*****Difference Between TCP-IP & UDP Protocol*****

	TCP-IP(Transmission Conrol Protocol)	UDP(User Datagram Protocol)
1.	ftp, http, smtp, ssh, email	dns, nfs, tftp, telnet, voice call
2.	which application have Login	which application don't ask for Login
3.	provide acknoledgement, rsync	don't provide acknoledgement, rsync
4.	Highly secure because no loss of Packet & Data of	Highly Unsecure because loss Packet & Data
5.	file transmitssion speed bit of less than UDP TCP	file transmission speed more than

eht 0 path in RHEL -> vi /etc/sysconfig/network-scripts/ifcfg-eth0
eth0 path in Ubuntu -> vi /etc/network/interfaces

***How to assign Temporary IP Address to machine
-> ifconfig ehto 192.168.3.40 netmask 255.255.255.0 gateway 192.168.3.1

***How to assign Parmanant IP Address to machine
-> vi /etc/sysconfig/network-scripts/ifcfg-eth0 (entry)
DEVICE=eth0 (The type of network interface device)
IPADDR=192.168.3.40
NETMASK=255.255.255.0
ONBOOT=yes (This interface is activated at boot time.)
GATEWAY=192.168.3.1

-> setup (Asign IP Address to used the setup tool or command)

*****NFS(Network File Shairing) *****

Port - 2049
Service - /etc/init.d/nfs
Confige file - /etc/exports

Network File System (NFS): Is a nfs server client protocol used for sharing files and directories between Linux / Unix to Unix/Linux systems vise versa. It is a popular distributed filesystem protocol that enables users to mount remote directories on their server.

- Centralized Management of Files
- Everyone can access same data
- Secured with Firewalls and Kerberos
- Reduce Storage Cost and Easy to use

Server side

-> rpm -qa |grep -i nfs
-> yum install nfs-* -y
-> yum install nfs-utils* -y ----rhel 7
-> /etc/init.d/nfs restart
-> systemctl start nfs-server ----rhel 7
-> chkconfig nfs on
-> systemctl enable nfs-server ----rhel 7
-> netstat -tulap |grep 2049
-> vi **/etc/exports** (entry)
/home/DataShare *(ro,sync) **(or)**
/home/PublicData 198.168.1.0/24(rw,sync) --->only within a organisation
-> chmod 770 /home/PublicData
-> /etc/init.d/nfs restart

Client side

-> ping 192.168.1.100
> showmount e <nfs-server-IP> ---->shwon nfs-server share data
-> mkdir /share
-> mount 192.168.1.100://home/PublicData /share (entry all 6 feild in fstab file)
-> vi /etc/fstab (entry)
192.168.1.100:/home/PublicData /share nfs defaults 0 0
-> mount -a
-> iptables stop
-> nfsstat (To monitor NFS Server)

*****How to allow dhcp parmanantly in firewall**

-> firewall-cmd --parmanent --add-service=nfs
-> firewall-cmd --parmanent --add-port=2049
-> firewall-cmd --reload

*****FTP(File Transfer Protocol)*****

Port - 20/21
Service - /etc/init.d/vsftpd
Config file - /etc/vsftpd/vsftpd.conf

- File Transfer Protocol (FTP) is a most popular way to transfer files from one machine to another machine across a network in heterogeneous environment.
- If you take an example of NFS (Network File system) it has an restriction to it can't be access from other platform such as windows. FTP server does not have such a restriction it can be accessed from Linux OR windows OR Osx.
- ftp having two type of user
  1. Application User – all application user are three type category
  a. anonymous user – if any file for public used like ganna.com users all are download song without any login activity if you not need anonymous user then
  ->vi /etc/vsftpd/vsftpd.conf (entry)
  anonymous = yes
  b. local user – which are present in server database in /etc/passwd file which are Linux user of that server.
  c.virtual user – which user does not exist in server database.
  2. System User - all system user's havin /sbin/nologin shell and userid v6 under 99 and v7 under 199
- ftp are two type - 1. Active ftp 2. Passive ftp
- home directory of ftp is **/var/ftp**
- **now days we used sftp – secure file transfer protocol using Port-22 that why this is very secure file transmission.**

Server side

-> rpm -qa |grep -i vsftpd
-> yum install vsftpd-* -y
-> /etc/init.d/vsftpd start
-> /etc/init.d/iptables stop
-> systemctl start vsftpd ----rhel 7
-> chkconfig vsftpd on
-> systemctl enable vsftpd ----rhel 7
-> netstat -tulap |grep 21
-> vi /etc/vsftpd/vsftpd.conf (entry)
anonymous_enable=NO
Allow local users to login in vsftpd.
local_enable=YES
Enable write access to local users.
write_enable=YES
Uncomment the line chroot_local_user
chroot_local_user=YES
Enable writable chroot.
allow_writeable_chroot=YESonymous_
-> ls -d /var/ftp (here we put all shared directory or folderand files)

