

Network Administration 101

Network Administration 101 is a course target to those who want to start their career in the field of network and system administration. Students with some knowledge in networking can also study this course. In this course I'll try to teach every aspects of networking in Linux to become a company System or Network Administrator. Working for 3 years as a Network administrator I've designed this course considering all the beginners who want to move their career to networking.

According to wiki “A **network administrator** is an individual that is responsible for the maintenance of [computer hardware](#) and software systems that make up a [computer network](#) including the maintenance and [monitoring](#) of active [data network](#) or [converged infrastructure](#) and related [network equipment](#).”

The role of Network Administrator and their tasks can be given as :

- Designing and planning the network
- Setting up the network
- Maintaining the network
- Expanding the network

Course Contents

Introduction to Networking [1]

Clamping & Network Devices[2]

Centos Installation & Basic Linux Commands[3]

Commands & Configuring Network[3]

DHCP Server[2]

Web & FTP Server[1]

DNS & Proxy Server[2]

Bandwith Management [1]

Securing Server with Firewall & NAT [2]

Remote Network Administration[1]

Bash Scripting [3]

Mikrotik-First Time Access[1]

IP,DHCP,NAT (masquerade) [1]

1. Introduction to Networking

Interconnection between any two nodes or system for resource sharing is defined as networking. Today we are in the age of Internet. Most of the task of our daily live has been attached to Internet. Data communications and networking are changing the way we do business and the way we live.

In this course we will be discussing on practical aspects of setting up the network. We'll use Linux for almost all purposes as it have good environment and tools for networking.

TCP/IP

Transmission Control Protocol / Internet Protocol is a standard protocol to provide network connection. It is part of the larger OSI model upon which most data communications is based. In this protocol data is splitted into multiple pieces or “packets”.

The two most popular transportation mechanisms used on the Internet are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is reliable protocol. In this protocol handshaking mechanism is used to ensure packets are properly delivered to receiver. It is used in those conditions where 100% delivery of packet is important like file transfer etc. UDP is unreliable protocol. It discards errors. Applications like video streaming uses this protocol where delay in transmission is critical. TCP is a "Connection Oriented Protocol" while UDP is TCP's "Connectionless" cousin .

IP Address

Each device in a network is represented by an address called IP Address. There are two types of IP address : IPv4 and IPv6. IPv6 is not used widely till now , so we'll use IPv4 in this training. IPv4 uses 32 bit address. For ease of use, this 32 bit address is divided into four sets of eight bits (or octets), each representing a number from 0 to 255. For eg. 97.65.25.12 .

There are various classes of IP address depending on their use. They are Class A,B,C,D,E.

Some groups of IP addresses are reserved for use only in private networks and are not routed over the Internet. These are called "Private IP addresses" and have the following ranges:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 – 192.168.255.255

Class A

Class A comprises networks 1.0.0.0 through 127.0.0.0. The network number is contained in the first octet. This class provides for a 24-bit host part, allowing roughly 1.6 million hosts per network.

Class B

Class B contains networks 128.0.0.0 through 191.255.0.0; the network number is in the first two octets. This class allows for 16,320 nets with 65,024 hosts each.

Class C

Class C networks range from 192.0.0.0 through 223.255.255.0, with the network number contained in the first three octets. This class allows for nearly 2 million networks with up to 254 hosts.

Classes D, E, and F

Addresses falling into the range of 224.0.0.0 through 254.0.0.0 are either experimental or are reserved for special purpose use and don't specify any network. IP Multicast, which is a service that allows material to be transmitted to many points on an Internet at one time, has been assigned addresses from within this range.

Address Resolution

ARP (Address resolution protocol) is used for getting Ethernet address from IP Address. ARP sends broadcast packet containing IP address to all device in network. And if the device match given address with its own then its reply with its Ethernet Address.

GATEWAY

To connect to another network we must go through a gateway. For eg. In our home we connect to Internet using Router which acts as gateway for our network. Generally IP address of gateway is set to starting ip address like 192.168.1.1. Gateway can be a router, a pc , a server etc.

NAT

NAT stands for Network Address Translation. Generally we need public IP address to connect to Internet. But let if we have only one public ip address and we have a home network of 10 computers. What to do if we want to connect all computers to Internet ? In such conditions we use NAT technology. NAT masquerades our local network and convert private IP to public IP address and all the computer will be connected to network. We'll practically do NAT later on the training.

There are two types of NAT : SNAT & DNAT

SNAT (Source NAT) : Private IP is converted into Public like in our home network.

DNAT (Destination NAT) : Public IP is converted into private.

MASQUERADE : Used to do Source Network Address Translation. ie.rewriting the source IP address of the packet .

Static vs Dynamic IP Address

Based on IP allocation there are two types of ip address : static and dynamic.

In static address allocation a computer defines its IP address manually and it becomes the permanent one. Generally servers use static IP address that remains constant always.

In dynamic address allocation a computer gets IP address dynamically from the server. It is used in network with changing computers. For eg let in our home network we have 50 computers and the computer will be added time to time, so in such situations it be best to provide them IP address dynamically. The most widely used technology for dynamic IP address is using DHCP (Dynamic Host Control Protocol) Server.

DNS (Domain Name Server)

Remembering the IP address of a server is difficult task for anyone. We IP to Name mapping is used because names are easy to remember. For eg. Ip address of my website is 74.23.123.90. If there is no domain how many could remember this address to open my website. But thanks to Domain Name System that translated this address to good domain name = www.geeknepal.com

This translation of IP to Domain name and domain name to IP is done via Domain Name Server.

Subnet Mask

Dividing the network is called subnetting. There are two parts in an IP address : network part and host part. Subnet mask is used to tell which part of IP represent network part and which part represent host part.

Most home networks use a subnet mask of 255.255.255.0. Each "255" means this octet is for the network portion. So if your server has an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0, then the network portion would be 192.168.1 and the server or host would be device #1 on that network.

