

You might remember when you installed Linux that the installation process prompted you for a list of partitions and the sizes of each in which your file systems would be placed.

When allocating disk space for the partitions, the first sector, or data unit, for each partition is always reserved for programmable code used in booting. The very first sector of the hard disk is reserved for the same purpose and is called the master boot record (MBR).

When booting from a hard disk, the PC system BIOS loads and executes the boot loader code in the MBR. The MBR then needs to know which partitions on the disk have boot loader code specific to their operating systems in their boot sectors and then attempts to boot one of them.

When Linux begins to boot with its kernel, it first runs the **/sbin/init** program, which does some system checks, such as verifying the integrity of the file systems, and starts vital programs needed for the operating system to function properly. It then inspects the **/etc/inittab** file to determine Linux's overall mode of operation or runlevel.

Linux Runlevels

Mode	Directory	Run Level Description
0	/etc/rc.d/rc0.d	Halt
1	/etc/rc.d/rc1.d	Single-user mode
2	/etc/rc.d/rc2.d	Not used (user-definable)
3	/etc/rc.d/rc3.d	Full multi-user mode (no GUI interface)
4	/etc/rc.d/rc4.d	Not used (user-definable)
5	/etc/rc.d/rc5.d	Full multiuser mode (with GUI interface)
6	/etc/rc.d/rc6.d	Reboot

Based on the selected runlevel, the init process then executes startup scripts located in subdirectories of the /etc/rc.d directory. Scripts used for runlevels 0 to 6 are located in subdirectories /etc/rc.d/rc0.d through /etc/rc.d/rc6.d, respectively.

Determining the Default Boot runlevel

The default boot runlevel is set in the file /etc/inittab with the initdefault variable. When set to 3, the system boots up with the text interface on the VGA console; when set to 5, you get the GUI. Here is a snippet of the file (delete the initdefault line you don't need):

```
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:                   # Console Text Mode
id:5:initdefault:                   # Console GUI Mode
```

Note the following:

- Most home users boot up with a Windows like GUI (runlevel 5)
- Most techies will tend to boot up with a plain text-based command-line-type interface (runlevel 3)
- Changing initdefault from 3 to 5, or vice-versa, has an effect upon your next reboot. See the following section on how to get a GUI login all the time until the next reboot.
- Of course, don't set the initdefault value to 6 or your system will constantly reboot. Setting it to 0 will never allow it to start!

```
[root@mysrv tmp]# startx
```

Automatic Method: You can have Linux automatically start the X terminal GUI console for every login attempt until your next reboot by using the init command. You will need to edit your initdefault variable in your /etc/inittab file, as mentioned in the preceding section to keep this functionality even after you reboot.

```
[root@mysrv tmp]# init 5
```

When the CPU capacity or available memory on your server is low or you want to maximize all system resources, you might want to operate in text mode runlevel 3 most of the time, using the GUI only as necessary with the startx command.

Servers that double as personal workstations, or servers that might have to be operated for an extended period of time by relatively nontechnical staff, may need to be run at runlevel 5 all the time through the init 5 command. Remember you can make runlevel 5 permanent even after a reboot by editing the /etc/inittab file.

Using Virtual Consoles

By default, **Linux runs six virtual console or TTY sessions running on the VGA console**. This makes the GUI run as number 7:

- You can step through each virtual console session by using the Ctl-Alt-F1 through F6 key sequence. You'll get a new login prompt for each attempt.
- You can get the GUI login with the sequence Ctl-Alt-F7 only in run level 5, or if the GUI is running after launching **startx.**

Root Password Recovery

Sometimes you might forget the root password, or the previous systems administrator may move on to a new job without giving it to you. To do this, follow these steps:

1. Go to the VGA console and press Ctrl-Alt-Del. The system will then shut down in an orderly fashion.
2. Reboot the system and enter single-user mode.
3. Once at the command prompt, change your password. Single user mode assumes the person at the console is the systems administrator root, so you don't have to specify a root username.

Switch on vsftpd Starting Up in Levels 3 and 5

The chkconfig command with the --level switch indicates that some action needs to be done at the runlevels entered as its values. The first argument in the command is the package you want to affect and the second defines whether you want it on or off. In this case we want vsftpd not to be started when entering runlevels 3 and 5:

```
[root@mysrv tmp]# chkconfig --level 35 vsftpd on
```

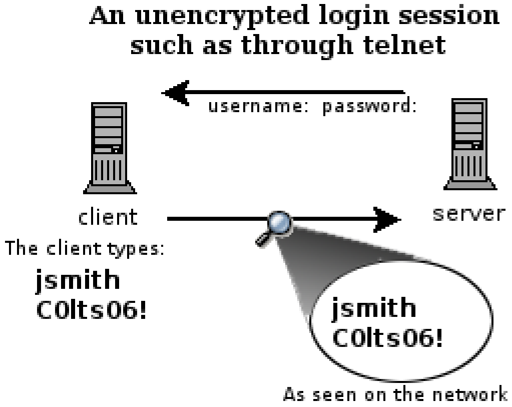
By not specifying the runlevels with the --level switch, chckconfig will make the changes for runlevels 3 and 5 automatically:

Telnet (Port 23)

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Controlling xinetd-Managed Applications

Xinetd-managed applications all store their configuration files in the **/etc/xinetd.d** directory. Each configuration file has a disable statement that you can set to yes or no. This governs whether xinetd is allowed to start them or not.



Telnet is a program that allows users to log into your server and get a command prompt just as if they were logged into the VGA console. The Telnet server RPM is installed and disabled by default on Fedora Linux.

One of the **disadvantages of Telnet is that the data is sent as clear text**. This means that it is possible for someone to use a network analyzer to peek into your data packets and see your username and password. A more secure method for remote logins would be via Secure Shell (SSH) which uses varying degrees of encryption.

In spite of this, the older Telnet application remains popular. Many network devices don't have SSH clients, making telnet the only means of accessing other devices and servers from them. I'll show you how to limit your exposure to Telnet's insecurities are mentioned later in this chapter.

1) vi /etc/xinetd.d/telnet

# Description: The telnet server serves telnet sessions; it uses
# unencrypted username/password pairs for authentication.

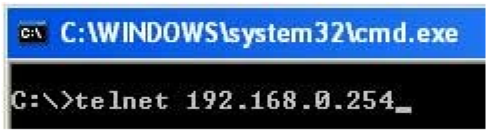
You can restrict telnet logins access to individual remote servers by using the **only_from** keyword in the telnet configuration file. add a list of trusted servers to the /etc/xinetd.d/telnet file separated by spaces:

```
service telnet

{

        disable         = no                                    //change yes to no for activate telnet
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        only_from       = 172.16.1.1 127.0.0.1 172.16.1.2       //only access telnet from given IP's
}
```

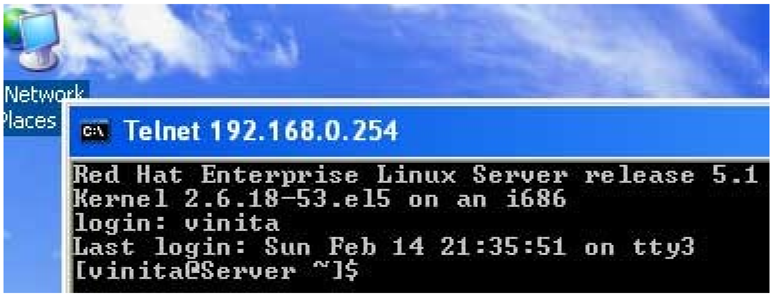
2) Restart telnet.

```
[root@mysrv tmp]# chkconfig telnet on
[root@mysrv tmp]# service xinetd start
```

3) Test the telnet session. Servers that are not on the trusted list get the message Connection closed by foreign host.



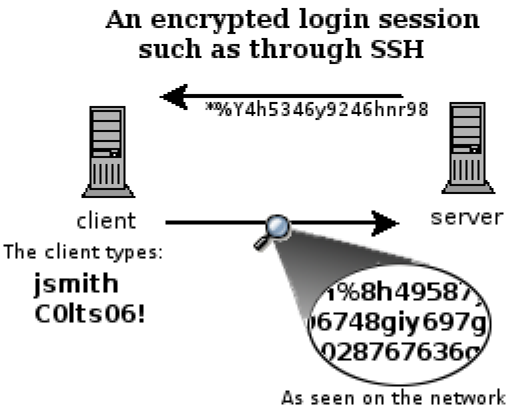
```
C:\>telnet 192.168.0.254_
```



```
Red Hat Enterprise Linux Server release 5.1
Kernel 2.6.18-53.el5 on an i686
login: vinita
Last login: Sun Feb 14 21:35:51 on tty3
[vinita@Server ~]$
```

SSH: (Port 22)

There are a couple of ways that you can access a shell (command line) remotely on most Linux/Unix systems. One of the older ways is to use the telnet program, which is available on most network capable operating systems. Accessing a shell account through the telnet method though poses a danger in that everything that you send or receive over that telnet session is visible in plain text on your local network, and the local network of the machine you are connecting to. So anyone who can "sniff" the connection inbetween can see your username, password, email that you read, and commands that you run. For these reasons you need a more sophisticated program than telnet to connect to a remote host.