Client side

-> ftp 192.168.1.10

ftp>mget <file name>	(to download file on server)
ftp>mput <file name>	(to upload file on server)
ftp>help	(for more options)
ftp>bye	(logout on ftp server)
-> ping 192.168.1.10	(ftp server ip)
-> ftp://192.168.1.10	(Open Any Browser enter url)

*****How any linux user access ftp server home directory**

Server side

-> ls /home/pravin

-> cp /var/ftp/* /home/pravin

-> setsebool -P ftp_home_dir=1	**or on** (selinux deny access home directory and how to ignore that we used this command)
-> vi /etc/vsftpd/vsftpd.conf	(entry)
anonymous_enable = no	
chroot_local = /home/pravin	(chroot mean only show that path info. Not outside of that path)

-> /etc/init.d/vsftpd reload

-> kill -1 <Pid of vsftpd> (**or used HUPSIGNAL = 1 for reload)**

Client side **(Filezilla used at client side which free source)**

-> open browser type in url - ftp://192.168.1.10 --->server ip

enter userID & password*

****SAMBA*****

Port - 139, 137
Service - /etc/init.d/smb & /etc/init.d/nmb
Confige file - /etc/samba/smb.conf

- We can also call this as CIFS (Common Internet File System) shares, Sharing the directories & Folders across the corporate network and Sharing the Directories / Folders from Linux to Windows and Windows to Linux wise versa we have to use SMB (samba) protocol.
- Samba is not only used for sharing directories, we can also use it for sharing printing services (printing server).
- SAMBA is file sharing server used for shared file both client machine linux and windows means Hetrogenous Enviroment. **cif , nfs, samba all are file system used over network.**
- Fully Secured shares using user authentication
- Samba configure file contain Two Session
  1.global session 2. shared session

Server side

-> rpm -qa |grep -i samba
-> yum install samba-* -y
-> /etc/init.d/smb restart port - 139
-> /etc/init.d/nmb restart port - 137
-> systemctl start smb nmb ----rhel 7
-> chkconfig smb nmb on
-> systemctl enable smb nmb ----rhel 7
-> netstat -tulap |grep 137
-> chmod 777 /opt/SharedData/*
-> adduser pravin (samba required VLU user means Valid Linux User)
-> smbpasswd -a pravin (passwd for samba user & all samba user stored in /etc/samba)
-> vi /etc/samba/smb.conf (enrty in last line)
[**common**] (Share name which used on client side)
path = /opt/SharedData ((Directory path which directory you would like to share))

[**share**] (Share name which used on client side)
comment = SharedData (Directory path which directory you would like to share)
path = /SharedData
writable = yes (Providing Write permissions to share (this permission will be overwritten by Actual Directory permissions)

valid users = pravin (User Name which user we are providing the access)
-> testparm **(check or refresh samba configration file in system)**
-> service iptables stop

Windows machine Client side

-> Open Run (entry)
-> \\<SAMBA-ServerIP >
-> Enter user ID and password

Linux machine Client side

-> ping <SAMBA Server IP>
-> mkdir /cif **(make directory where samba shared data shown)**
> yum install cif-utils
-> mount -t cifs //<SAMBA ServerIP>**/common** /cif -o username=pravin
-> mount -t cifs //<SAMBA ServerIP>**/share** /cif -o username=pravin

*****DHCP Server(dhcp-4.1*)*****

port - 67
Service - /etc/init.d/dhcpd
Confige file - /etc/dhcp/dhcp.conf

- DHCP meaning providing IP address to client machine.
- DHCP server : Dynamic host configuration protocol is a Client/Server protocol which will automatically provide IP address to the requested client and Not only IP address along with IP it will also provide subnet mask or multiple subnet mask, gateway IP and DNS IP address.
- With DHCP-Server this entire process is automated and managed centrally.
- DHCP-Server will provide a automatic IP address using DORA process which means, D=Discovery, O=Offer, R-REquest and A=Ackowledgement

Server-Side

-> rpm -qa |grep i dhcp-4.*
-> yum install dhcp-4.* -y
-> /etc/init.d/dhcpd restart
-> systemctl start dhcpd ----rhel 7
-> chkconfig dhcpd on
-> systemctl enable dhcpd ----rhel 7
-> netstat -tulap |grep 67

*****All services having one sample configure file stored location /usr/share/doc/***

copy dhcp cofigure file
-> cp /usrs/hare/doc/dhcp4.*/dhcpd.conf.sample or example /etc/dhcp/dhcpd.conf
-> vi /etc/dhcp/dhcp.conf (entry only given below things)

```
subnet 192.168.0.0 netmask 255.255.255.0{
range 192.168.0.100 192.168.0.200;
```

