Linux Notes

Subject: System and Network Administration
Class: BSIT (6th)
Teacher Name: Miss. Umaira Nazar Hussain

Session No :1

(Basic Linux, OS introduction)

1. **Define Linux:**

   Linux is an operating system very much like Unix. Linux is an open source and community -developed operating system for computers, server, mainframes and embedded system. Users can modify and create the variation of source code.

2. **Define Windows:**

   Windows is a client side mostly used operating system.

3. **Types of Windows:**

i.   Client side:

   (Windows 98, windows XP, Windows 8, Windows 10)

ii.   Server side

   (Windows 2003,2008, 2012,2016,2019)

4. **Benefits of Linux over windows:**

i.   Linux is a virus free operating system
ii. Linux is free source operating system

5. **Benefits of windows over Linux**

i.   It is very simple and straightforward to use.
ii. Windows is extensible and portable.

Session No : 2

(Linux installation, directory structure, Basic commands User &Group management, Network Monitoring Tools)

1. Linux installation & Directory Structure:

Following parameters should be set for Linux installation:
  i.   Software Selection (Select GUI server(KDE))
  ii. Installation Destination (configure disk partitions)
        Root (top level directory)
        /Boot (operating system)
         SWAP(Memory)
         /Home (user data)
  iii. Network &Host Name

2. Basic Commands:

su: su command is used to switch from normal user to root or super user.
cd: this command is used to change the directory.
cd-:   This command is used to go to previous location.
cd..   Go one step back
cd.. /..   Go two step back
Pwd .   Show the present working directory.

Command to create files:

touch:

Notepad files can be created by using touch keyword for example:
touch file1.txt
txt is an extension for Notepad file.

Vim:

when a file is created by touch command we can write anything in it by using vim editor.

Vim file1.txt
Press i to enter in insert mode and write anything in file.
:wq! Come back to the terminal.

Cat>file1:

by using this command file also created, no need to use vim editors.

Command to combines two or more files in another file:

Cat file1 file 2> newfile

Create directory or folders:

mkdir: this command is used to create directory or folder for example:

mkdir mysoftwrae

Command to remove files and directory:

rm: used to delete files for example:

rm file1

rm-fr*:   remove file forcefully or recursively.

Copy files:

cp: this command is used to copy files
Cp file1.txt   xyz.txt

Remove directory:

rmdir : is used to remove directory for example :
rmdir my software

How to filter data:

|grep :   we can use |grep command to filter data or get specific data for

example:
Cat/etc/passwd|grep student

3. Process management:

ps: see the list of files running in system.
ps aux: see the detail of ran time process.
ps -ef: more detail of process.
ifconfig: provide name and IP address of a system.

4. Monitoring Tools:

netstate:describes network related information.
netsate -a|more: is used to list all port.
netsate -at|more: is used to list only Tcp port.
netsate -au|more: is used to list UDP port.

5. How to restart system services?

The following command are used to restart the system services:
  i.   Systemctl restart network services
  ii. Systemctl restart Tcpd services
  iii. Systemctl restart samba services
  iv. Systemctl restart http services

6. User and group management:

1. User:

 There are two types of user in Linux:

i. Normal User:

A normal user can only access what they have or have been given the permission to run.

ii. Root User:

The root user is allowed to access all files and program in the system,

whether or not owns them. Root user also called superuser.

Useradd, Usermod and Userdel commands:

Useradd-m:
    this command is used to add user and user home directory for example:

useradd-m user1

Or we can also add user by using following command:

useradd user1

usermod:
   this command is used to modify the user account.

usermod-c:
    comment any user.

usermod-G group1 user1:
        add user 1 in group1.

usermod-L:
   to lock the user account for example:
usermod-L user1

usermod-U:
    to unlock the user account for example:
usermod-U user1
Passwd user1

Userdel:
  this command is used to delete user account for example:
userdel user1

2. **Storage place of user data:**

Cat/etc/shadow

3. Group management:

groupadd:
by using groupadd command groups are created for example:

groupadd group1

groupmod : groupmod -n group1 group

groupdel : groupdel group1

7. Software management:

Software in Linux called rpm, packages.

RPM:
Is used to install, uninstall maintain, verify and validate all the packages on system.

rpm-qa Command to list all the installed packages on system

rpm-qa|grep: query a specific software to check whether it install or not fir example:
rpm-qa|grep ssh

rpm-qi ssh:
query to show the information of installed packages.

rpm-ivh:
Install rpm (we can install any package with this command for example rpm-ivh createrepo)

I: install
V: verbosely

rmp-Uvh/media/:
update rpm.

Session No: 3

((Software management (Yum Server), FTP Server, NFS Server, SAMBA Server)

Yum:

RedHat provide yum package to make repository to resolve the dependency issue. Help rpm to install any packages

dev/cdrom   : Default path of ISO images when they mounted on CDROM.

Server:

Server's installation consists of following steps:

1. Installation of server RPM
2. Server configuration (configuration exist at specific path)
3. Server services restart
4. Server services enable
5. Allow server services in firewall
6. Server testing

Yum configuration:

cd/etc/yum.repos.d/: Directory of yum server placed at yum.repos.d location
  vim rhel.repos: is used to create yum repository.
By using vim editor following parameters should be defined:
[RHEL 7]
Name=Redhat7 yum server
basehrl= file:///mysoftware/
enable=1
gpgcheck=0 (noneed to check the yum repository license)

FTP:

File transfer protocol is used to transfer files within or between machines.