Below is a list from which you can find the number of address in a subnet.

Subnet with /	Available Address
255.255.255.0 /24	256
255.255.255.128 /25	192
255.255.255.192 /26	64
255.255.255.224 /27	32
255.255.255.240 /28	28
255.255.255.248 /29	18
255.255.255.252 /30	4

Hub , Switch & Routers

Hub are featureless device to connect devices on network. If a server sends packet to a specific computer then the hub sends the packets to every computer and each will receive the packet. Only the computer with matching IP header accepts the packets and other will discard this. So due to this limitation and slow networking with hub it has been replaced by switch. Switch uses MAC based authentication and only the computer that matched MAC will get the packet. There are various smart switches that can be used to manage bandwidth , gateway , ip address etc.

Router are more smarter . They work on Network Layer . Their main responsibility is routing of packets from one network to another.

In this training we use Cisco switch and TP-Link Router.

Firewalls

Each network is vulnerable from different security attacks. So network administrator must configure strong firewall to prevent their network from different attacks. Firewalls can also be used to setup various rules to block and allow different services and ports on network.

In this training we use firewall for following purposes

- Throttling traffic to a server when too many unfulfilled connections are made to it
- Restricting traffic being sent to obviously bogus IP addresses
- Providing network address translation or NAT
- Blocking unwanted ports
- Preventing various security attacks

Iptables is the tool that we will be using. It is the most popular firewall in Linux world. It is build on Linux Kernel.

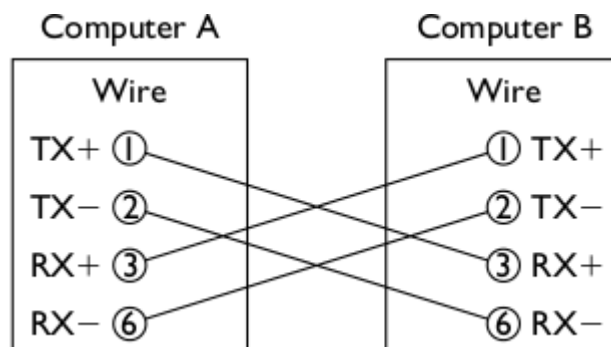
Clamping Network Wires

This was a bit theory. Now we'll start our practical training with clamping network wires.

We'll use UTP cable for small cost effective networking. Given table show various categories of UTP cables. We'll use CAT5

Generally there are two modes of connection : Crossover cables & Straight-through cables.

Crossover : It is used to connect two computers directly.



Wire	Connector #1	Connector #2
1	White wire/orange stripe (white-orange)	White wire/green stripe (white-green)
2	Orange wire	Green wire
3	White wire/green stripe (white-green)	White wire/orange stripe (white-orange)
4	Blue wire	Blue wire
5	White wire/blue stripe (white-blue)	White wire/blue stripe (white-blue)
6	Green wire	Orange wire
7	White wire/brown stripe (white-brown)	White wire/brown stripe (white-brown)
8	Brown wire	Brown wire

Straight-through : connect switch-computer or router-computer

Computer	Hub
Wire	Wire
TX+ ①	① RX+
TX- ②	② RX-
RX+ ③	③ TX+
RX- ④	④ TX-

Wire	Connector #1	Connector #2
1	White wire/orange stripe (white-orange)	White wire/orange stripe (white-orange)
2	Orange wire	Orange wire
3	White wire/green stripe (white-green)	White wire/green stripe (white-green)
4	Blue wire	Blue wire
5	White wire/blue stripe (white-blue)	White wire/blue stripe (white-blue)
6	Green wire	Green wire
7	White wire/brown stripe (white-brown)	White wire/brown stripe (white-brown)
8	Brown wire	Brown wire



Crimping tool

2. Basic Linux Commands

In this part we'll study why we need Linux for networking and get started from basic Linux commands for network administration.

Why Linux

Linux is extremely powerful operating system. It is best due to following reasons :