-> vi /etc/sysconfig/network-scripts/ifcfg-eth0 (entry)

```
BOOTPROTO=dhcp
```

-> /etc/init.d/dhcpd
-> dhcpd -t
-> dhcpd configtest
restart
(to test dhcp-server configuration)
(to test dhcp-server configuration)
-> vi /var/lib/dhcp/dhcp.leases --->dhcp.leases file contain all information of client and client mac id

*****How to allow dhcp parmanantly in firewall**

-> firewall-cmd --parmanent --add-service=dhcp
-> firewall-cmd --parmanent --add-port=67
-> firewall-cmd --reload

*****DNS – (Domain Name System)*****

Port - 53
Service - /etc/init.d/named
Confige file - /etc/named.conf

- DNS meaning IP Mapping which is used for resolved IP addres issue
- we can't memorised all IP address over network but we can memorised Name of IP address which are mapped in DNS server.
- Total over world 13 - DOT Server also called root server.

Server side

-> rpm -qa |grep -i bind
-> yum install bind-* -y ---->bind-9.8.0version
-> /etc/init.d/named restart
-> systemctl start named ----rhel 7
-> chkconfig named on
-> systemctl enable named ----rhel 7
-> netstat -tulap |grep 53
-> **vi /etc/named.conf** (entry 1st removed all)

Client side

-> /etc/init.d/named restart
-> vi /etc/resolv.conf (Entry **Contain List DNS servers ip for internet DNS resolution)**
nameserver 198.168.1.10 (DNS server IP- 192.168.1.10)
-> ping youtube.com (if output shown IP address then our DNS server is working)
-> dig facebook.com (Tool for test DNS)
output----> facebook.com IN A 157.39.42.45

Process of DNS server

1. client machine send request from Brower https://www.facebook.com. Called Fully Qulified Domain Name (FQDN)
2. then request goto in /etc/hosts path to match or found IP if not found any match
3. then goto /etc/resolv.conf to match or found IP here we found our Local DNS server machine with ip 192.168.1.10
4. when we did not found IP match on our local DNS server then request goto DNS server 8.8.8.8 vai our DNS server which made by google also called DOT server
5. then match here IP with name facebook.com and once match IP here then all information stored on our Local DNS server for cache purpose
6. then url get IP then url search that IP machine to send client machine request
7. then all communication done with port 80 and 53 because of serve web pages from facebook.com server machine to client machine
8. Also all IP mapping Cache stored on our Local DNS server
9. ctrl+alt+delete for Delete Browser cache

*****How to allow DNS parmanantly in firewall**

-> firewall-cmd --parmanent --add-service=named
-> firewall-cmd --parmanent --add-port=53
-> firewall-cmd --reload

*****APACHE Web Server version 2.4.*****

Port - 80
Service - /etc/inint.d/httpd
Confige file - /etc/httpd/conf.d/httpd.conf

- Native American people called as Apache men.
- **Apache have two type hosting**
  - **1. Name Based hosting – Multiple website Run on One IP**
  - **2. IP Based hosting – Multiple IP run only one website**
- **Apache tag called Directives**

Server side

-> yum install httpd-* -y
-> /etc/init.d/httpd restart
-> systemctl start httpd.service ----rhel 7
-> chkconfig httpd on
-> systemctl enable httpd.service ----rhel 7
-> netstat -tulap |grep 80
-> mkdir /opt/pravin.com
-> touch index.html (your web file programme file)
-> vi /etc/httpd/conf.d/httpd.conf (In Apache config file we found Three Secssion)

1. global section 2. main section 3. virtual host section
(goto Virtual host section see all tag then write for our website)

DocumentRoot /opt/pravin.com
ServerName pravin.com (Here we match servername then provide web page to client)
DocumentRoot /opt/facebook.com
ServerName facebook.com
DirectoryIndex my.html (we can put souce file name here or replce with index.html)
-> /etc/init.d/httpd restart
-> httpd -t ---->rhel 6 test apache configure file
->apachectl configtest ---->rhel 7 test apache configure file

Client side

-> vi /etc/hosts (Entry **Lists hosts IP with name to be resolved locally DNS)**
192.168.1.10 pravin.com (pravin.com match with server name on server side)
goto Browser enter in url pravin.com
-> vi /etc/selinux/conf (entry)
selinux=disable

******How to allow apache parmanantly in firewall***

-> firewall-cmd --parmanent --add-service=https
-> firewall-cmd --parmanent --add-port=443/tcp
-> firewall-cmd --reload