An unencrypted telnet session

SSH, which is an acronym for Secure SHell, was designed and created to provide the best security when accessing another computer remotely. Not only does it encrypt the session, it also provides better authentication facilities, as well as features like secure file transfer, X session forwarding, port forwarding and more so that you can increase the security of other protocols.

Install/Configure SSH in Linux

Secure shell server also use to remotely access of server through client, it provide security than telnet and it’s port in 22 on which it is work.

Now we will see how to configure it

Step 1

First of all we will check it is installed or not

```
[root@mysrv ~]#   rpm -qa openssh
openssh-3.9p1-8.RHEL4.12
```

Step 2

By default root is not permitted to login at ssh, so to give it permission we will edit the file

```
[root@mysrv ~]#   vi /etc/ssh/sshd_config
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
```

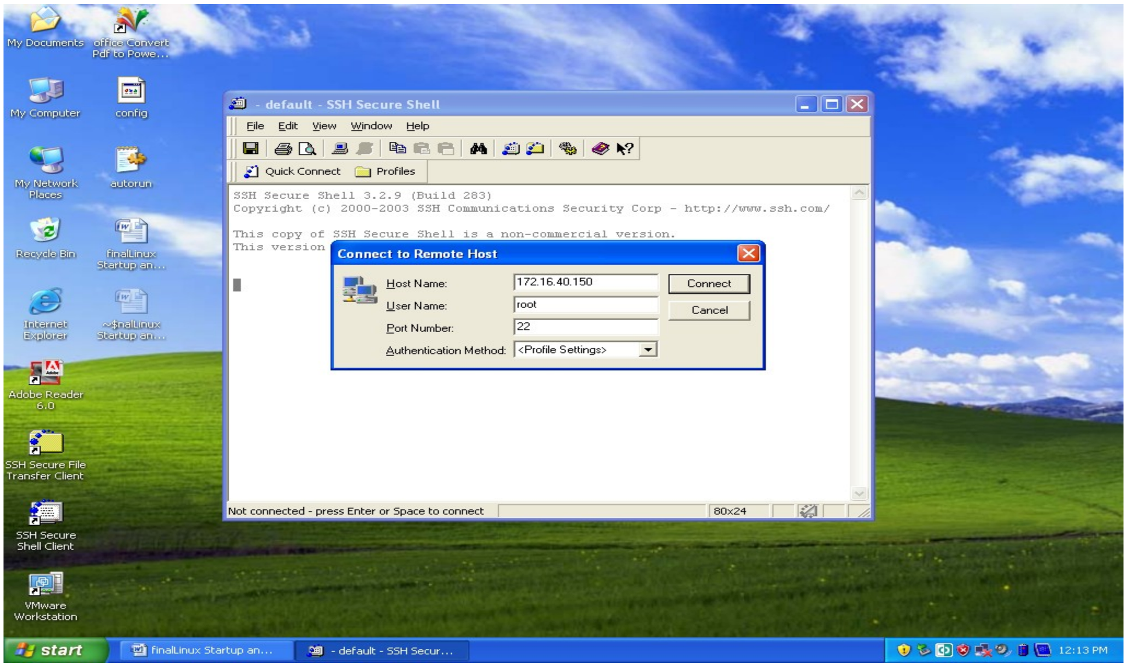
Step 3

Now we are able to start the service of sshd

```
[root@mysrv ~]#   service sshd start
Starting sshd:                                    [  OK  ]
```

Step 4

Now we will go to client and use third party software just like putty or SSH secure shell, for remotely access to the server and write the ip address of the server machine and user name .



```
SSH Secure Shell 3.2.9 (Build 283)
Copyright (c) 2000-2003 SSH Communications Security Corp - http://www.ssh.com/

This copy of SSH Secure Shell is a non-commercial version.
This version
```

Connect to Remote Host

Host Name: 172.16.40.150

User Name: root

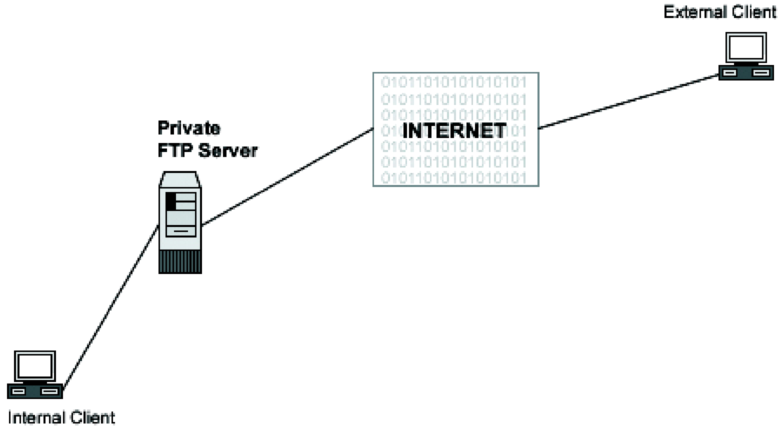
Port Number: 22

Authentication Method: <Profile Settings>

Not connected - press Enter or Space to connect   80x24

FTP CONFIGURATION

File transfer protocol work on the port of 20 and 21, this is a server through which we transfer the files, users can access the data which is placed inside the public directory without authentication, but if we edit a file of vsftpd.conf we can allow authentication, we well see both way to access the file to give permission and without permissions.



Directory that can be access any user if anonymous_enable=yes option is select and you can upload your data in /var/ftp/pub directory.

```
[root@mysrv ~]#   cd /var/ftp/pub/
```

Step 1

We will check that it is installed or not by using command

```
[root@mysrv ~]#   rpm -qa vsftpd

vsftpd-2.0.1-5.EL4.3
```

Step 2

Know we on the service of the telnet with the help of these commands

```
[root@mysrv ~]#   /etc/init.d/vsftpd start

Starting vsftpd:                          [  OK  ]
```

Or

```
[root@mysrv ~]#   service vsftpd start

Starting vsftpd:
```

Step 3

In this step we will be editing in the file of vsftpd.conf there will be option of anonymous_enable=yes this mean that we can access the file without authentication when we turn it no, than it will ask user name and password to access the file, and restart the service of vsftpd

```
[root@mysrv ~]#   vi /etc/vsftpd/vsftpd.conf

# Allow anonymous FTP? (Beware - allowed by default if you comment this out).

anonymous_enable=no

:wq!

[root@mysrv ~]#  /etc/init.d/vsftpd restart
```

Step 4

Also we can restrict the users that can not access the file, we just uncomment the user and userlist_deny=Yes to which we do not want to give access the file

```
[root@mysrv ~]#   vi /etc/vsftpd.user_list

# vsftpd userlist

# If userlist_deny=NO, only allow users in this file

# If userlist_deny=YES (default), never allow users in this file, and

# do not even prompt for a password.

# Note that the default vsftpd pam config also checks /etc/vsftpd.ftpusers

# for users that are denied.

#root
#amir
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

Step 5

This is another way to restrict the users to access the file, just comment the user to which you want to allow.

```
[root@mysrv ~]#   vi /etc/vsftpd
```

```
vsftpd/         vsftpd.ftpusers   vsftpd.user_list

[root@mysrv ~]#   vi /etc/vsftpd.ftpusers

# Users that are not allowed to login via ftp

#root
#amir
bin
daemon
adm
shutdown
halt
news
games
nobody
```

Step 6

we simply write in the browser address of internet on the client system and access the file

```
Fttp:\\172.16.40.150                              //access ftp from browser
```

Apache: (Port 80)

Apache is probably the most popular Linux-based Web server application in use. Once you have DNS correctly setup and your server has access to the Internet, you'll need to configure Apache to accept surfers wanting to access your Web site.

Download and Install The Apache Package

Most RedHat and Fedora Linux software products are available in the RPM format. When searching for the file, remember that the Apache RPM's filename usually starts with the word httpd followed by a version number, as in httpd-2.0.48-1.2.rpm. It is best to use the latest version of Apache.

Use the chkconfig command to configure Apache to start at boot:

```
[root@mysrv tmp]# chkconfig httpd on
[root@u-mysrv tmp]# /etc/init.d/apache start
```

You can test whether the Apache is running

```
[root@u-mysrv tmp]# http://192.168.1.100
```

General Configuration Steps

The configuration file used by Apache is /etc/httpd/conf/httpd.conf in Redhat / Fedora distributions and /etc/apache*/httpd.conf in Debian / Ubuntu distributions. As for most Linux applications, you must restart Apache before changes to this configuration file take effect.

Package used to configure the apache server is "httpd"

Cchanges are made in httpd.conf

```
[root@u-mysrv tmp]#     vi /etc/httpd/httpd.conf

                    Server name          172.16.1.250:80
                    Time out               120 second
                    Document  root         /var/www/html
                    Maximum client             150
                    Server admin             amir@yahoo.com
                    Directory  index          index.html
                    :wq!