Extremely Fast

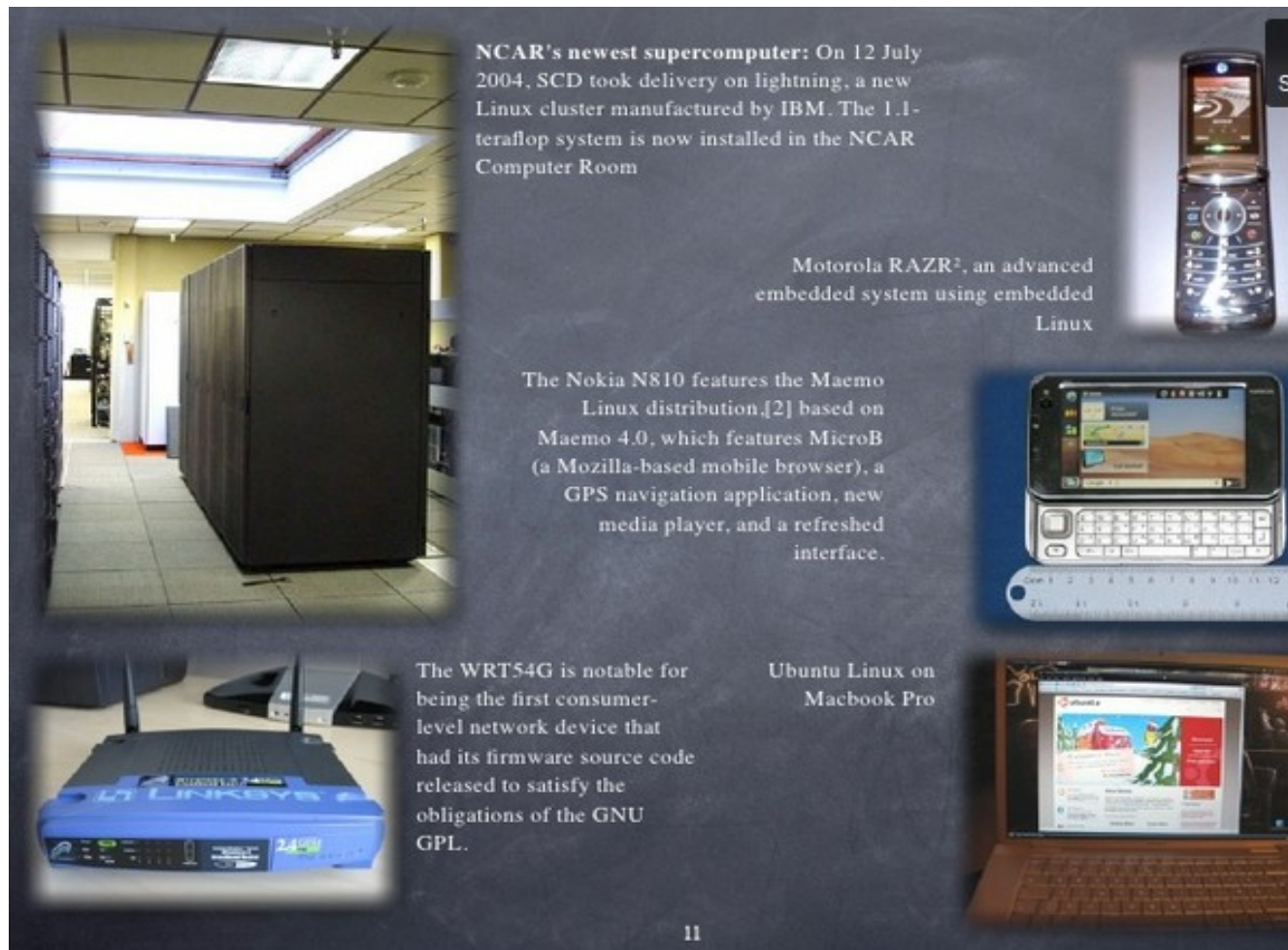
Efficient Allocation of Resources

No Viruses

Large Community Help

Everything Free

Highly Secure



NCAR's newest supercomputer: On 12 July 2004, SCD took delivery on lightning, a new Linux cluster manufactured by IBM. The 1.1-teraflop system is now installed in the NCAR Computer Room

Motorola RAZR², an advanced embedded system using embedded Linux

The Nokia N810 features the Maemo Linux distribution,[2] based on Maemo 4.0, which features MicroB (a Mozilla-based mobile browser), a GPS navigation application, new media player, and a refreshed interface.

The WRT54G is notable for being the first consumer-level network device that had its firmware source code released to satisfy the obligations of the GNU GPL.

Ubuntu Linux on Macbook Pro

There are more than 300 flavors of Linux. They are also called distros. Some of them are :
Ubuntu, Centos , Linux Mint , RedHat , Fedora , Kali , Puppy Linux etc.

About 90% of servers use linux as their core operating system. Networking under linux has following advantages :

Unix Initially developed for Networking

Lots n lots of tools for networking

Large community support

Absolutely free

Highly secure

Frequent Updates

Centos Installation

Get a copy of centos 6.5 iso from its official website www.centos.org. You can install it directly to hard disk or you can install it in virtual machine.

Linux Commands

Linux commands are heart of Linux network administration, so it is vital for every administrator to become familiar with most of the Linux commands. We'll cover some important Linux commands under following topics :

- General Commands
- Basic I/O
- Searching fast with Grep & Regular Expressions
- Accessing Remote Systems
- Archiving & Compressing
- Run levels
- Process Management
- Network services
- File Systems
- Permissions

- ACL
- User Management
- Configuring Network
- Package Management
- Scheduling Jobs
- Firewall
- SELinux

General Commands

Ls : List files

Cp/mv : Copy & move/rename files

Rm : Delete files

Cd : Change directory

Pwd : Print current directory name

Mkdir/rmdir : Create/delete directory

Cat : view files

Head/tail : view top/bottom 10 lines of file

Basic I/O

Input/Output in Linux takes place in three modes. They are STDIN, STDOUT , STDERR . Each are represented by a number i.e. 0 , 1 and 2 respectively.

abgeek@geeknepal:~\$

Each time I type above text , it indicates that I'm working from terminal as abgeek user in geeknepal computer. So every time you see this indication open your terminal.

abgeek@geeknepal:~\$ read MESSAGE < afile

This is take standard input from a file and saves in the variable MESSAGE. If you echo \$MESSAGE

then you'll get content from the variable printed on STDOUT

```
abgeek@geeknepal:~$ ls > afile
```

It will outputs the contents of folder to afile. It is simple example of STDOUT

```
abgeek@geeknepal:~$ ls invalid_folder 2> afile
```

If there is not any folder name invalid_folder then this will sends error to the file. 2> is for STDERR

Grep & Regular Expressions

Grep is an useful tool for searching any text or patterns. It uses mathematical concept of regular expressions. We'll not discuss complex mathematical regex in this training but learn how to use it.

The basic syntax of grep is

```
grep <searchterm> <fromwhere> or STDIN
```

It means we are searching for a “searchterm” from a file or location “fromwhere” or STDIN

eg. grep apple afile.txt

It searches for term apple on the file “afile.txt”

The searchterm can be regex “regular expression”

- * term repeats 0 or more times
- . any single character but not end of line
- [] any of items or range in brackets
- ^ term at begin of line
- \$ term is at end of line
- Examples :
 - Grep test.g afile grep ^sh afile grep \$t afile
 - Grep [0-9] afile grep ^[0-9] afile

Accessing Remote Systems

Sometime as a network admin you have to access your system from outside the network. So in such conditions you have to establish a secure connection to your server. You can connect in following two

ways :

- a. VNC (virtual network computing) : It is done through graphical interface. Usually slow and unencrypted connection. To use it port 5900 should be made trusted on firewall.
- b. SSH (Secure Shell) : It is the best way to connect remotely. I always prefer this. It works on port 22 and is encrypted connection.