1. FTP installation:

yum install vsftpd: is used to install ftp server.
/var/ftp/pub **:** is directory which automatically created by ftp after installation

2. Server services restart:

systemctl start vsftpd. services: is used to start the services of ftp.
systemctl status vsftpd. services: is used to check the status of ftp server.

3. Server Services Enable:

Systemctl enable vsftpd. services: is used to enable the ftp services forever.

4. Allow Server Services in Firewall:

Firewall-cmd--permanent--add.services=ftp: is used to allow the server in firewall for security purposes.
Firewall-cmd--reload: is used add this rule in ftp directory for further traffic.

5. Server Configuartion:

vsftpd.config : is used to configure ftp file for example:
cd/etc/vsftpd/ is used to enter in vsftpd directory than configure file by using vim editor
vim vsfptd.config.

6. **Server services restart:**

systemctl restart vsftpd. services: after configuration all the ftp services should be restart.

NFS Server:

Linux to Linux communication

1. Installation:

yum install nfs: is used to install NFS server.
yum install nfs*: is used to install all the rpm which come along with nfs or have matched files.

2. Configuration:

etc/export : is used to configure nsf
Vim/etc/export : by using vim editor we insert the following data to configure the network (nfs server)
nfs-share: is used to share files with other machine for example
nfs-share i92.168.0.22 (ro sync)
exportfs-r : is used to check the configuration files and detect problems

3. Start services

systemctl start nfs -server.services: is used to start the NFS services.
systemctl status nfs -server.services: is used to check the status.

4. Server Services enable:

systemctl enable nfs -server.services: is used to enable nfs services at run time
showmount-e   : A client side nfs send request to server side nfs to show all the files for example:
showmount-e 10.53.14.134   client send request to the particular server   by using its ip address
systemctl restart nfs -server.services: after configuration. we will have to restart nfs services .

5.**Allow Server Services in Firewall.**

Firewall-cmd--permanent--add -services=nfs: this command is used to allow firewall in nfs server for security purpose.
Firewall-cmd--permanent--add -services=mountd

Firewall-cmd--permanent--add -services=rpc-bind
Firewall-cmd--reload: add this rule to nfs directory for further use.
mount -t nfs/nfs-share/shared-nfs- folder/: is used for mounting between two machine share data by using nfs protocol for example:
  mount -t nfs 10.53.14.134/nfs-share/shared-nfs- folder/
df-H: is used to see the list of devices mounted on machine.

SAMBA Server:

(Linux to window communication)

1. **Installation**

yum install samba*: is used to install all the samba rpm.

2. **Configuration**

Like NFS in   samba we need to create folder for configuration for example mkdir samba-share.We add several user and one group and than add user to that group for example
Useradd   user1,useradd user2 ,useradd user3, groupadd BSit, usermod -G BSit user2 user3
cd/etc/samba.   path   of samba file for configuration
vim smb.conf: smb .conf is samba configuration file ,by using vim editor we will insert the following data for file configuration:
[share]
Comment = sambashare
Path   = /samba-share
browseable=yes
valid users= student1 student2&BSit
hosts allow = 10 .53.14.0/24
Writable = yes
Write list = student1 &BSit
guest = ok
read only =   no

testparm: used to validate the configuration file
firewall-cmd--permanent--add-service=samba: Is used to allow firewall in samaba services for security purposes.

firewall-cmd--reload: is used to add this rule for further traffic.
Systemctl start samaba.services

Logs:

/var/log/messages: this command is used to detect problems and troubleshoot the network.

Session No: 4

(Apache Server, DHCP Server, IP Table, Securing Network Traffic, Active Directory)

1. Apache server:

Is also called web server. All the running website must place on internet so everyone can access them or browse them for specific purposes. Web servers are configured to place the website publicly.

2. Installation:

yum install http*: is used to install all the rpm which come along with http name.
   Firewall
firewall-cmd--permanent--add-services=http: is used to allow firewall in http services.
firewall-cmd--reload: Is used to add this rule for further traffic.

3. Services:

systemctl start httpd .service: is used to start the http services.
systemctl enable httpd .service: is used to enable http services.
systemctl status httpd .service: is used to check the status,check whether or not the is active.

4. Configuration:

httpd.conf   is http configuration file.
cd/etc/httpd/conf: is path of configuration file.
vim httpd.conf :   add some configuration by using vim editor for example
  <virtualHost 10.53.14.134:80>
ServerAdmin root@studentlab.com
ServerAdmin www.studentlab.com
documentRoot /var/www/html
</virtualHost >