   [root@u-mysrv tmp]#      /etc/init.d/httpd   restart
```

Where To Put Your Web Pages

All the statements that define the features of each web site are grouped together inside their own <VirtualHost> section, or container, in the httpd.conf file. The most commonly used statements, or directives, inside a <VirtualHost> container are:

- **servername**: Defines the name of the website managed by the <VirtualHost> container. This is needed in named virtual hosting only.
- **DocumentRoot**: Defines the directory in which the web pages for the site can be found.

By default, Apache searches the DocumentRoot directory for an index, or home, page named index.html. So for example, if you have a servername of www.my-site.com with a DocumentRoot directory of /home/www/site1/, Apache displays the contents of the file /home/www/site1/index.html when you enter http://www.my-site.com in your browser.

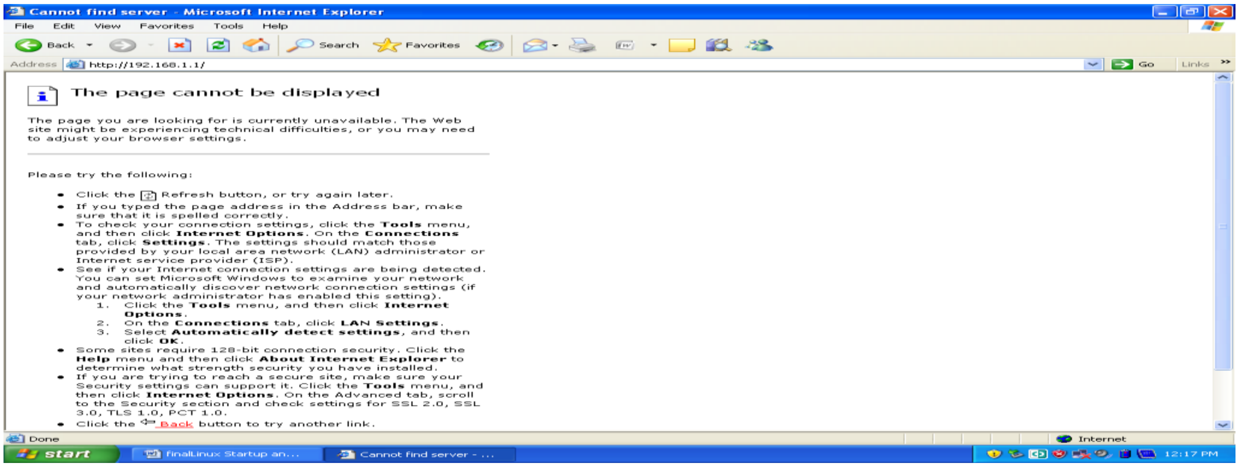
Configuration - Multiple Sites and IP Addresses

These statements would normally be found at the very bottom of the file where the virtual hosting statements reside. The last section of this configuration snippet has some additional statements to ensure read-only access to your Web pages with the exception of Web-based forms using POSTs (pages with "submit" buttons). Remember to restart Apache every time you update the httpd.conf file for the changes to take effect on the running process.

Step 1: Configure Virtual Hosting

Here is an example:

```
<VirtualHost 192.168.1.1:80 >
   ServerAdmin info@uoe.edu.pk
  DocumentRoot /var/www/mysite
   Directoryindex index.html
   ServerName 192.168.1.1
```



http://192.168.1.1/

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

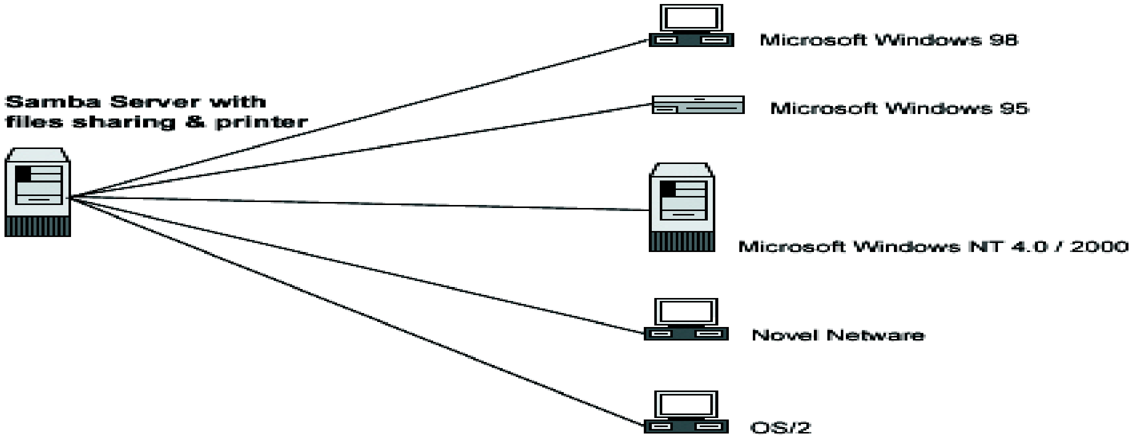
Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the Back button to try another link.

Samba Server (Port 137 138)

Samba is a suite of utilities that allows your Linux box to share files and other resources, such as printers, with Windows boxes. This chapter describes how you can make your Linux box into a Windows Primary Domain Controller (PDC) or a server for a Windows Workgroup. Either configuration will allow everyone at home to have:

- their own logins on all the home windows boxes while having their files on the Linux box appear to be located on a new Windows drive
- shared access to printers on the Linux box
- shared files accessible only to members of their Linux user group.



What's the difference between a PDC and Windows Workgroup member? A detailed description is beyond the scope of this chapter, but this simple explanation should be enough:

- A PDC stores the login information in a central database on its hard drive. This allows each user to have a universal username and password when logging in from all PCs on the network.
- In a Windows Workgroup, each PC stores the usernames and passwords locally so that they are unique for each PC.

By default, Samba mimics a Windows PDC in almost every way needed for simple file sharing. Linux functionality doesn't disappear when you do this. Samba Domains and Linux share the same usernames so you can log into the Samba based Windows domain using your Linux password and immediately gain access to files in your Linux user's home directory. For added security you can make your Samba and Linux passwords different.

When it starts up, and with every client request, the Samba daemon reads the configuration file /etc/samba/smb.conf to determine its various modes of operation. You can create your own smb.conf using a text editor

Download and Install Packages

Most RedHat and Fedora Linux software products are available in the RPM format. Downloading and installing RPMs isn't hard. If you need a refresher.

Samba is comprised of a suite of RPMs that come on the Fedora CDs. The files are named:

- samba
- samba-common
- samba-client

When searching for the file, remember that the RPM's filename usually starts with the RPM name followed by a version number as in samba-client-3.0.0-15.i386.

How to Get Samba Started

- You can configure Samba to start at boot time using the chkconfig command:

```
[root@mysrv tmp]# chkconfig smb on
[root@mysrv tmp]# service smb start
```

Note: Unlike many Linux packages, Samba does not need to be restarted after changes have been made to its configuration file, as it is read after the receipt of every client request.

- You can test whether the smb process is running with the pgrep command, you should get a response of plain old process ID numbers:

```
[root@mysrv tmp]# pgrep smb
```

The Samba Configuration File

The /etc/samba/smb.conf file is the main configuration file you'll need to edit. It is split into five major sections:

File Format - smb.conf

Section	Description
[global]	General Samba configuration parameters
[printers]	Used for configuring printersUsed for configuring printers
[homes]	Defines treatment of user logins

[netlogon]	A share for storing logon scripts. (Not created by default.)
[profile]	A share for storing domain logon information such as "favorites" and desktop icons. (Not created by default.)

The [Global] Section

The [global] section governs the general Samba settings. parameters you need to set in order to create a PDC.

smb.conf Minimum Settings, "Global" Section

Parameter	**value**	**Description**
domain logons	Yes	Tells Samba to become the PDC
preferred master	Yes	Makes the PDC act as the central store for the names of all windows clients, servers and printers on the network. Very helpful when you need to "browse" your local network for resources. Also known as a local master browser.
domain master	Yes	Tells Samba to become the master browser across multiple networks all over the domain. The local master browsers register themselves with the domain master to learn about resources on other networks.
os level	65	Sets the priority the Samba server should use when negotiating to become the PDC with other Windows servers. A value of 65 will usually make the Samba server win.
Local master	Yes	The local master browsers register themselves with the domain master to learn about resources on other networks.

time server	Yes	Lets the samba server provide time updates for the domain's clients.
workgroup	"MYDOMAIN"	The name of the Windows domain we'll create. The name you select is your choice. I've decided to use "MYDOMAIN".
security	user	Make domain logins query the Samba password database located on the samba server itself.
smb passwd file	/etc/samba/smbpasswd	It is useful to specify the name and location of the Samba password file. This helps to make Samba version upgrades where the default locations may change.
private dir	/etc/samba	Specifies default directory for some supporting temporary files. As with the password file, it is a good practice to specify this value.