Basic syntax to connect to a server is

```
abgeek@geeknepal:~$ ssh abgeek@geeknepal -p 22
```

To connect from external network

```
abgeek@geeknepal:~$ ssh abgeek@116.90.239.2 -p 22
```

You can also login to graphical interface via ssh by :

```
abgeek@geeknepal:~$ ssh -X abgeek@116.90.239.2 -p 22
```

To copy a test folder from our pc to remote server :

```
abgeek@geeknepal:~$ scp test -r abgeek@116.90.239.2:/home/user1
```

This will copy a folder named test to /home/user1 folder of server.

To save the authentication you can generate keys and copy to server. It will prevent you from asking password in future logins

```
abgeek@geeknepal:~$ ssh-keygen -t rsa
```

This will generate rsa key. You have to enter a key. Stronger the key stronger will be encryption.

The keys are stored in /.ssh/id_rsa

Now copy the above key to server.

```
abgeek@geeknepal:~$ scp /.ssh/id_rsa abgeek@116.90.239.2:/home/user1/.ssh/authorized_keys2
```

Note : Set permission for authorized_keys file

To login to root user type :

```
abgeek@geeknepal:~$ su root
```

To login to root user and change home directory to root type :

```
abgeek@geeknepal:~$ su -l root
```

Archiving & Compressing

Archiving is like collecting all the files, source codes in one file but compressing is to collect and reduce the size.

Archiving can be done either by tar or star command. Star supports selinux acl.

```
abgeek@geeknepal:~$ tar -cvf afile.tar afolder/
```

This will create afile.tar of folder afolder. C = create , v = verbose , f = file

```
abgeek@geeknepal:~$ tar -xvf afile.tar
```

It will extract tar file to folder

```
abgeek@geeknepal:~$ tar --selinux --xattrs --acls -cvf afile.tar afolder/
```

This will create afile.tar of folder afolder with Selinux features.

Compressing can be done by gzip or bzip2.

```
abgeek@geeknepal:~$ gzip afile.zip afolder
```

```
abgeek@geeknepal:~$ tar -zxvf afile.tar.gz afolder
```

Manuals

In linux you can view and learn about commands by using following tools :

man = this will shows manual page of a command

eg. **abgeek@geeknepal:~\$ man cat**

man -k

apropos

whatis

info

Vi editor

Vi is the best editor I liked ever. It is very easy to use and comes with a lot of shortcuts.

```
abgeek@geeknepal:~$ vi test.txt
```

Vi runs in different modes. The most useful are command and insert mode. In insert mode we enter our text and in command mode we perform different functions on text. To switch between these two modes press 'I' to insert and 'ESC' to command.

Below are some shortcuts :

:w write to file

:wq save and quit file

:q! force quit

shift + g goto end of file

5yy copy file lines below current line

v paste the copied (yanked lines)

Vi is a vast editor. There is one entire book on VI. Try to learn it yourself.

Runlevels

Linux runs in different run levels. Generally there are 6 run levels. Their files are located at /etc/rc.

0 : halt

1 : single user mode

2: multiuser , no network

3: multiuser, with network

4: no used in Centos

5: multiuser,network : X windows

6: reboot

Linux runs in anyone of the above mode. You can switch to another mode by using telinit command.

```
abgeek@geeknepal:~$ telinit 6
```

This will switch to 6 runlevel and restarts the system.

You can view current runlevel by :

```
abgeek@geeknepal:~$ runlevel
```

Runlevel defaults can be changed by configuring /etc/inittab file

```
abgeek@geeknepal:~$ vi /etc/inittab
```

```
id:5:initdefault
```

In the file you'll see like above result. Then you can change no.5 to anyone you'd like to make default runlevel.

Process Management

Process Management is an important task in network administration. You should be able to find out and kill rouge process and change the priority of a process for faster execution.

Lets view the top process by executing top command.

```
abgeek@geeknepal:~$ top
```

Use shift + < to sort by columns

```
abgeek@geeknepal:~$ ps -ef
```

This will show everything and full list of all programs

Now use kill and pkill to kill the process

```
abgeek@geeknepal:~$ kill -9 PID           #PID is process id of process to kill
```

You can kill all program associated with a program by killall

```
abgeek@geeknepal:~$ killall -9 firefox
```

You can kill a program by pattern name. Each program related with this pattern will be killed.

eg. pkill -9 fox

#It will kill all program consisting of fox pattern

Note : *pgrep before pkill to ensure the program is wise !!*

Sometime we want to increase/decrease the priority of some process. For that we nicing and renicing commands.

```
abgeek@geeknepal:~$ nice -n 19 firefox
```

It will start firefox with 19 priority.

-20 has highest priority , 0 is default and 19 is lowest priority. The higher(more negative) the priority , the faster will be process execution.

To change the priority of a process use :

```
abgeek@geeknepal:~$ renice -n 20 PID
```

Network Services

All the configuration files in linux are stored on /etc/ folder and all the startup files are located on /etc/init.d/xxx directory. Xxx are services.

The basic command for services is :

```
abgeek@geeknepal:~$ service xxx start/stop/status/restart
```

In Centos you have to enable the run level for services in order to run.

To list all services with runlevel enter :

```
abgeek@geeknepal:~$ chkconfig --list <servicename>
```

To on all runlevels for httpd

abgeek@geeknepal:~\$ chkconfig httpd on

To turn on httpd for runlevel 3 and 5 enter :

abgeek@geeknepal:~\$ chkconfig httpd on --level 35

Log Files

To become a good network administrator you must be able to view the log files. These files will help to find a problem in system and can give hint to troubleshoot them.

All log files in Linux are stored on /var/log directory.