*****Sendmail Server Or MTA(mail transfer agent) Server*****

Port - 25
Service - /etc/init.d/sendmail
Confige file - /etc/mail/sendmail.mc

- **Now days we used Postfix Sendmail-Server and sendmail server used SMTP(Sendmail Transfer Protocol) eg. Gmail.com application used this Mail-Server**
- **Zimbra is mail suite which contain many email integrated tool.**
- **postfix, Qmail, Exim, sendmail, Exchange all are MTA (mail transfer agent) server.**
- **All Linux user are mail user but not samba user.**

Server side

-> yum install sendmail-* -y
-> /etc/init.d/sendmail restart
-> systemctl start sendmail ----rhel 7
-> chkconfig sendmail on
-> systemctl enable sendmail ----rhel 7
-> netstat -tulap |grep 25
-> vi **/etc/mail/sendmail.mc** (entry search line no. 127 comment it)
#dnlDAEMON_OPTION('port')

*****How to send a e-mail**

-> mail pravin.shinde@tiss.edu press enter then write subject then message
->. (for comes out)
-> cd **/var/spool/mail**
-> cat pravin.shinde (to check mail)

*****How to Install Postfix In centos or rhel**

Service - postfix
Confige file - /etc/postfix/main.cf

- Before install postfix, remove sendmail from the server. Because sendmail is the default MTA in Redhat/CentOS.
- Firewall and SELinux should be disabled.

Server-Side

-> yum remove sendmail
-> service iptables stop
-> chkconfig iptable off
->vi /etc/selinux/config (entry)
SELINUX=disabled
-> yum install postfix
-> vi /etc/postfix/main.cf (no entry)
-> service postfix start
-> chkconfig postfix off
-> telnet localhost smtp (To test postfix)

Client-Side

-> cd /home/user1/Maildir/ (this path shown all inbox mail)

*****RPM(Redhat Packege Management)**

-> rpm -ivh<*.rpm> (install package)
-> rpm -e <*.rpm> (erase package)
-> rpm -qa |wc -l (count all rpm)
-> rpm -qa |grep -i <*.rpm> (find any rpm package which is stored in **/var/lib/rpm/package)**
-> rpm -qlp <*.rpm> (shown all list of file before rpm file installation)
-> rpm -Uvh<*.rpm> (upgrade Package)
-> rpm --rebuildbd (rebuild rpm database **/var/lib/rpm/package**)

*****YUM(yellow-Dog Update modifier)*****

-> yum install <PackageName>
-> yum update
-> yum list
-> yum checkupdate
-> yum upgrade or downgrade
-> yum –help
-> yum repolist

*****How to update OS in Linux also called Linux partial paching server also Red Hat Satelite server meaning full paching server**

-> yum check-update
-> mail all cheklist to all group
-> yum update -x mysql php or mariadb **(Don’t update Database packages and php)**

*****Xinetd-Server(Extended Internet Service Daemon))*****

Port - 9098
Service - /etc/init.d/xinetd
Configefile - /etc/xinetd.conf
All directory - /etc/xinetd.d ---->all child service file are stored here

It's standalone server which is console of multiple child service which is below mention.

1) Telnet-Server
2) tftp-Server
3) rsync-Server
4) nrpe-Server ---->which is agent of Nagios monitoring tool

- **Xinetd**-server used for reduce RAM Load.
- **Xinetd**-server used for reduce Memory Utilization.
- **Xinetd** is one service for Multiple child services.
- **60** is the maximum number of requests xinetd can handle at once.
- **socket_type**: Sets the network socket type to stream.
- **protocol**: Sets the protocol type to TCP

Server -Side

->rpm -qa |grep -i xinetd
-> yum install xinetd-* -y
-> /etc/init.d/xinetd restart
-> systemctl start xinetd ----rhel 7
-> chkconfig xinetd on
-> systemctl enable xinetd ----rhel 7
-> netstat -tulap |grep -i xinetd

*****telnet-server*****

Port - 23
Service - /etc/init.d/xinetd
Confige file - /etc/xinetd/telnet

which is used for remote login purpose and used communication in clear text Mode so that session is not secured that why we used ssh (Secured Socket Host) because that used communication in encryption Mode

Server-Side

-> yum install xinetd telnet-server* -y --->telnet port - 23
-> vi /etc/xinetd.d/telnet (entry)
disable=no
-> /etc/init.d/xinetd reload
-> vi /etc/sysconfig/iptables --->Allow telnet into Linux firewall
-> iptables-A INPUT -p tcp --dport 23 -j ACCEPT
-> service iptables restart

Client-Machine

-> telnet < serverIP > or <username@server IP> Bydefault root login for telnet is disable but we can login with any user then after that we used su – for root access.