```
[global]

    workgroup = MYDOMAIN
    time server = Yes
    domain logons = Yes
    os level = 65
    preferred master = Yes
    domain master = Yes
    local master = Yes
    smb passwd file = /etc/samba/smbpasswd
    private dir = /etc/samba
```

Note: security = user and WINS support = yes are default settings for Samba and they may not show up in your smb.conf file.

The [homes] Section

Part of the process of adding a user to a Samba domain requires you to create a Linux user on the Samba PDC itself. When you log into the Samba PDC, you'll see a new drive, usually named Z:, added to your PC. This is actually a virtual drive that maps to the corresponding Linux users' login directories on the Linux PDC.

Samba considers all directories to be shares that can be configured with varying degrees of security. The [homes] section governs how Samba handles default login directories.

smb.conf Minimum Settings, "Home" Section

Parameter	**Value**	**Description**
browseable	No	Doesn't allow others to browse the contents of the directory
read only	No	Allows the samba user to also write to their Samba Linux directory
create mask	0664	Makes new files created by the user to have "644" permissions. You want to change this to "0600" so that only the login user has access to files.
directory mask	0775	Makes new sub-directories created by the user to have "775" permissions. You want to change this to "0700" so that only the login user has access to directories.

```
[homes]
 read only = No
 browseable = No
 create mask = 0644
 directory mask = 0755
```

The [printers] Share Section

Samba has special shares just for printers, and these are configured in the [printers]. There is also a share under [printers] called printers which governs common printer settings. Print shares always have the printable parameter set to yes. The default smb.conf [printers] share section looks like this:

```
[printers]
   comment = All Printers
   path = /var/spool/samba
   printable = Yes
   browseable = No
```

Make Your PC Clients Aware Of Your Samba PDC

There are many types of Windows installed on people's PCs and each version has its own procedure for joining a domain. The next sections show you how to add the most popular versions of Windows clients to your domain:

Windows 200x and Windows XP Professional

For the 200x and XP Professional varieties of Windows, create a dynamic Samba machine trust account, then go through these steps:

1. Press the Windows and Break keys simultaneously to access the System Properties dialogue box.
2. Click on the 'Network Identification' or 'Computer Name' tab on the top.
3. Click the "Properties" button.
4. Click on the "Member of Domain" button.
5. Also enter your domain name and computer name and then click "OK"
6. You will be prompted for a user account and password with rights to join a machine to the domain. Enter the information for your Samba administrator. In this home environment scenario, the user would be root with the corresponding smbpasswd password. Now, you should get a "Welcome to <DOMAIN>" message confirming that you've been added.
7. Reboot.

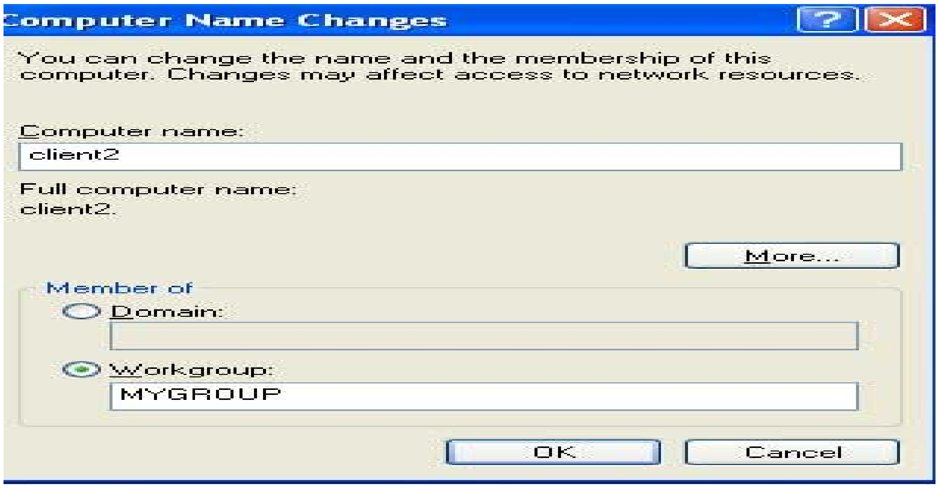
Log in using any account in the /etc/smbpasswd file with your domain as the domain name.

Note: With Samba version 2 you may also have to make a few changes to your system's registry using the regedit command and reboot before continuing.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
"signsecurechannel"=dword:00000000
```

Client configuration for samba server

Go on windows system and ping samba server, change computer name to client2 and workgroup name to MYDOMAIN



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: client2

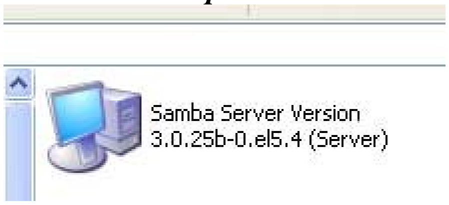
Full computer name: client2.

○ Domain:

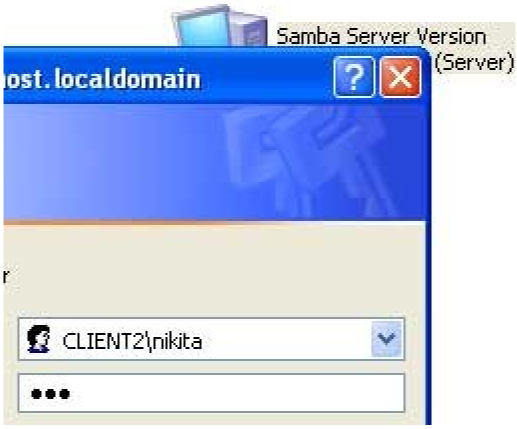
● Workgroup: MYGROUP

reboot system after changing workgroup name

After reboot open my network place here you can see samba server [if not see then click on view workgroup computer in right pane, if still not see then use search button from tool bar and search computer samba server form ip]



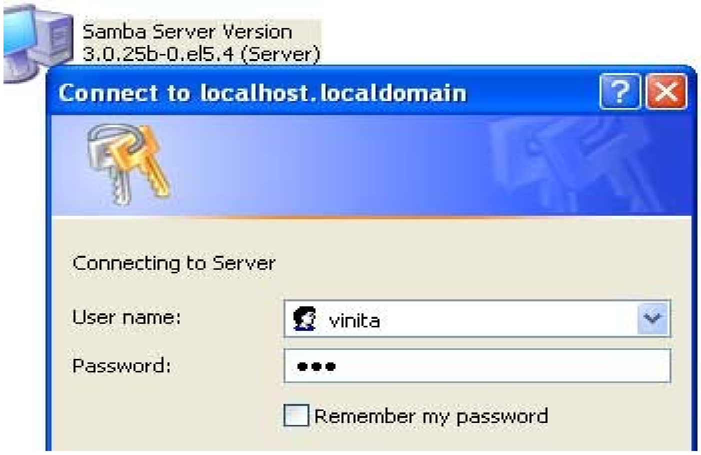
First try to login from user nikita she will not successes as nikita have not permission to login



CLIENT2\nikita

●●●

Now login from user vinita [give the password which you set with smbpasswd command]



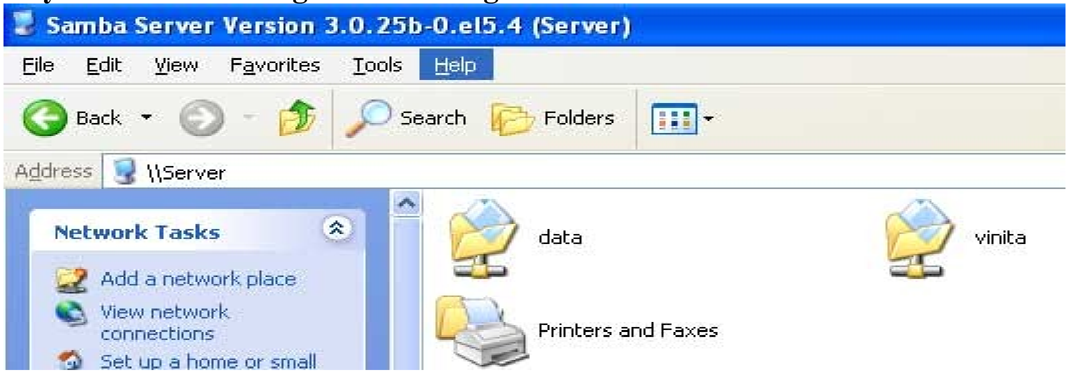
Connecting to Server

User name: vinita

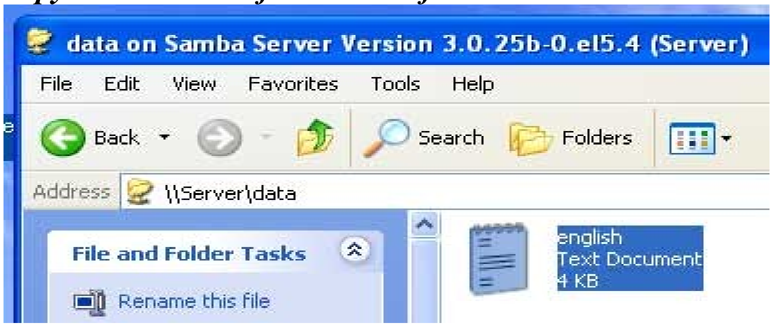
Password: ●●●

□ Remember my password

As you can see in image user vinita gets the /data folder which we share from samba server