To view logs you can use many tools like : tail , less , more , cat , grep

To view last 50 lines of log file message use :

abgeek@geeknepal:~\$ tail -50 /var/log/messages

To view 10 fresh lines in log file use :

abgeek@geeknepal:~\$ tail -f

File System

Linux uses Journal File System for better memory cache and data tracking. In Journal file system , data is tracked so that any error can be checked and corrected. EXT4 is the most widely used filesystem for Linux environment now-a-days.

Before any partition can be used it have to be mounted. Mounting is the process of making a partition ready to use. Mounting is done in a directory.

To view all available partitions :

abgeek@geeknepal:~\$ fdisk -l

You can see /dev/sda* in the result. They are partitions in your disk.

To mount a partition enter :

abgeek@geeknepal:~\$ mount -t ntfs /dev/sda2 /mnt

This will mount /dev/sda2 partition of type ntfs to /mnt folder. Now you can access your files from /mnt folder.

To unmount the partition :

abgeek@geeknepal:~\$ umount /dev/sda2

Encryption in partition is often needed to protect your files from unauthorized access. Cryptsetup is a very good partition encrypting tool available with us. It uses LUKS (Linux Unified Key Setup) extension. is a standard for hard disk encryption. It standardizes a partition header as well as the format of the bulk data. LUKS can manage multiple passwords that can be individually revoked and effectively scrubbed from persistent media, and that are protected against dictionary attacks with

PBKDF2.

Now try the following commands to encrypt a drive , open it and again encrypt after using :

Encrypt /dev/sda2 drive

```
abgeek@geeknepal:~$ cryptsetup luksformat /dev/sda2
```

Now prepare the encrypted drive to enc_drive folder

```
abgeek@geeknepal:~$ cryptsetup luksopen /dev/sda2 enc_drive
```

Formatting the drive with ext4 filesystem

```
abgeek@geeknepal:~$ mkfs.ext4 /dev/mapper/enc_drive
```

Mounting the partition

```
abgeek@geeknepal:~$ mount /dev/mapper/enc_drive /mnt/home
```

Now close the encrypted drive after using

```
abgeek@geeknepal:~$ cryptsetup luksclose enc_drive /dev/sda2
```

To auto mount the partition change configuration of /etc/fstab file

To auto decrypt drive : /etc/crypttab

You can format a disk using either fdisk or parted tool.

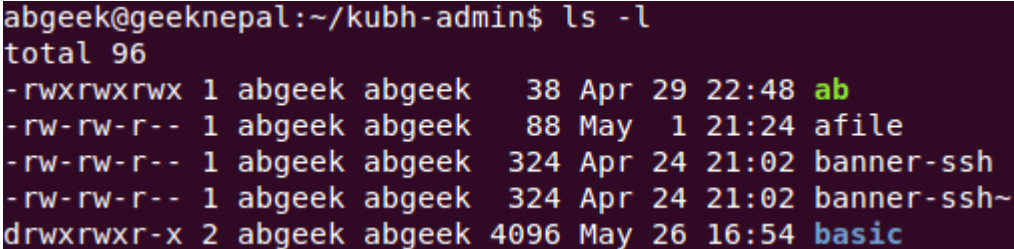
Permissions

In Linux every file consists of various types of permission. The permission can be different for its owner or group or others or even an individual users. We have variety of options to change the permissions of files.

At first lets understand permission bits.

In any folder run following command , you can see output like below :

```
abgeek@geeknepal:~$ ls -l
```



```
abgeek@geeknepal:~/kubh-admin$ ls -l
total 96
-rwxrwxrwx 1 abgeek abgeek  38 Apr 29 22:48 ab
-rw-rw-r-- 1 abgeek abgeek  88 May  1 21:24 afile
-rw-rw-r-- 1 abgeek abgeek 324 Apr 24 21:02 banner-ssh
-rw-rw-r-- 1 abgeek abgeek 324 Apr 24 21:02 banner-ssh~
drwxrwxr-x 2 abgeek abgeek 4096 May 26 16:54 basic
```

Notice the first column on the above output :

drwxrwxr-x

d = directory (- for file)

The first group of rwx = read+write+execute. This first group of rwx is for owner of file/folder, second group of rwx is for groups of the owner and the third group is for other than owner and groups.

Here for the folder **basic** owner has read/write/execute all permission , so for group also , but for others the permission is only for reading and executing.

You can set the permission by using chmod command.

Lets create a new file test_file and add read ,write ,execute permission for others.

```
abgeek@geeknepal:~$ touch test_file
```

```
abgeek@geeknepal:~$ chmod o+rw test_file
```

This will add read(r),write(w) and execute(x) permission for others to test_file

```
abgeek@geeknepal:~$ chmod g-rw test_file
```

This will remove read(r) and write(w) permission for group to test_file

```
abgeek@geeknepal:~$ chmod uo+r test_file
```

This will add read(r) permission for owner and others to test_file

You can set the permission using numeric value also. The value of read , write and execute are 4 , 2 and 1 respectively.

```
abgeek@geeknepal:~$ chmod 777 test_file
```

This will add read(r),write(w) and execute(x) permission for all users to test_file

First 7 is for owner = $4+2+1 = 7$

Second 7 is for groups = $4+2+1 = 7$

Thirid 7 is for others = $4+2+1 = 7$

```
abgeek@geeknepal:~$ chmod 741 test_file
```

This will give all permission to owner , only read to groups and only execute to others.

First 7 is for owner = $4+2+1 = 7$ (read,write,execute)

Second 4 is for groups = $4 + 0 + 0 = 4$ (read)

Thirid 1 is for others = $0 + 0 +1 = 1$ (execute)

In this way you can set the permissions.

You can also change the ownership of a file/folder

```
abgeek@geeknepal:~$ chown user1.group1 test_file
```

This will change the owner of test_file to “user1” user of group1

Note : Linux consists of a special permission that enable us to run files or commands in user/group/other mode. They are SUID, SGID and Stickybit.