index.html: the first default page website is store with index.html name.And we open it with vim editor for example:
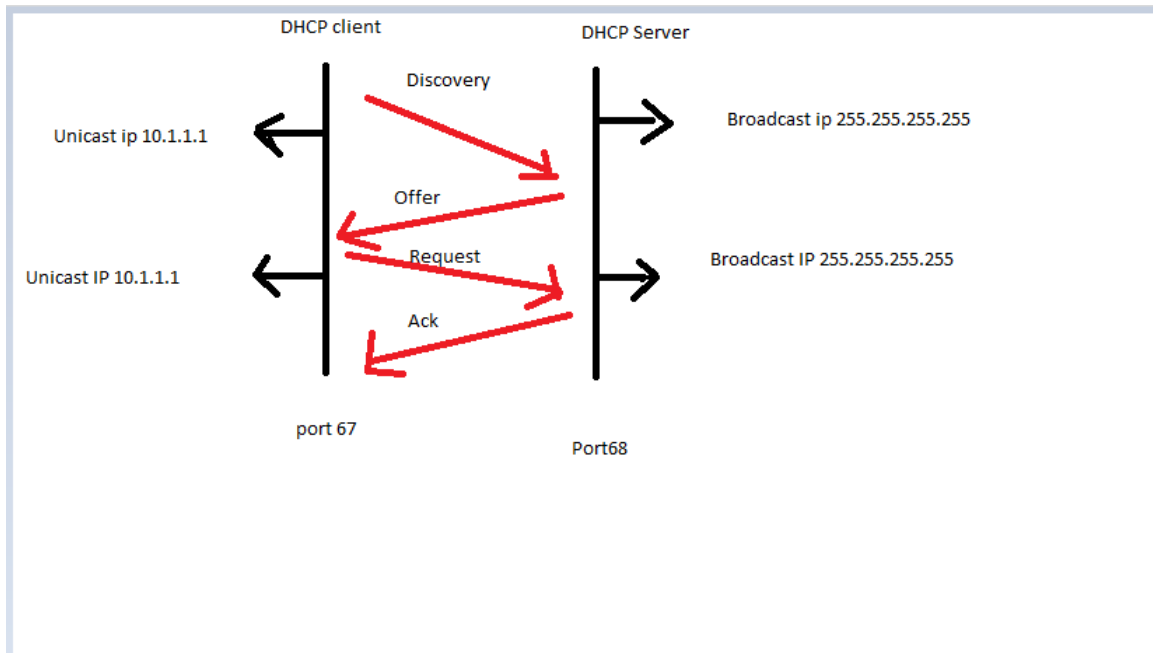
vim index.html

hostname www.studentlab.com: is used to set host name.

DHCP:

The communication between machines is done only when the sender machine know the ip address of destination machine. DHCP create a pool of ip address

Process

First of all, the client discovers whether the DHCP server is available on network or not.

DHCP server offer a IP address to client.

Then client request a particular address from a DHCP server.

Finally DHCP server assign the requested IP to a client a send acknowledgment.

DHCP Installation:

yum install dhcp*: Install all the rpm which come along with dhcp name.
Firewall
firewall-cmd--permanent--add-services=dhcp: Allow firewall in dhcp services.
firewall-cmd--reload: add this rule for further traffic.

Configuration:

dhcpd.conf: is a dhcp configuration file.
cd/etc/dhcp: is a path of configuration file.We can configure the file by using vim editor for example:
vim dhcpd.conf
Subnet 198.168.100.0 netmask 255.255.255.0
Range198.168.100.101 198.168.100.150

Services:

systemctl start dhcp.services: is used to start services
systemctl enabe dhcp.services: is used to enable services
systemctl status dhcp.services: is used to check status

<u>DNS SERVER:</u>

1. **DNS History:**

    Concept of DNS was introduced during second world war to enable communication between machine placed geographically. DNS is a classical naming system for translating host name to IP address. Machines usually understand digits, by nature human can easily understand and remember names. DNS server fill this gap and convert the IP address to name and name to IP address.
  Internet is one of the best example of DNS

2. **Host file:**

    Host file contain lists of IP address of different machines. Host file

performs a name to IP address mapping and was used on early computer network for name resolution before DNS developed. But host files are difficult to manage when internet scope became wide and updating entries in host file is not easy the whole record needs modification.

```
PC-1        192.168.1.101
PC-2        192.168.1.102
PC-3        192.168.1.103
PC-4        192.168.1.104
PC-5        192.168.1.105
```

Host file

To overcome this problem, the concept of DNS was introduced
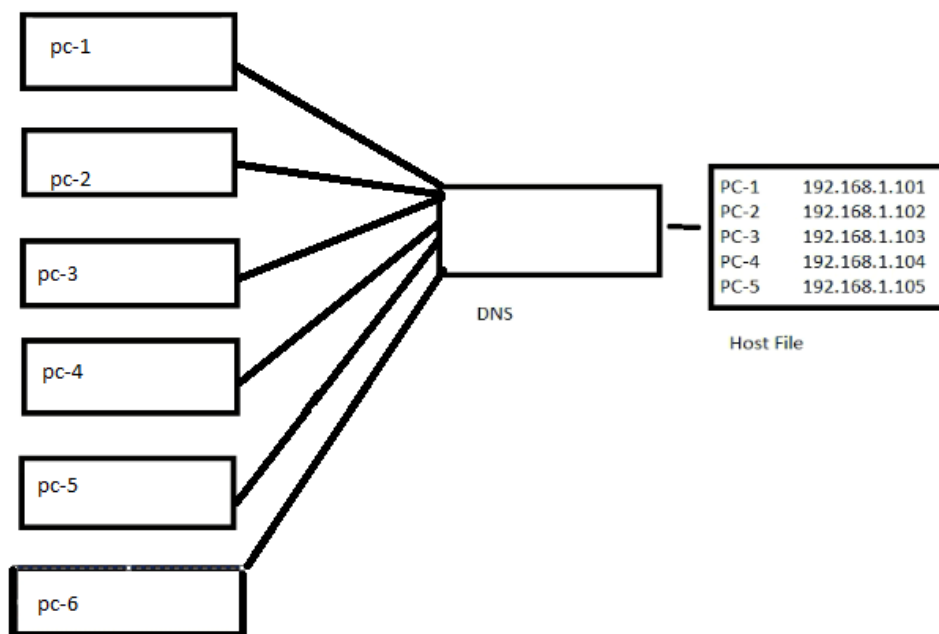
If PC-1 want to communicate with PC-4 .It will send request to DNS for PC-4   address .DNS check the requested address in address pool and then send it to PC-1.DNS gives the IP address of websites.