Copy some window files in data folder



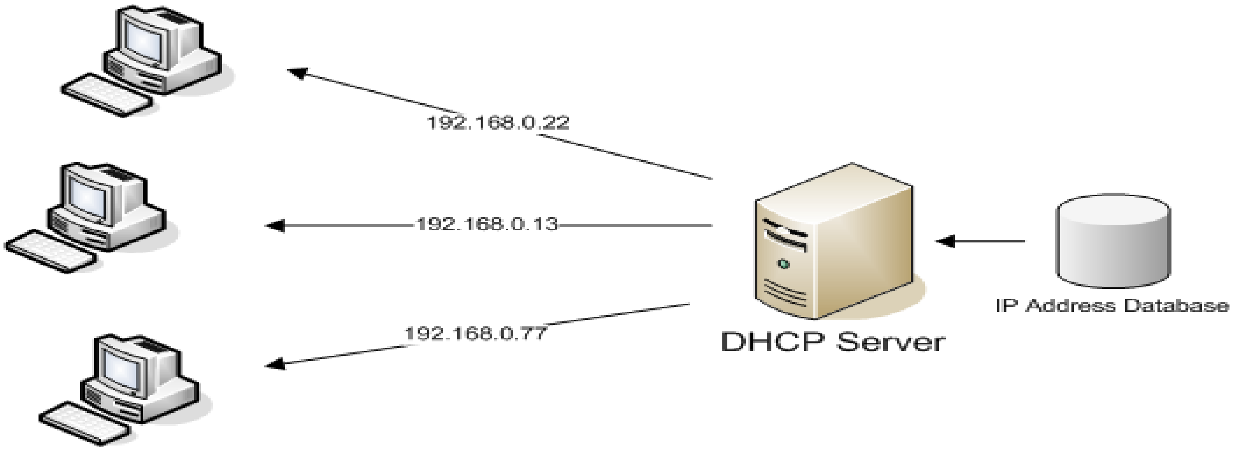
Check status on samba server

on samba server you can check runtime status of samba server to check it run smbstatus command

DHCP (Port 67, 68)

DHCP stands for dynamic host configuration protocol. What it does is dynamically assign network settings from a server. In other words, instead of having to configure the parameters related to how your computer communicates with a network, it happens automatically.

Assigning an IP address dynamically is the most basic piece but there is a lot more to DHCP. This includes the netmask, host name, domain name, gateway and name servers. In addition, DHCP can supply other information such as a Network time server.



Download and Install the DHCP Package

Most RedHat and Fedora Linux software products are available in the RPM format. Downloading and installing RPMs aren't hard. If you need a refresher, Chapter 6, "Installing Linux Software", covers how to do this in detail.

When searching for the file, remember that the DHCP server RPM's filename usually starts with the word dhcp followed by a version number like this: dhcp-3.0.1rc14-1.i386.rpm.

The /etc/dhcpd.conf File

When DHCP starts, it reads the file /etc/dhcpd.conf. It uses the commands here to configure your network. The standard DHCP RPM package doesn't automatically install a /etc/dhcpd.conf file, but you can find a sample copy of dhcpd.conf in the following directory which you can always use as a guide.

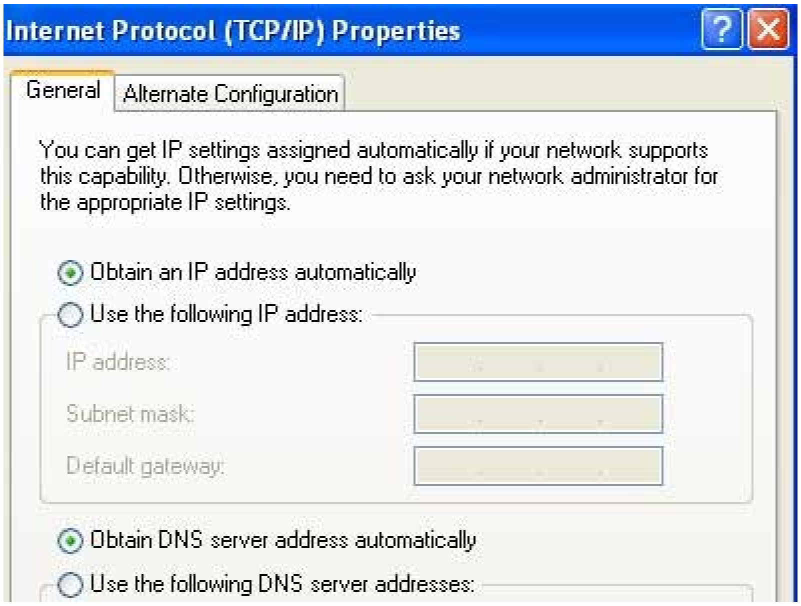
/usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample

You have to copy the sample dhcpd.conf file to the /etc directory and then you'll have to edit it. Here is the command to do the copying for the version 3.0p11 RPM file:

```
[root@mysrv tmp]# cp /usr/share/doc/dhcp-3.0pl1/dhcpd.conf.sample /etc/dhcpd.conf
```

Here is a quick explanation of the dhcpd.conf file: Most importantly, there must be a subnet section for each interface on your Linux box.

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.1 netmask 255.255.255.0 {

# --- default gateway
#       option routers                  192.168.0.254.;
#       option subnet-mask              255.255.255.0;

#       option nis-domain               "domain.org";
#       option domain-name              "domain.org";
        option domain-name-servers  192.168.0.6;

        option time-offset              -18000;         # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers  192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

      range dynamic-bootp 192.168.0.40 192.168.0.250;
      range dynamic-bootp 192.168.5.50 192.168.5.254;

        default-lease-time 691200;
        max-lease-time 5529600;
# we want the nameserver to appear at a fixed address

host net-001 {
                hardware ethernet 00:50:ba:8e:4a:7c;
                fixed-address 192.168.0.10;
        }
host net-002 {
                hardware ethernet 00:50:ba:8e:4f:09;
                fixed-address 192.168.0.15;
        }
}
 [root@mysrv tmp]# service dhcpd restart
```



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

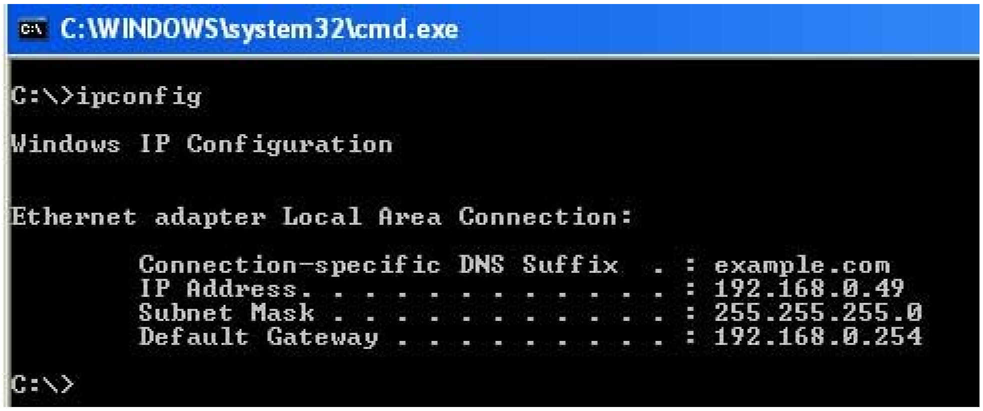
IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : example.com
        IP Address. . . . . . . . . . . . : 192.168.0.49
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.254

C:\>
```

Simple DHCP Troubleshooting

The most common problems with DHCP usually aren't related to the server; after the server is configured correctly there is no need to change any settings and it therefore runs reliably. The problems usually occur at the DHCP client's end for a variety of reasons. The following sections present simple troubleshooting steps that you can go through to ensure that DHCP is working correctly on your network.

DHCP Clients Obtaining 169.254.0.0 Addresses

Whenever Microsoft DHCP clients are unable to contact their DHCP server they default to selecting their own IP address from the 169.254.0.0 network until the DHCP server becomes available again. This is frequently referred to as Automatic Private IP Addressing (APIPA). Here are some steps you can go through to resolve the problem:

- Ensure that your DHCP server is configured correctly and use the pgrep command discussed earlier to make sure the DHCP process is running. Pay special attention to your 255.255.255.255 route, especially if your DHCP server has multiple interfaces.
- Give your DHCP client a static IP address from the same range that the DHCP server is supposed to provide. See whether you can ping the DHCP server. If you cannot, double-check your cabling and your NIC cards.
- DHCP uses the BOOTP protocol for its communication between the client and server. Make sure there are no firewalls blocking this traffic. DHCP servers expect requests on UDP port 67 and the DHCP clients expect responses on UDP port 68. Use tcpdump on the server's NIC to verify the correct traffic flows.