*****tftp-server(Trivial File Transfer Protocol)*****

Port - 69
Service - /etc/init.d/xinetd
Confige file - /etc/xinetd/tftp

Server-Side

-> yum install xinetd tftp-server-* -y --->tftp port – 69
-> vi /etc/xinetd.d/tftp (entry)
disable=no
-> /etc/init.d/xinetd reload
-> mkdir /tftpshare --->tftpshare - folder name of tftp
-> chmod 777 /tftpshare
-> vi /etc/xinetd.d/tftp (entry)
1. flags = Ipv4 2. server_args = -c -s /tftpshare 3.disable=no
-> /etc/init.d/xinetd reload

*****ssh-server or Openssh-server*****

Port - 23
Service - /etc/init.d/sshd
Configefile - /etc/ssh/ssh_config

which is used for remote login purpose but it is highly secure because ssh used communication in encryption mode if session is hack by hacker then they will not understood the session because it is in ecrypted.

Server-Side

-> rpm -qa |grep -i ssh
-> yum list | grep -i ssh
-> yum install openssh-server* -y
-> /etc/init.d/sshd restart

Client-Machine (no need to install ssh on client side only required in server machine)
-> ssh <server IP> or <username@serverIP**>**

*****How to change port in SSH for remote Access on Server Machine (OS Hardning)**

-> vi /etc/ssh/ssh_config (entry)
#port 22 (replace or next line) port 1025 (enter only >1024 port no.)
-> /etc/init.d/sshd restart --->rhel 6
-> systemctl restart sshd
-> netstat -tulap |grep -i 1025 or grep ssh

client machine

-> vi /etc/services (entry)
#ssh 22/tcp (replace or next line) ssh 1025/tcp

*****How to disable Root Login by SSH on Server Machine (OS Hardning)**

-> vi /etc/ssh/ssh_config (entry)
#PermitRootLogin yes (replace or next line) PermitRootLogin no
-> /etc/init.d/sshd restart --->rhel 6
-> services sshd restart --->rhel 6
-> systemctl restart sshd --->rhel 7

client machine

-> ssh <serverIP> (that time you get error or did not give root login)
-> ssh <username@serverIP> (that time you get login with any user after that used below)
-> su - (for root login then enter root userID and password)

*****How to Create Without Password Login in SSH(RSA algorithm) (OS Hardning)**

ServerIP 192.168.1.10

-> sshkeygen -t rsa
-> Press 2 time Enter button (In that time server saved both identificartion in path of /home/pravin/.ssh/id_rsa and public ket in path of /home/pravin/.ssh/id_rsa.pub)
-> ssh pravin@192.168.1.25 mkdir -p .ssh (Remote access and create .ssh direcorty on client machine)
-> cat .ssh/id_rsa.pub | ssh pravin@192.168.1.25 `cat >> .ssh/autherized_keys`
(copy or upload generated public key on Client machine192.168.1.25)

Login on ClientIP 192.168.1.25

-> chmod 700 .ssh ; chmod 640 .ssh/autherized_keys (set permission on client machine)
-> ssh <username@serverIP> (now your login with ssh without pass.)

*****Kernel Management - /boot/vmlinuz 2.6.32-504*****

- The Linux kernel is a free and open-source, monolithic file contain number of functions, information, sheduler, variable etc
- kernel manual file contain all information related of kernel file **/boot/config- 2.6.32-***
- There are three type of kernel in Unix

1.Monolithic (linux support) 2. Micro (aix & solaries support) 4. Exo (Development Support)

- **Patching System** meaning update kernel, add or remove any driver which supported or not or update all driver's in server or add any script to application support.
- *.ko file means kernel object all are linux driver's and path **/lib/module/2.6.32-*/kernel**
- Driver having two type categories

1. **KLM**(Kernel Loadable Module) 2.**LKM**(Loadable Kernel Module)

***How to update Kernel in linux

-> yum update kernel (to update kernel using yum or rpm)

-> rpm -Uvh kernel 2.6.32-*

*****How to count and install and modify and delete and check all Loaded Drivers in the RAM**

-> lsmod (show all system related driver details eg. DriverName, DriverSize, DriverUsed)

-> modprobe drivername.ko

-> insmod drivername.ko

-> rmmod drivername.ko

-> modinfo drivername.ko

-> depmod drivername.ko

-> cat /proc/modules |wc -l

Kernel Tunning - Changed Kernel file or parameter value when kernel is running.