Chmod u+s file = This sets SUID for file

You'll be clear with the use of SUID from following example :

```
abgeek@geeknepal:~$ ls /root
```

It will gives permission denied error.

Now if we set SUID of ls command by :

```
abgeek@geeknepal:~$ chmod u+s /bin/ls
```

abgeek@geeknepal:~\$ ls /root

Now it will list the files. I think you have understood the use of SUID. It will gives owner privilege of a file. But using this feature is dangerous for security purposes. So use it wisely.

ACL (Access Control List)

In the previous section we saw how to set permission to file/folder but if we want to set a file permission to specific user then how to do it ? It can be done using Access Control List. It allow us to set individual user/group permission.

#getfacl => It is used to view access control list associated with files

#setfacl => It will set ACL for file.

To set read and write ACL to user abgeek use :

abgeek@geeknepal:~\$ setfacl -m u:abgeek:rw afile

It will set read and write permission to user abgeek to “afile:

abgeek@geeknepal:~\$ getfacl afile

It will list ACL of file

3. Setting up DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. It is a very good protocol used in those situations where we have to assign IP address to changing computers or where number of computers are changing everyday.

For eg. If in an organization everyday 10-100 computers need a new IP address or have to get IP address automatically then it will not be feasible for network administrator to assign static IP address to each and every computers. In such case DHCP Server is used.

When a DHCP server is started in a computer then clients connect to this server by discovering it. The process of connection between clients and DHCP server is explained as below :

1. A client turns on a computer with a DHCP client.
2. The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
3. The router directs the DISCOVER packet to the correct DHCP server.
4. The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.
5. The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
6. The server sends an ACK (or DHCPACK) packet, confirming that the client has been given a lease on the address for a server-specified period of time.

In this way client connects to DHCP server and gets IP Address. DHCP server can statically allocate IP address to its client. It assigns a specific IP address to specific MAC address.

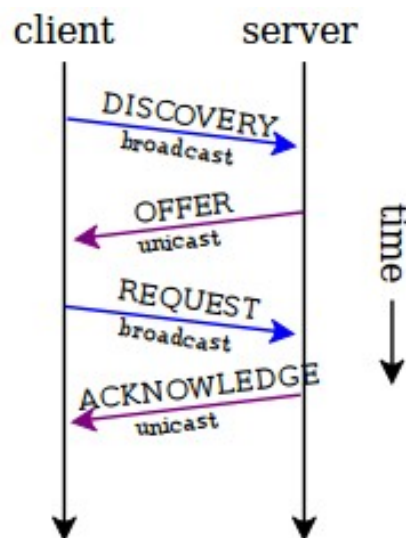
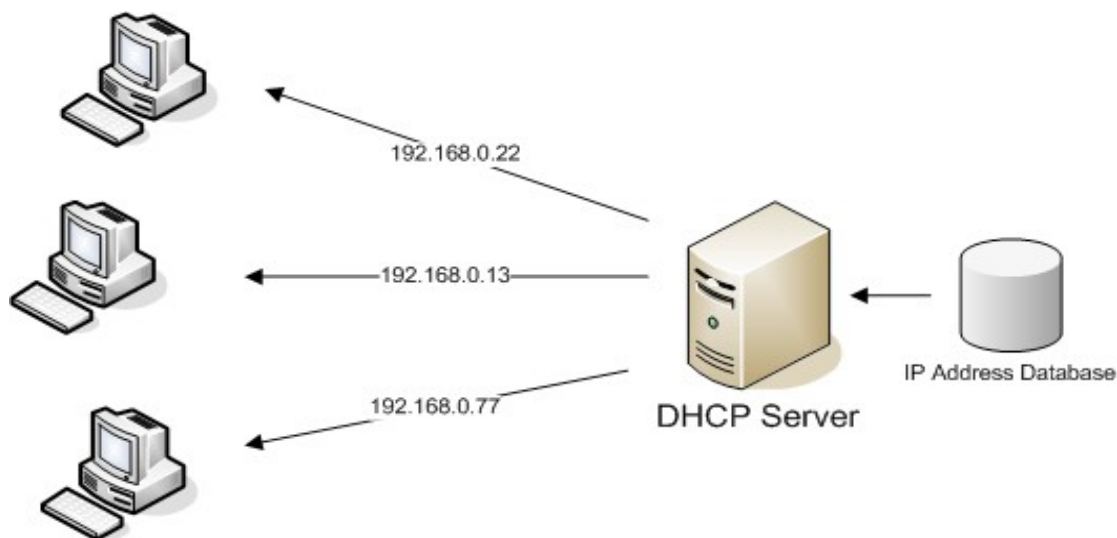


Fig : DHCP Connection Process



Now we'll configure DHCP server on CentOS :

At first install all necessary package for DHCP :

```
abgeek@geeknepal:~$ yum -y install dhcp
```

Before configuring DHCP server we should assign a static IP address to our interface for listening to DHCP clients.

On Centos : Open `/etc/sysconfig/network-scripts/ifcfg-eth0` and make change as per your requirement.

```
DEVICE="eth0"
```

```
HWADDR="00:0C:29:F1:01:4B"
```

```
NM_CONTROLLED="yes"
```

```
ONBOOT="yes"
```

```
BOOTPROTO="none"
```

```
IPADDR=192.168.1.1
```

```
NETMASK=255.255.255.0
```

```
GATEWAY=192.168.1.1
```

Here our server will listen for DHCP clients on eth0 interface. You can assign another interface.

Here our server has IP address 192.168.1.1.

On Ubuntu : nano `/etc/network/interfaces`

```
auto lo
```

```
iface lo inet loopback
```

```
iface eth0 inet static
```

```
address 192.168.1.1
```

```
gateway 192.168.1.1
```

```
netmask 255.255.255.0
```

```
dns-nameservers 8.8.8.8
```

Now we have configured our interface with static IP.