This step is important, because the IP address of a Web site's server, not the Web site's name, is used in routing traffic over the Internet.

DNS (Port 53)

Domain **N**ame **S**ystem (or **S**ervice or **S**erver), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Fully Qualified Domain Name

A *fully qualified domain name* consists of a host and domain name, including top-level domain. For example, www.abc.com.com is a fully qualified domain name. **www** is the host, abc.com is the second-level domain, and.com is the top level domain.

A FQDN always starts with a host name and continues all the way up to the top-level domain name, so www.parc.xerox.com is also a FQDN.

Forward" DNS zones

A forward lookup zone is a DNS zone in **which hostname to IP address relations are stored**. When a computer requests the IP address of a specific hostname, the forward lookup zone is queried and the result is returned. A reverse lookup zone does just the opposite. When a computer requests the hostname of an IP address, the reverse lookup zone is queried and the result is returned. Also, it is possible to have secondary forward lookup zones when using active directory integrated DNS. The secondary zone won't be ADI, but the primary zone from which it pulls can be. Also, DNS zone can only be Active Directory Integrated if the DNS server on which they reside also happens to be a domain controller. If your dns server isn't a domain controller, the zones aren't ADI, just standard forward lookup zones. **BIND** is an acronym for the **Berkeley Internet Name Domain** project, which is a group that maintains the DNS-related software suite that runs under Linux. The most well known program in BIND is named, the daemon that responds to DNS queries from remote machines.

Reverse DNS Zone

Reverse dns lookup is the inverse process of this, the resolution of an IP address to its designated domain name.

The reverse DNS database of the Internet is rooted in the *Address and Routing Parameter Area* (arpa) top-level domain of the Internet. IPv4 uses the in-addr.arpa domain and the ip6.arpa domain is delegated for IPv6. The process of reverse resolving an IP address uses the *pointer* DNS record type (PTR record).

How DNS Servers Find Out Your Site Information

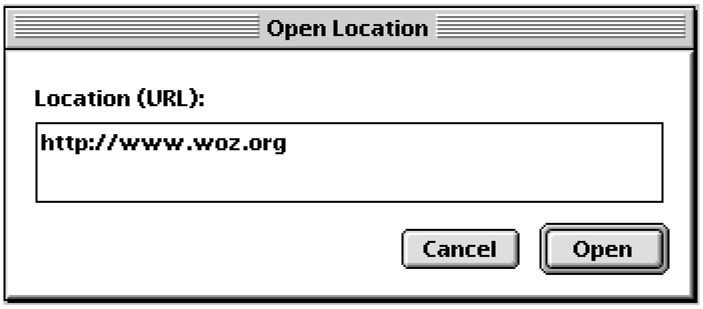
There are 13 root authoritative DNS servers (super duper authorities) that all DNS servers query first. These root servers know all the authoritative DNS servers for all the main domains - **.com, .net.org.edu**, and the rest. This layer of servers keep track of all the DNS servers that Web site systems administrators have assigned for their sub domains.

For example, when you register your domain my-site.com, you are actually inserting a record on the .com DNS servers that point to the authoritative DNS servers you assigned for your domain. (More on how to register your site later.).

How DNS Work?

How Lookups Are Handled

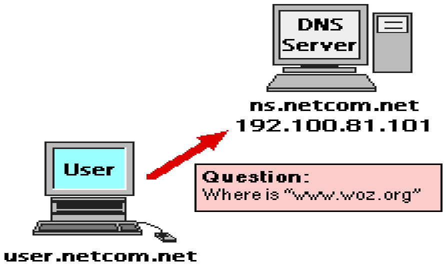
Here's how a DNS request is fulfilled. We'll use an example of a computer running Browser
1. The user enters asks Browser to go to "http://www.woz.org" and hits return.



Open Location

Location (URL): http://www.woz.org

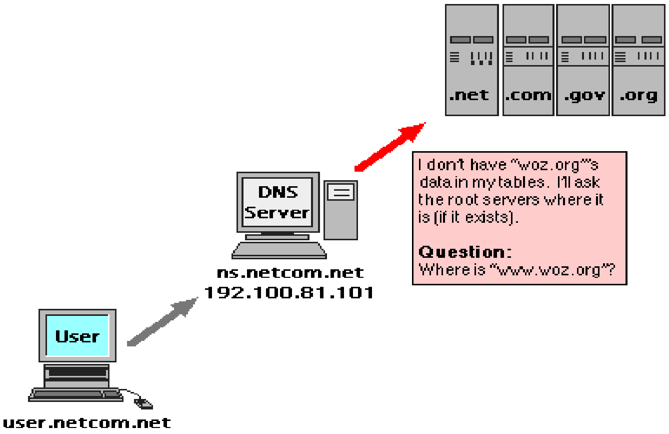
2. The computer's TCP stack doesn't know what address "www.woz.org" points to, so it calls upon its DNS server (192.100.81.101) for the address.



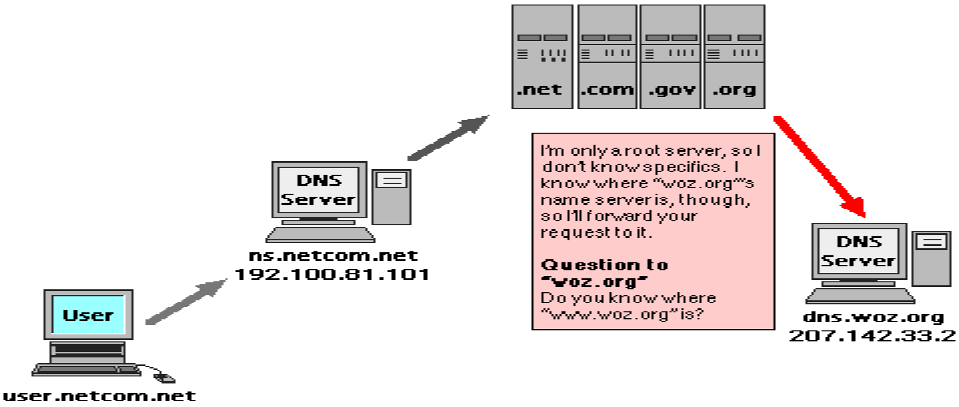
3. The DNS server runs the zone "netcom.net" and doesn't handle "woz.org". It first looks in its cache to see if its looked it up before, if so it just returns the address. Unfortunately the server hasn't looked up "netcom.net" before (or its cache entry has timed out), so it queries the server above it ".com" name server at the InterNIC (Internet Information Center) for the "woz.org" server.

Cached lookups on a domain name server are given "time-out values." This rids us of the problem of old entries being passed around. Time-out values are usually a minutes (for often-changed names) to more than a week. Time-out values are set by the person who runs the name server for a zone. This means that the administrator of "woz.org" can only set the time-out values for "woz.org" entries, and cannot modify "netcom.net" or "apple.com" entries, etc.

The InterNIC is where everybody must register their domain names. It keeps the hierarchy in tact so it works. It also houses what is called the "root servers," which point to "**.org", ".net", ".com",** etc. points in the Domain Name Space hierarchy.

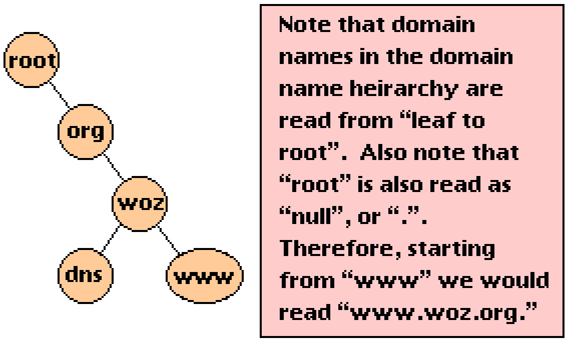


4. The root servers pass the request to the ".org" root server.


.net
.com
.gov
.org
DNS Server
ns.netcom.net
192.100.81.101
I'm only a root server, so I don't know specifics. I know where "woz.org"'s name server is, though, so I'll forward your request to it.
Question to "woz.org"
Do you know where "www.woz.org" is?
DNS Server
dns.woz.org
207.142.33.2
User
user.netcom.net

5. The ".org" root server passes looks up the "woz.org" server and finds it, so it passes the request to "woz.org"'s name server.