->cd /proc/sys ('sys' directory contain all kernel file parameter)

*****How to find kernel file parameter and Edit that parameter value. <u>(OS Hardning)</u>**

-> sysctl -a | grep -i <file parameter> (shown all kernel file parameter and parameter value)

-> sysctl -w vm.swapiness = 100 (we can edit kernel file parameter using sysctl)

-> cd /proc/sys

-> vi file-max **(but did not open because of live in RAM all /proc)**

-> echo 300000 > /proc/sys/fs/file-max (to change maximum file creation limit to 300000)

*****How to install Any Driver in the system**

1. Download source file using wget <download link>
2. -> ./configue (run or compile driver configure file)
3. -> make
4. -> make install
5. that s/w or driver stored then goto -> cd /usr/local/<drivername>
6. -> mv drivername.ko /lib/modules/2.6.32..../kernel (to move driver at actual path)

*****How to count all drivers which is present in system without using find command.**

-> ls -R /lib/module/2.6.32-..../kernel |grep -i .ko | wc -l

*****LVM(Logical Volume Manager)*****

-path -/dev/mapper/mylvm-lv1 or /dev/mylvm/lv1 -all driver stored in /dev

*****How to Create 500MB LVM partition in linux**

->fdisk /dev/sdb
|
press ‘n’ for new partition
|
press ‘p’ for primary partition
|
press ‘1’ for ‘sdb1’
|
press ‘+500’ for sdb1 size
|
press ‘w’ for save changes
|
-> partx -a /dev/sdb
-> partx -a /dev/sdb
-> fsdisk -l (check sdb1 partion add or not)
-> pvcreate /dev/sdb1 (to create physical volume)
-> vgcreate vg1 /dev/sdb1 (vg1 – to create volume group name)
-> lvcreate -L 300G -n lv1 vg1 (-L to create lv1 logical volume name)
| |
lvm size new name

*****How to Delete LVM partition in Linux**

-> lvs -o +devices (check lv to vg relation)
-> df -h (check mount point)
-> rsync -parv /LVM1 /opt/LVM_backup (for backup security)
-> umount /LVM1
-> vi /etc/fstab (remove lvm1 entry)
-> mount -a
-> df -h
-> lvremove /dev/vg1 /lv1
-> **vgreduce** vg1 /dev/sdb
-> pvremove /dev/sdb
-> fdick /dev/sdb press ‘d’ for delete partition press ‘w’ for save changes
-> partx -a /dev/sdb

*****How to check all details of partition in LVM**

->pvdisplay
->vgdisplay
->lvdisplay

*****How to check all details of partition Background Mapping in LVM**

->pvscan
->vgscan
->lvscan
-> Below three commands shown all partion mapping
-> pvs ->lvs -o +devices ->df -h

*****How to make permanant Partition**

-> vi /etc/fstab (entry)
/dev/mylvm/lv1 /data2 ext4 defults 1 2 (data2- lvm mount folder /data2)
-> mount -a
-> df -h

*****TCP Wrapper also called Application Level Firewall*****

- This Application level firewall used for Block Unautherised session or port or login or services to perticular ip or users.
- TCP Wrapper can only block those sevices which services or application depend upon libwrap.so.0 file eg. APACHE-httpd, FTP-vsftpd, SSH-sshd, NFS-nfs
- Some time we add lib file by rescue mode libwrap.so.0
- TCP wrapper having two Important files

-> vi /etc/hosts.allow - that file used for add any IP or user allow for service and port but Bydefault all user or ip are allow for all services which depend on TCP wrapper and we did not used this file.
-> vi /etc/hosts.allow (entry)
sshd : 192.168.1.10 (allow only system admin IP for ssh service on server) (OS Hardning)
-> vi /etc/hosts.deny - that file we used commonly to Block any user and IP for TCP wrapper Services in the organisation.

-> vi /etc/hosts.deny	(entry)
vsftpd : 192.168.1.52/32	(Block ftp service for this IP)
sshd : ALL or sshd : 0.0.0.0	(Block all user or IP for SSH Service)
nfs : ALL EXCEPT 192.168.1.10/24	(Block all user or IP for nfs Service except Admin IP)

*****IPTABLES*****

service - /etc/init.d/iptables **confige file- /etc/sysconf/iptables**

- iptables used for block ports, unautherized access, Login, NAT(network address translation), PAT(port address translation), reject Request and Response.
- Iptables is a tool or service and called sandalone firewall or system level firewall.
- Opensource firewall 1. IPCOP 2. Pfsense
- Hardware Firewall 1. Sonicwall 2.CISCA 3.Cyberrom 4.Check Point
- iptable --->RHEL6 firewalld---->RHEL7 nftables------>RHEL8
- **netfilter.ko** driver which is achual firewall
- three type of chain in iptables

1. INPUT Chain - Outside to Organisation also called incoming request
2. OUTPUT Chain - Organisation to Outside also called outgoing request
3. FORWARD Chain- Outside to Organisation then modify then Organisation to Outside

iptable work with four layer

- 1. Raw – used for packet tracking
- 2. Mangle – used for packet modification
- 3. Nat (Network Address Transmission)- used for ip address transmission
- 4. Filter - used for block filtering and forwording and allowing bydefault