DNS Hierarchy

When the DNS became too large management become more complex to overcome this problem the concept of DNS segregation was introduced.

Hierarchical Domain Tree
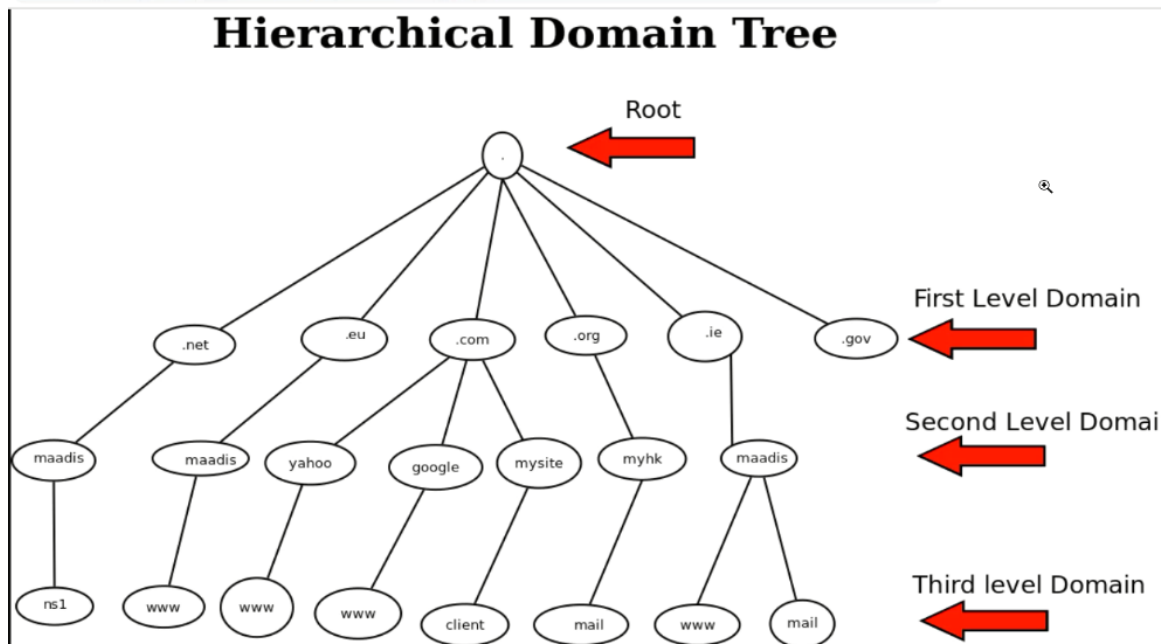
1. **Root Level Domains:**

It is at top, by default a. is always placed at the end of a domain, there are 13 root servers and each server has many of its backup copies in different parts of the world.

2. **TOP level domain**

A top-level domain is the label at the right end of the domain name, after the dot. There are two types of top-level domains, generic and country code.

3. **Second-Level Domains**

A domain is a second-level domain if it is contained within a top-level domain. A second-level domain is the label immediately to the left of the top-level domain, separated by a dot. It is also called authoritative server.

4. **Third level domain**

Third level domain follow the following sequences:
host1 >.   google >.   Com >.
Also called fully qualified domain name.

QUERIES:

There are two types of query in DNS.
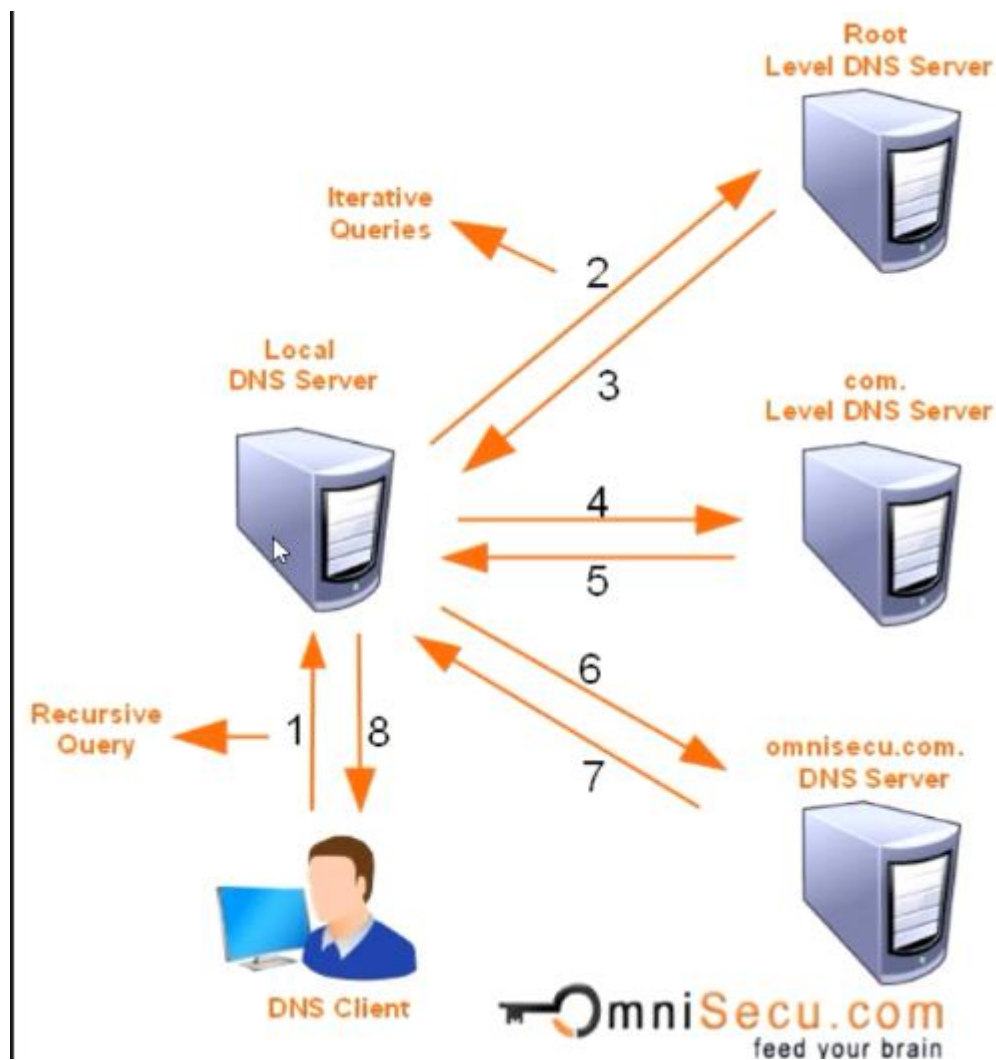
1. **Recursive query:**

  Recursive DNS queries occur when a DNS client requests information from a DNS server that is set to query subsequent DNS servers until a definitive answer is returned to the client. In short words a query from DNS client to local DNS server is called recursive query.

2. **Iterative query:**
A query from local DNS server to Root level DNS servers is called iterative query.
In iterative client is responsible for sending query to different servers until query is resolved.

DNS types:

1. **Authoritative DNS:**

Authoritative DNS is the final holder of the IP of the domain you are looking for a server who has the ability to resolve different queries.

2. **Cache DNS server:**

  This server stores the most frequently used queries for DNS client. When client request for some specific IP address cache server first check it in its own storage and provide the requested IP address.
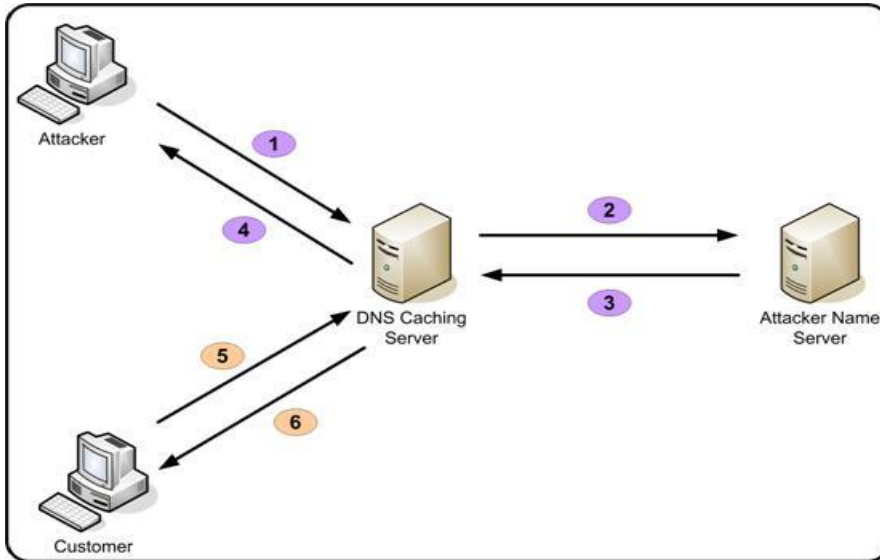
3. Forwarder DNS:

Forwarder server is only responsible for describing the directions of queries and used to forward DNS queries for external DNS names to DNS servers outside the network.
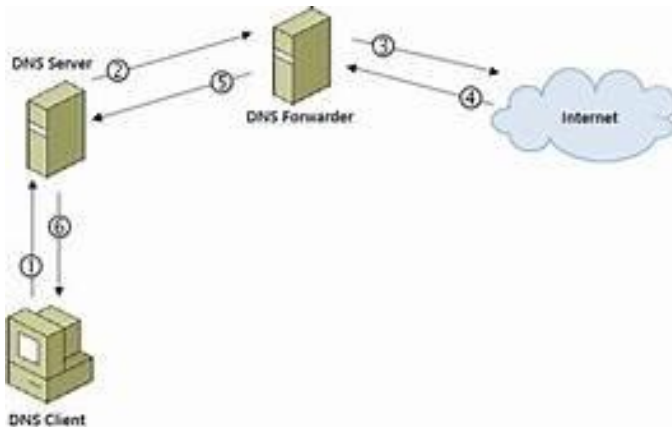
DNS ZONES:

Both of the DNS zones are types of host file

1. Forward zones

Forward zones -> name to IP conversion
PC-1 198.168.100.11
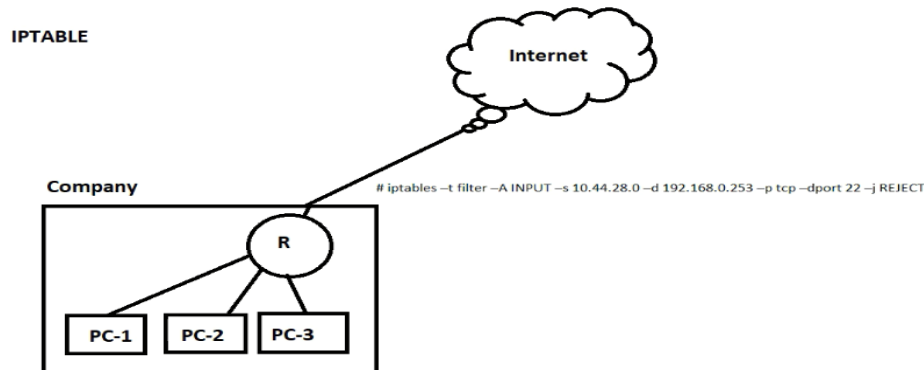
2. Reverse Zone

Reverse Zone -> IP to name conversion
198.168.100.11 PC-1

IP Tables:

IP tables might contain multiple tables and tables might contain multiple chains and chains contain multiple rules where rules are defined for incoming and outgoing packets.

Structure of IP Tables
IPTables->Tables->Chains->Rules

Table name:

-t   filter,NAT, Mangle

Chain Name:

-A   Append
-i   Insert

-D   Default
-R   Replace

Chain of Filter Table:

Filter   > INPUT,OUTPUT,FORWARD

Possible conditions:

Conditions are operated with AND operator.
-s   Source
-d   Destination
-p   protocol
!   Except this
--sport   Sourse Port
--dport   Destination Port
-i   Incoming Ethernet
-o   outgoing Ethernet

Action/Decision:

Actions are represented with -j.
Accept
Reject
Drop

Example of IP Tables:

Add accepting rule for incoming traffic in filter table for a packet which source is 10.53.24.0 and destination is 198.168.0.253 bu using tcp protocol and coming on 22 port.

IPtable -t filter -AINPUT -s 10.53.24.0 -d 198.168.0.253 -p tcp -dport 22 Accept

Active directory:

  Active directory provides a central point of administration within Windows. But for Linux and Unix, user identities may reside on individual server or in separate identity silos, complicating operations and compromising security.

Server manager option differentiate the windows server from other windows (client side Windows)
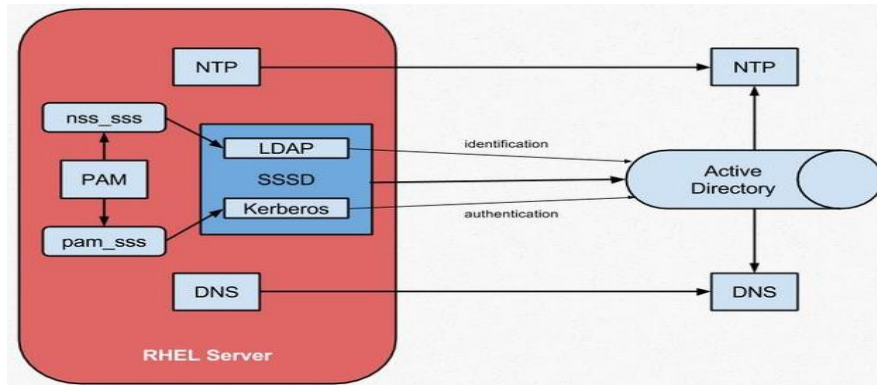
Active directory process consists of following steps:

1. Windows server convert into Domain controller.
2. Join client machine to Domain controller.
3. Create a policy in Domain controller and apply it to clients.

Session No: 5
(RAID)

RAID:

Stands for redundant array of independent disks. RAID is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purpose of data redundancy, performance improvement or both.

RAID		Minimum Physical Drives	Fail PDs Allowed	Method	Capacity	Read Speed	Write Speed	Good Usage
0		2	NONE	Striping (speed)	100%	Excellent	Excellent	High throughput workstation
1		2 min & max	1	Mirroring (redundancy)	50%	Very good	Good	OS, apps entry level
5		3	1	Striping & distributed parity (fault tolerance)	n-1 (67-94%)	Very good	Good	Data, web/media server
6		4	2	Striping with dual distributed parity	n-2 (50-88%)	Good	Good	High fault tolerance
10		4	1 per mirror set	Striping across mirrors	50%	Very good	Good	Database, file, mail servers
50		6	1 per R5 set	Striping across R5 arrays	n-2 (67-94%)	Excellent	Very Good	Database, file, mail servers
60		8	2 per R6 set	Striping across R6 arrays	n-4 (50-88%)	Very good	Good	Critical data

Choosing the Right RAID Level

RAID 0:

Also called no raid or stripping. Raid o obtained maximum capacity (full capacity.). RAID 0 has no failure support. The disks range in RAID 0
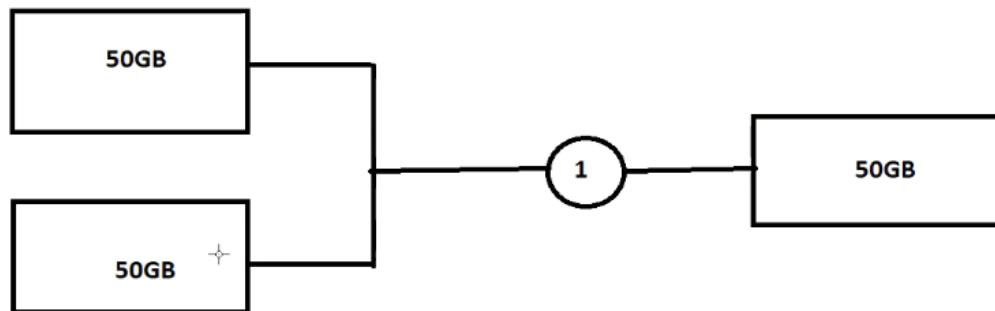
from minimum 2 to maximum 32disks. Data are broken into chunks, called "stripes".

Why we use Raid 0:

We used RAID 0 in application that require high performance and are able to tolerate lower reliability.

RAID 1:

RAID 1 also called mirroring. RAID 1 obtained 50% capacity. RAID 1 support failure. RAID 1 consist of 2 disk.

IF one disk fail the failure must be on that disk. The other disk operates without any concern of the failure disk and provide data. Mirroring is the replication of data between two drives.

USES of RAID 1:

We used RAID1 for applications that require high performance and high availability.

RAID 5:

RAID 5 also called Single Parity Raid and consist of minimum 3 to maximum 32 disks. RAID 5 provide N-1 capacity and also support failure.
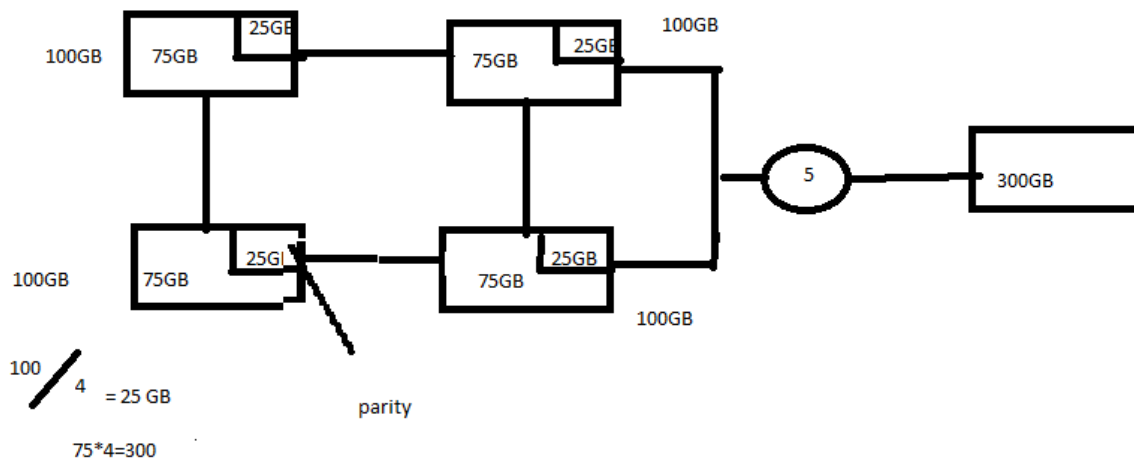
The above diagram proved N-1 capacity claim. The 75 GB data in each disk is compressed into the 25gb parity of next drives so the RAID 5 support failure. Suppose that one disk failed but the total capacity remains unaffected because the data of the failure drive compressed in the parity of next drive.

Uses of RAID 5:

RAID 5 is most commonly used RAID in business and is used to increase performance and reliability of data storage.

Risk of RAID 5:

If two drives failed at the same time, then the RAID 5 will be in risk and the data will be lost. The RAID 5 provides one disk failure support.

RAID 6:

Also called dual parity RAID. RAID6 consist of minimum 4 or maximum32 disks and also support 2 disk failure. RAID 6 provides N-2 capacity.
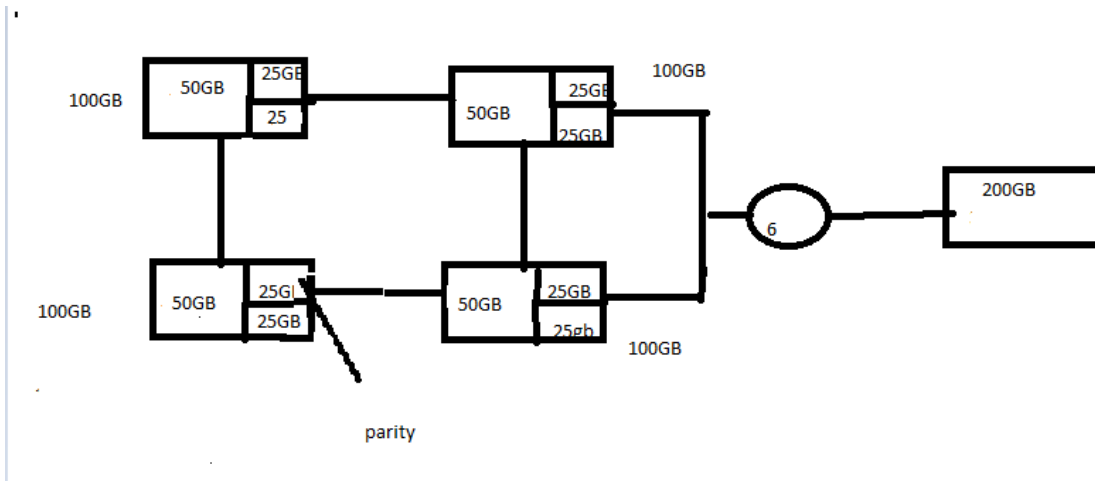
In RAID 6 the 50% data of one drive is compressed into the parity of next two drive (25% compressed in parity of one disk and the remaining 25 percent into the parity of next disk). So the claim of N-2 capacity and 2 disk failure support is proved by above diagram.