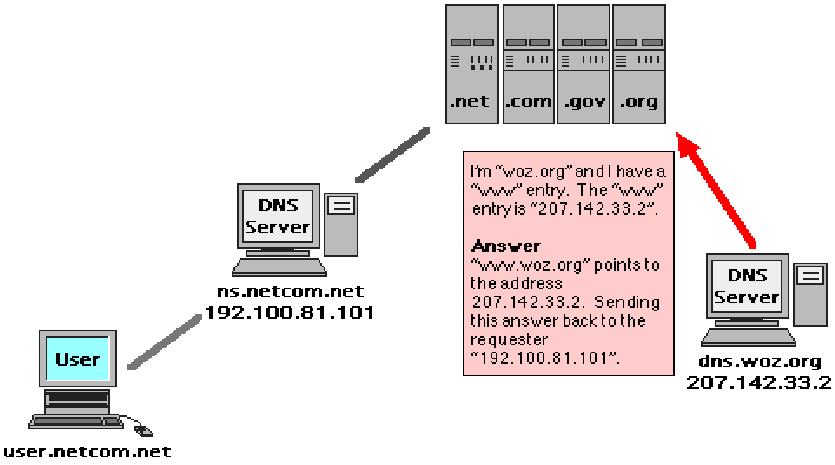
Note that the root servers only look up where "woz.org" is. They are not responsible for any of the **children** ("www", "dns", etc.) that "woz.org" is **authoritative** for. In this case, the root servers are authoritative for ".org", ".com", etc. They **delegate** authority for other domains to their children in the **domain name space tree**. Here is what the tree would look like going to the "woz.org" domain:



Note that domain names in the domain name heirarchy are read from “leaf to root”. Also note that “root” is also read as “null”, or “.”. Therefore, starting from “www” we would read “www.woz.org.”

Note that the root servers are "parents" to ".org", which is the "parent" of anything under it, including "woz", which is the "parent" of "dns", "www" and anything else that ends with "woz.org".

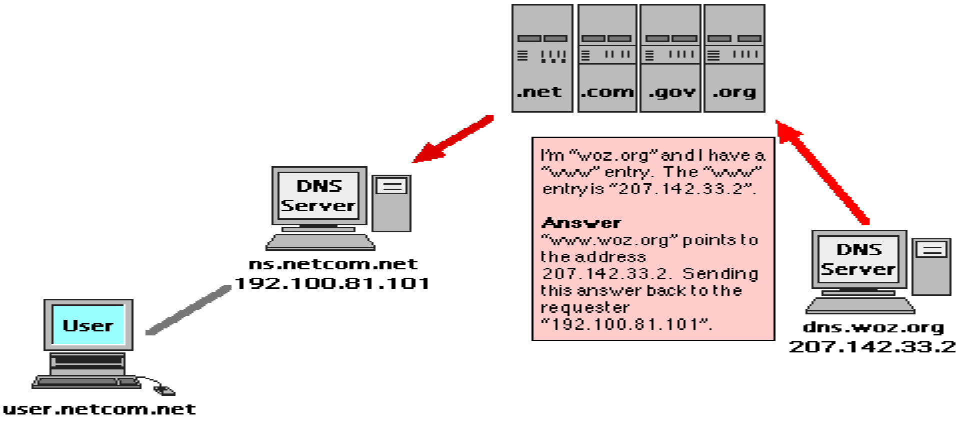
6. The "woz.org" name server looks in its table for a "www" entry. It finds it, and returns its address, 207.142.33.2.



I'm “woz.org” and I have a “www” entry. The “www” entry is “207.142.33.2”.

Answer
“www.woz.org” points to the address 207.142.33.2. Sending this answer back to the requester “192.100.81.101”.

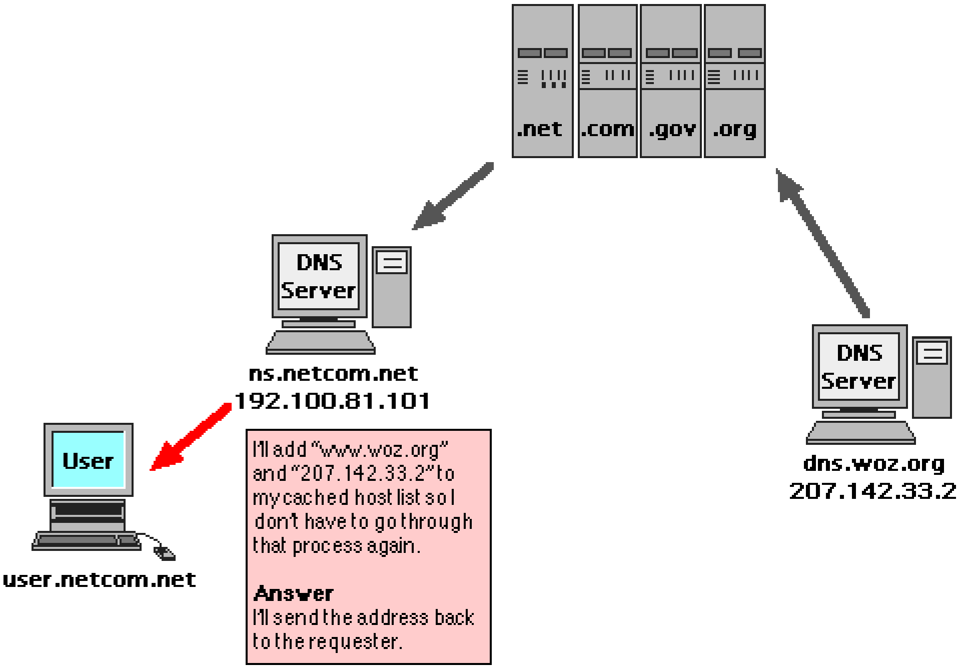
7. The request goes back to the sender, who's address has been retained the entire time as the originator of the name query.



I'm “woz.org” and I have a “www” entry. The “www” entry is “207.142.33.2”.

Answer
“www.woz.org” points to the address 207.142.33.2. Sending this answer back to the requester “192.100.81.101”.

8. The address 207.142.33.2 is added to the "netcom.net" name server's cache with a 1 day time-out, which means that it doesn't have to take the above steps again for an entire day.



I'll add "www.woz.org" and "207.142.33.2" to my cached host list so I dont have to go through that process again.

Answer
I'll send the address back to the requester.

9. The "netcom.net" name server returns the address to the user's TCP stack, which tells Netscape what address on the Internet to connect to (see above diagram).

10. The user gets connected to "www.woz.org".

How Name Servers Get Their Data

Parent name servers have to be able to query their siblings for data. This is called a "Zone Transfer" and is a special type of request. Zone transfers are used for when a zone's DNS server goes down. For example, if "ns1.apple.com" does zone transfers with "ns2.apple.com" we can be sure if "ns1" goes down that "ns2" will handle DNS queries until "ns1" is fixed (assuming "ns2" isn't down as well). How do servers know to switch? When you set up your domain with the InterNIC you specify a secondary name server, that's how! Isn't this structured approach great?

When the zone transfer request is sent by a parent server the name server sends a complete zone list in response and increments the zone's "serial number". If the parent server's last serial number from a zone transfer is less than the one in the transferred zone file then it needs to update its entries. If the number is the same then no updates have been made and the zone transfer data isn't used.

DNS SERVER CONFIGURATION

The package used to configure the DNS is “Bind” package. We can configure the DNS with the help of this package. First of all we will check whether the package is installed or not

The nslookup Command

The nslookup command provides the same results on Windows PCs. To perform forward lookup, use.

```
C:\> nslookup www.abc.com
Server:  192-168-1-200.my-site.com
Address:  192.168.1.200
```

The /etc/resolv.conf File

DNS clients (servers not running BIND) use the /etc/resolv.conf file to determine both the location of their DNS server and the domains to which they belong. The file generally has two columns; the first contains a keyword, and the second contains the desired values separated by commas. See for a list of keywords.

Important File Locations

Main file:	/etc/named.conf
Zone files:	/var/named/*.zone
Host conf:	/etc/host
Resolve conf:	/etc/resolve.conf

The SOA Record

The first resource record is the Start of Authority (SOA) record, which contains general administrative and control information about the domain. It has the format:

Name Class Type Name-Server Email-Address Serial-No Refresh Retry Expiry Minimum-TTL

NS, MX, A And CNAME Records

Like the SOA record, the NS, MX, A, PTR and CNAME records each occupy a single line with a very similar general format. Table 18.5 outlines the way they are laid out.

NS, MX, A, PTR and CNAME Record Formats

Record Type	Name Field	Class Field[2]	Type Field	Data Field
NS	Usually blank[1]	IN	NS	IP address or CNAME of the name server
MX	Domain to be used for mail. Usually the same as the domain of the zone file itself.	IN	MX	Mail server DNS name
A	Name of a server in the domain	IN	A	IP address of server
CNAME	Server name alias	IN	CNAME	"A" record name for the server
PTR	Last octet of server's IP address	IN	PTR	Fully qualified server name

1. If the search key to a DNS resource record is blank it reuses the search key from the previous record which in this case of is the SOA @ sign.
2. For most home / SOHO scenarios, the Class field will always be IN or Internet. You should also be aware that IN is the default Class, and BIND will assume a record is of this type unless otherwise stated.

Quota in Linux

You may eventually need to restrict the amount of disk space used on each partition by each user or group of users as your disk drives become filled with data. The disk quota feature of RedHat/Fedora Linux enables you to do this, and the setup is fairly simple.