Now open `/etc/sysconfig/dhcpd` file and add the preferred interface name to DHCPDARGS variable as below :

```
abgeek@geeknepal:~$ vi /etc/sysconfig/dhcpd
```

```
# Command line options here
```

```
DHCPDARGS=eth0
```

In case of Ubuntu : nano `/etc/default/isc-dhcp-server`

```
INTERFACES="eth0"
```

Now lets Start configuring DHCP Server :

open `/etc/dhcp/dhcpd.conf` file and paste the below lines and save it.

```
#specify domain name
```

```
option domain-name "geeknepal.com";
```

```
#specify DNS server ip and additional DNS server ip
```

```
option domain-name-servers 192.168.1.1, 8.8.8.8;
```

```
#specify default lease time
```

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

```
#specify Max lease time
```

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

```
#specify log method
```

```
log-facility local7;
```

```
#Configuring subnet and iprange
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
range 192.168.1.50 192.168.1.254;
```

```
option broadcast-address 192.168.1.255;
```

```
#Default gateway ip
```

```
option routers 192.168.1.1;
```

```
}
```

```
#Fixed ip address based on MAC id
```

```
host abgeek{
```

```
hardware ethernet 02:34:37:24:c0:a5;
```

```
fixed-address 192.168.1.55;
```

```
}
```

At last restart the DHCP service :

```
abgeek@geeknepal:~$ service dhcpd restart
```

In this way you can configure dhcp server.

Now connect a client through switch to your computer and it is seen that client will get an IP address from your DHCP server.

In case of Centos enter following to enable DHCP on server boot :

```
abgeek@geeknepal:~$ chkconfig --levels 235 dhcpd on
```

Note : Sometime we have to configure default gateway. So do as following :

```
abgeek@geeknepal:~$ vi /etc/sysconfig/network
```

and edit as below

```
NETWORKING=yes
```

```
HOSTNAME=geeknepal.com
```

```
GATEWAY=192.168.1.1
```

and restart the network service

```
abgeek@geeknepal:~$ service network restart
```

4. *Bandwidth Management*

Bandwidth management is one of the most important task in any organization. As the bandwidth of organization is limited , so the network administrator has to utilize the bandwidth properly among all users. He must implement efficient bandwidth managing actions.

In sense of Network layer, bandwidth management is a process of managing and controlling packets,traffic flowing through a network. Bandwidth management is measured in bits per second (bit/s) or bytes per second (B/s). There are various bandwidth managing algorithms. Some of the popular of them are :

Token bucket

Hierarchical Token bucket (HTB)

Leaky bucket

First In First Out (FIFO)

Hierarchical Fair Service Curve (HFSC)

We'll do with both FIFO and HTB algorithms.

Traffic Shaping

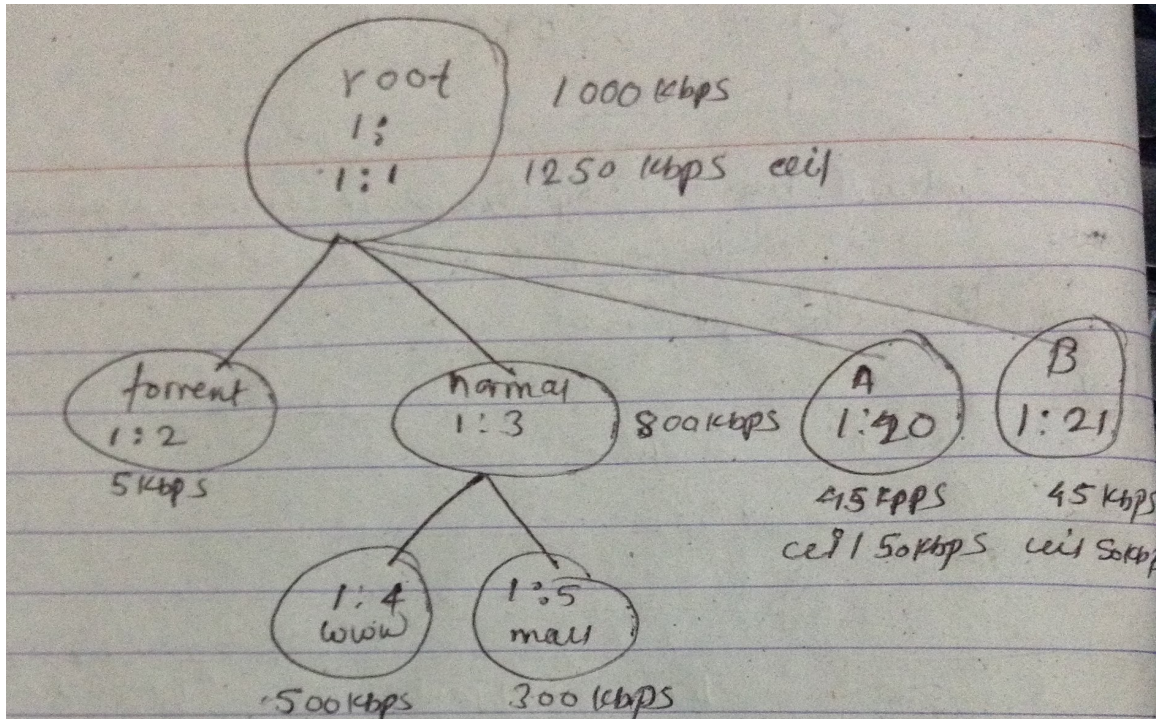
Traffic Shaping (Bandwidth Shaping or Packet Shaping) is an attempt to control network traffic by prioritizing network resources and guarantee certain bandwidth based on predefined policy rules. Traffic shaping uses concepts of traffic classification, policy rules, queue disciplines and quality of service (QoS). Traffic shaping lets you (1) control network services, (2) limit bandwidths and (3) guarantee Quality Of Service (QoS).

Queue Discipline

A queue discipline (qdisc) is rules that determine the order in which arrivals are serviced. It is like the algorithm given above.