RAID 6 Uses:

RAID 6 is the most commonly used RAID and used for application that require failure tolerance.

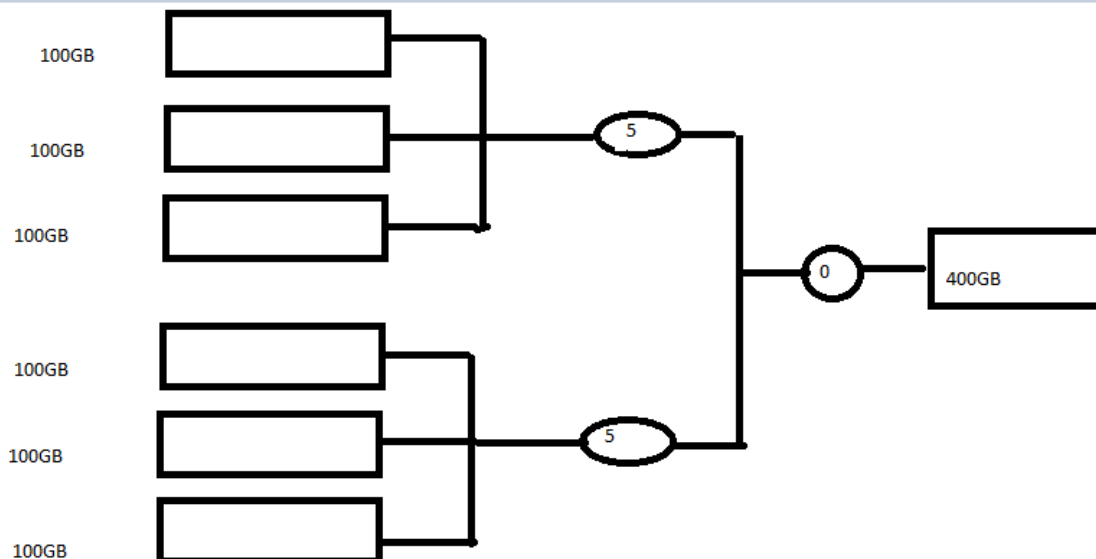## RAID 10:

Is the combination of raid 1 and 0. RAID 10 consist exactly 4 disks? RAID 10 provides 50% capacity and also provides failure support.
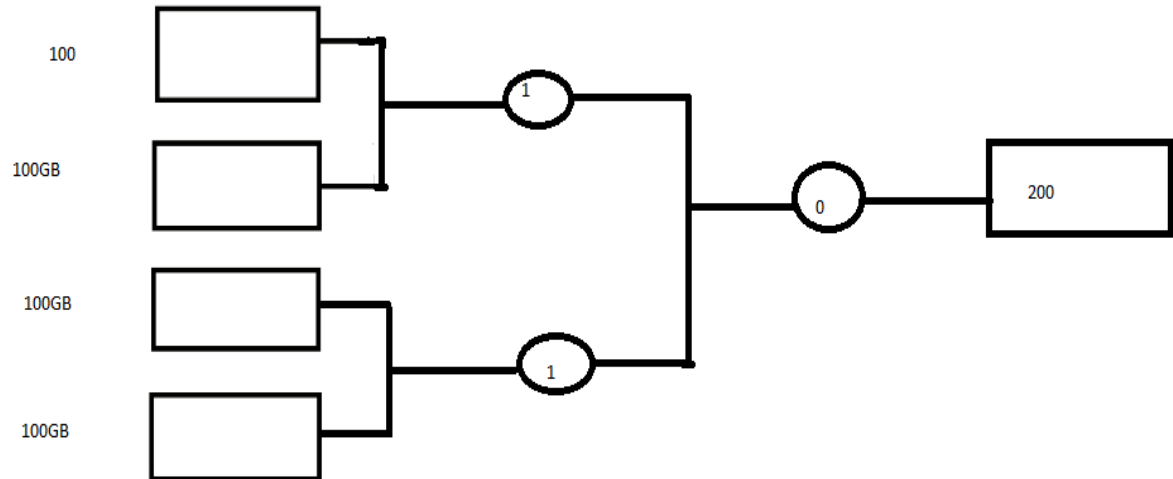
RAID 50:

Is the combination of raid 5 and 0. RAID 50 consist of exactly 6 disks? RAID 50 provides N-1 storage capacity and also support failure.

RAID 60:

Is the combination of raid 6 and raid 0? RAID 60 consist of exactly 8 disk. RAID 60 provides N-2 storage capacity and also provide failure support. RAID 60 improve performance.