***flags** **P-Policy, p- protocol, s-Source, d- Destination, j- Jump, A- Append, D- Delete, F-Flush L- List, --dport – Destination Port**

-> rpm -qa | grep -i iptables
-> /etc/init.d/iptables restart
-> chkconfig iptbales on

-> iptables -L	(list of all iptables rule present in system)
-> iptables -F	(Delete or flush all iptables rule present in system)
-> iptables -D INPUT 2	(Delete only 2nd incoming iptables rule present in system)
-> iptables -D OUTPUT 2	(Delete only 2nd outgoing iptables rule present in system)

-> iptables -A INPUT -s 192.168.1.12/32 -j REJECT (Reject incoming server for ip 192.168.1.12)

-> iptables -A INPUT -s 0/0 -j REJECT	(Block all incoming Traffic on server)
-> iptables -A OUTPUT -d 0/0 -j REJECT	(Block all outgoing Traffic on server)

***How to allow only 25 and 35 ip but block for all ip over organisation.**

1. iptables -A INPUT -s 192.168.1.25/32 -j ACCEPT
2. iptables -A INPUT -s 192.168.1.35/32 -j ACCEPT
3. iptables -A INPUT -s 0/0 -j REJECT
4. service iptables save

***How to make server fully sercure (**Drop all three policy in iptable rule) Because **iptables 1st compare rule then compare with policy** and **Default all Policy are ACCEPT**

1. iptable -F
2. iptables -P INPUT DROP
3. iptables -P OUTPUT DROP
4. iptables -P FORWORD ACCEPT or DROP
4. service iptables save

***How to allow for all over world for only website and allow ssh only for 192.168.1.10 website-80port for all user over world and ssh-22port allow to 192.168.1.10 both are used tcp protocol**

-> iptable -F
-> iptables -A INPUT -s 192.168.1.10/32 -p tcp --dport 22 -j ACCEPT
-> iptables -A INPUT -s 0/0 -p tcp --dport 80 -j ACCEPT
-> service iptables save

How to allow for only for admin for ssh on server

-> iptable -F
-> iptables -A INPUT -p tcp -s 198.168.1.10/32 --dport 22 -j ACCEPT
-> service iptables save

*****User Management*****

-> useradd pravin (70's things happens in background & **TWO files Refer when user Create**)
1> cat /etc/login.defs (created user with UID, GID, Permission, /home/pravin,Mail Directory)
2> cat /etc/defaults/useradd (Change user home directory, shell, INACTIVE Day, Expire Day)
->cp /etc/skel/.bash* /home/pravin

Update Below 4 no's files with Feild's and also called user database file's

-> vi /etc/password 7(User_Name, Password, UID, GID, gecos/finger, Home_Directory, Shell)

-> vi /etc/shadow 9(User_name, Encrypted_Password, Date_of_last_password_change, Minimum_password_age, Maximum_password_age, password_warning_period, password_inactivity_period, account_expiration_date, reserved_field)

-> vi /etc/group 4(group_name, Encrypted_group_password, GID, user_list)

-> vi /etc/gshadow 4(group_name, Encrypted_group_password, administrators, members)

*****How to Set a group Name and change group Password**

-> usermod -g BEIT -G Engineer pravin (BEIT-Primary group Engineer – Secondary group)

-> gpasswd <group name> (change group password)

*****How to Create 5000 user at a time with password**

-> touch UserNameFile (write 5000 user name in this file)

-> newusers UserNameFile or

-> for i in `cat UserNameFile` ; do useradd $i ; done ;

(` ` this called bactic sign do first between any command)

->for i in `cat UserNameFile` ; do echo "test@123" | passwd $i ; done ;

*****How to Modify pravin user**

-> usermod -u 1005 -d /otp/pravin -s /bin/sh pravin

(u - change uid, d – change home directory, s – change shell)

-> id pravin (shown all detail related to pravin user)

*****How to set Change Password Promt on user next login**

-> adduser pravin

-> change -d 0 pravin (change 3rd feild value in shadow file to zero)

*****How to disable pravin user Login**

->vi /etc/passwd (entry)

1.Replace x to blank space in 2nd feild of pravin user

2. Replace /bin/bash to /bin/false of /bin/nologin in 7th feild of pravin user

*****How to disable all user Login but root can login**

-> touch /etc/nologin (create nologin file in /etc)

*****How to lock user and unlock pravin user**

-> passwd -l pravin

-> passwd -u pravin

*****How to asign SUID, SGID, STICKG*****

1.**SUID**- Set user id means (-rws r-- r-- /sbin/fdisk) set userid + execute this file which user having root permission or which user can run root level or priveleged command

-> chmod u+s /sbin/fdisk

-> chmod 4777 /sbin/fdisk

2.**SGID** -Set group id means (-rwx rws r-- /sbin/fdisk) set group id + execute this file which user's having same group ID like ramu and shamu having one group ID then both can access this file.