Setting Up Quotas

For example, your family Linux server is running out of space in the /home filesystem because of an abundance of Data downloads.

Edit Fstab file

```
[root@mysrv tmp]# vi /etc/fstab
```

The /etc/fstab file lists all the partitions that need to be auto-mounted when the system boots. You have to alert Linux that quotas are enabled on the filesystem by editing the /etc/fstab file and modifying the options for the /home directory. You'll need to add the usrquota option. In case you forget the name, the usrquota option is mentioned in the fstab man pages.

The old /etc/fstab looked like

```
LABEL=/home      /home       ext3    defaults          1 2
```

but your new /etc/fstab should be add usrquota for quota activation on /home drive

```
LABEL=/home      /home       ext3    defaults,usrquota  1 2
```

Remount The Filesystem

Editing the /etc/fstab file isn't enough, Linux needs to reread the file to get its instructions for /home. You can do this using the mount command with the -o remount qualifier.

```
[root@mysrv tmp]# mount -o remount /home
```

Create The Partition Quota Configuration Files

The uppermost directory of the filesystem needs to have an aquota.user file (defines quotas by user) and an aquota.group file (defines quotas by group), or both. The man page for quota lists them at the bottom. In this case just enable per-user quotas for the /home filesystem.

```
[root@mysrv tmp]# touch /home/aquota.user
```

```
[root@mysrv tmp]# chmod 600 /home/aquota.user
```

Initialize the Quota Table

Editing the /etc/fstab file and remounting the file system only alerted Linux to the fact that the filesystem has quota capabilities. You have to generate a quota table, separate from the aquota files, that lists all the current allocations for each user on the file system. This table will be automatically and transparently updated each time a file is modified. Linux compares the values in this table with the quota limitations that the systems administrator has placed in the aquota files and uses this information to determine whether the user has rights to increased disk usage. You initialize the table with the quotacheck command. Be prepared: You'll get an error the first time you enter the command, because Linux will realize that the aquota file wasn't created using one of the quota commands:

```
[root@mysrv tmp]# quotacheck –vagum
```

```
quotacheck: WARNING -  Quotafile /home/aquota.user was probably truncated. Can't save
quota settings...
quotacheck: Scanning /dev/hda3 [/home] done
quotacheck: Checked 185 directories and 926 files
[root@mysrv tmp]#
```

Edit The User's Quota Information

Now you need to edit the user's quota information. The edquota command enables you to selectively edit a portion of the aquota.user file on a per-user basis:

```
[root@mysrv tmp]# edquota -u amir
```

The command will invoke the vi editor.

```
Disk quotas for user amir (uid 503):
  Filesystem  blocks     soft     hard    inodes    soft    hard
  /dev/hda3      24        0        0         7       0       0
```

From here, you can edit a number of fields:

- **Blocks:** The amount of space in 1K blocks the user is currently using.
- **Inodes:** The number of files the user is currently using.
- **Soft Limit:** The maximum blocks/inodes a quota user may have on a partition. The role of a soft limit changes if grace periods are used. When this occurs, the user is only warned that their soft limit has been exceeded. When the grace period expires, the user is barred from using additional disk space or files. When set to zero, limits are disabled.
- **Hard Limit:** The maximum blocks/inodes a quota user may have on a partition when a grace period is set. Users may exceed a soft limit, but they can never exceed their hard limit.

Here user **amir is limited to a maximum of 5MB** of data storage on /dev/hda3 (/home):

```
Disk quotas for user amir (uid 503):

  Filesystem  blocks     soft     hard    inodes    soft    hard
  /dev/hda3       24     5000        0         7       0       0
```

Testing

Linux checks the total amount of disk space a user uses each time a file is accessed and compares it against the values in the quota file. If the values are exceeded, depending on the configuration, then Linux prevents the creation of new files or the expansion of existing files to use more disk space.

Other Quota Topics

Creating disk quotas frequently isn't enough. You also have to manage the process by reviewing the quota needs of each user and adjusting them according to the policies of your company. You'll need to make Linux scan its hard disks periodically to check for exceeded quotas. This section describes the most common quota management activities.

Editing Grace Periods

The edquota -t command sets the grace period for each filesystem. Like the edquota -u command, it invokes the vi editor.

The grace period is a time limit before the soft limit is enforced for a quota-enabled file system. You can use time units of seconds, minutes, hours, days, weeks, and months. This is what you'll see with the command edquota -t.

```
[root@mysrv tmp]# edquota -t
```

```
Grace period before enforcing soft limits for users: Time units may be: days, hours, minutes, or
seconds

 Filesystem           Block grace period    Inode grace period
 /dev/hda3                  7days                 7days
```

Note: There should be no spaces between the number and the unit of time measure. Therefore in this example, "7days" is correct and "7 days" is wrong.

Editing Group Quotas

Editing quotas on a per-group basis can be done similarly with the edquota -g command.

Getting Quota Reports

The repquota command lists quota usage limits of all users on the system. Here is an example.

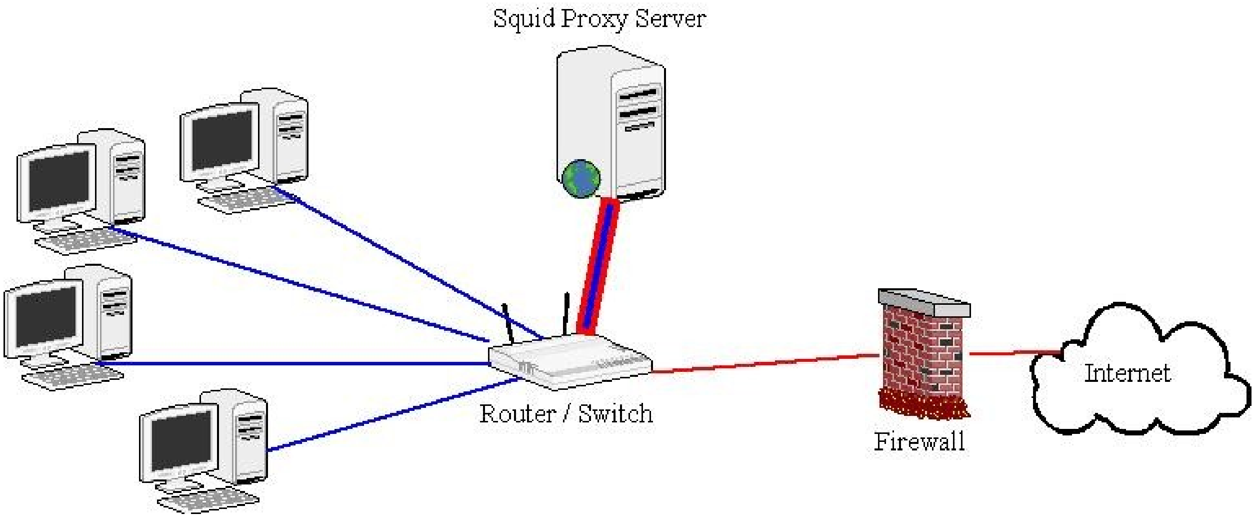
```
[root@mysrv tmp]# repquota /home
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
                    Block limits              File limits
User          used    soft    hard  grace    used  soft  hard   grace
----------------------------------------------------------------------
root     --   52696      0       0             1015     0     0
...
...
...
amir   --     24       0       0                  7     0     0

[root@mysrv tmp]#
```

Conclusion

Disk quotas are good to put in place for specific users whose disk usage activities need to be curtailed. It helps to not only limit the use of physical disk resources that could potentially be put to better use, but also reduces the likelihood of having fragmented disk structures that slow disk access due to the presence of too many files. User education must play a major role in your strategy too; users must be made aware of the challenges you face as a result of excessive disk usage. Of course, there comes a time when you are faced with no option but to expand the number of disks in your system.

Squid Proxy Server

Squid is a proxy server and web cache daemon. It has a wide variety of uses, from speeding up a web server by caching repeated requests, to caching web, DNS and other computer network lookups for a group of people sharing network resources, to aiding security by filtering traffic.



Users configure their web browsers to use the Squid proxy server instead of going to the web directly. The Squid server then checks its web cache for the web information requested by the user. It will return any matching information that finds in its cache, and if not, it will go to the web to find it on behalf of the user. Once it finds the information, it will populate its cache with it and also forward it to the user's web browser. The Squid web caching proxy server can achieve both these goals fairly easily

1- Reduce Internet bandwidth charges

2- Limit access to the Web to only authorized users.

PROXY SERVER CONFIGURATION

The package used to configure the proxy server is called "squid"

To make the proxy server accessible following changes are required in **squid.cof**

[root@mysrv]# vi /etc/squid/squid.conf

1 Http_Port **8080** (set the port)

2 **Cache _ dir** (uncomment)

3 **Cache _ access** (uncomment)

4 **Cache _ store** (uncomment)

5 **Cache_ Log** (uncomment)

6 **visible _ hostname** (write the machine name)

7 **Cache _ mgr** **mysrv@yahoo.com**

8. **http_access allow all**

:wq!

[root@mysrv] # service squid restart