HTB uses the concepts of tokens and buckets along with the class-based system and **filters** to allow for complex and granular control over traffic. With a complex borrowing model, HTB can perform a variety of sophisticated traffic control techniques. One of the easiest ways to use HTB immediately is that of shaping.

Lets implement a simple bandwidth management for our network using HTB.



Consider the diagram above. At first we have a root node that have bandwidth of 1000kbps and ceil value 1250kbps. Ceil is the value that can be borrowed from other nodes. The root node will be the main node from which all child node will get their bandwidth.

At first we have to define the main root node.

Enter following command :

```
tc qdisc add dev eth1 root handle 1: htb default 12
```

Then we have to attach queuing discipline to the main node. We are assigning class id 1:1 to root node with bandwidth 1000kbps and ceil value 1250kbps.

```
tc class add dev eth1 parent 1: classid 1:1 htb rate 1000kbps ceil 1250kbps
```

Now lets create a child node for torrent. It will have bandwidth 5kbps and will be used to allocate a blocked user.

```
tc class add dev eth1 parent 1:1 classid 1:2 htb rate 5kbps
```

Now create another node with 800kbps and classid 1:3

```
tc class add dev eth1 parent 1:1 classid 1:3 htb rate 800kbps
```


Now create a node for user A and B

```
tc class add dev eth1 parent 1:1 classid 1:20 htb rate 45kbps ceil 50kbps
```

```
tc class add dev eth1 parent 1:1 classid 1:21 htb rate 45kbps ceil 50kbps
```

From the given command we are assigning 1:3 i.e. 800kbps bandwidth to youtube IP.

```
tc filter add dev eth1 parent 1:0 protocol ip prio 1 u32 match ip src 74.125.235.13/32 flowid 1:3
```

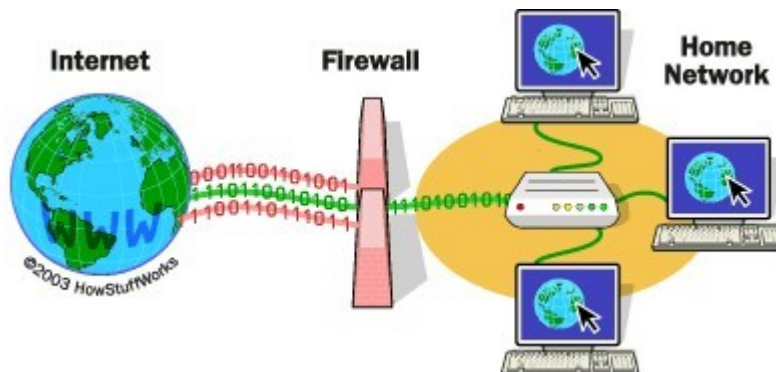
Now to assign 1:20 class based bandwidth to user of ip 192.168.1.11 enter :

```
tc filter add dev eth1 protocol ip parent 1:0 prio 1 u32 match ip dst 192.168.1.11 flowid 1:21 #
```

In this way bandwidth can be allocated using tc in Linux server.

5. Firewall

Firewall is like the wall of our house that prevents us from external attacks and also helps to filter various rules as per our requirement. Firewall Controls the incoming and outgoing network traffic based on applied rules. It helps to create trusted and secured network. It also prevents hackers, viruses, and worms that try to reach your computer over the Internet.



Iptables is an extremely flexible firewall utility built for Linux operating systems. It is a linux kernel tool. Iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action.

iptables uses three different chains: input, forward, and output :

- INPUT - All packets destined for the host computer. For example, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.

- OUTPUT - All packets originating from the host computer.
- FORWARD - All packets neither destined for nor originating from the host computer, but passing through (routed by) the host computer. This chain is used if you are using your computer as a router.

Lets start using iptables

abgeek@geeknepal:~\$ iptable -L -v

It will list all iptables rules. By default there may not be any rule.

abgeek@geeknepal:~\$ sudo iptables -L INPUT -n --line-numbers

It will list input rules with line numbers

To delete a rule with line number 4

abgeek@geeknepal:~\$ iptables -D INPUT 4

By default in your server , you do not want any other to connect with your server,so enter following to drop all :

```
iptables --policy INPUT DROP
iptables --policy OUTPUT DROP
iptables --policy FORWARD DROP
```

Note : Accept – Allow the connection.

Drop – Drop the connection, act like it never happened. This is best if you don't want the source to realize your system exists.

Reject – Don't allow the connection, but send back an error. This is best if you don't want a particular source to connect to your system, but you want them to know that your firewall blocked them.

Lets drop or block a single IP address :

abgeek@geeknepal:~\$ iptables -A INPUT -s 192.168.1.11-j DROP

It will block 1.11 IP.

abgeek@geeknepal:~\$ iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP

It will block ssh port. You can replace ssh with number 22

Now save all iptables rules by :

abgeek@geeknepal:~\$ sudo /sbin/iptables-save

To delete all iptables rules :

```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
```

Now let's block www.facebook.com in your server.

1. At first we have to find IP address of www.facebook.com server

```
abgeek@geeknepal:~$ host -t a www.facebook.com
```

Output may be : 173.252.110.27

2. Then we have to find CIDR (Classless interdomain routing) for given site. (because the site may be hosted in multiple servers)

```
abgeek@geeknepal:~$ whois 69.171.228.40 | grep CIDR
```

CIDR: 173.252.64.0/18

It will print the subnet.

3. Now drop the subnet with iptables

```
abgeek@geeknepal:~$ iptables -A OUTPUT -p tcp -d 173.252.64.0/18 -j DROP
```

Also domain name can be used to block the site

```
abgeek@geeknepal:~$ iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
```

```
abgeek@geeknepal:~$ iptables -A OUTPUT -p tcp -d facebook.com -j DROP
```

In this way you can block a site using iptables.

You can set more stronger firewall with iptables. Keep on exploring it.