-> chmod g+s /sbin/fdisk

-> chmod 2777 /sbin/fdisk

3.**STICKG** -Set sticky bit permission (-rwx rwx rws /sbin/fdisk) means any file having fully permission but only owner can delted this file.

-> chmod o+t /sbin/fdisk

-> chmod 1777 /sbin/fdisk

*****Find Command Examples*****

-> find . -type f -name pravin (find **file** in current directory which name is pravin)

-> find . -iname pravin (find all in current directory with **ignore** case pravin)

-> find / -type d -iname pravin (find only **directory** in "/ " which name is pravin)

-> find / -type f -name "*.txt" (find all **.txt file** in ' / ')

-> find . -type f -perm 777 (find all file in current directory with **permission 777**)

-> find . -type f ! -perm 777 (find all file in current directory **without permission 777**)

->find / -type f -perm 777 -print -exec rm -f {} \; (**find** and **delete** file with permission 777)

->find / -type f -name "pravin" -exec rm -f {} \; (**find** and **delete** file with name pravin)

-> find /tmp -type f -empty Find Empty file in /tmp directory

-> find /tmp -type f -name ".*" Find Hidden file in /tmp directory

->**f**find / -mtime 50 (find all the files which are **modified** 50 days back)

->find / -atime 50 (find all the files which are **accessed** 50 days back)

->find / -mtime 50 -mtime -100 (To find all the files which are modified more than50days back and less than100days)

->find / -mmin 60 (find all the files which are modified in last1 hour back)

->find / -amin 60 (find all the files which are accessed in last1 hour back)

->find / -cmin 60 (find all the files which are changed in last 1 hour back)

->fins / -size +50M -size -100M (find all the files with size between 50MB to 100MB)

->find / -type f -name "*.mp3" -size +10M -exec rm -f {} \; (**find** and **delete** all .mp3 file which having size more than **10MB**)

*****LILO BOOT PROCESS-Runlevel 3&5*****

System Space

(LILO-Linux Loader, Grub- grub unified boot loader, MBR- Master Boot Record)

1. Person Press Button
2. SMPS get start then BIOS load Automatically in RAM
3. after CPU pin 66 signal ROM having one programme called BIOS loaded in the RAM then BIOS done Power On Self Test (POST)Check then BIOS Load CMOS Programme who have information related system H/W
4. BIOS goto 1st Sector of 1st Track of 0th Cylinder of HDD to search and Load MBR in RAM(1st time load from DVDor if not present in DVD then Anaconda write MBR programme and after OS install BIOS get MBR from HDD)

   MBR size 512 byte |----------446byte----------|----------64byte----------|--2byte-------|
   | Boot Sector | Partition Table | Magic no |
5. MBR Boot Sector contain only boot loader eg- ntldr(windows BootLoader), LILO(Linux Loader) and partion table contain 4 programme which having size 16byte that why we can only create 4 No's of Primary Partition Magin no. Have two value yes or no whch check MBR status and if MBR fine then output is yes else no and MBR created by IBM company and MBR size 512byte why beause one Sector size is 512 byte.
6. BIOS load LILO from MBR boot sector but LILO did not understood MBR CHS (Cylindrical Head Sector)so that time BIOS come four time in RAM by help of Intrrupt-13 Function and load below four CHS in the RAM for LILO and BIOS Load LILO that process called **stage1**
7. LILO load /boot/boot.b called **stage 2** (after that boot.b load three things in RAM)

   |

   1. /boot/message (Splash Screen)
   2. /boot/map
   3. /boot/vmlinuz (Kernel)
8. BIOS get Free after vmlinuz or linux kernels get load into RAM
9. vmlinuz file Load /boot/initramfs (initrd, dracut) file in RAM
10. initramfs file 1st mount "/" then load below content

    |

    1. JBD.ko (HDD Driver)
    2. ext4.ko (file system friver)
    3. nash (minimum shell)
    4. mount /dev/root / ro (setup root in "/")
    5. **mount /dev/sdax / ro (switch root "/" with readonly permission)**

Load in RAM and Access the partion called mounting.

*****Grub BOOT PROCESS-Runlevel 3&5*****

System Space

1. Person Press Button
2. SMPS get start then BIOS load Automatically in RAM
3. after CPU pin 66 signal ROM having one programme called BIOS loaded in the RAM then BIOS done Power On Self Test (POST)Check then BIOS Load CMOS Programme who have information related system H/W
4. BIOS goto 1st Sector of 1st Track of 0th Cylinder of HDD to search and Load MBR in RAM(1st time load from DVDor if not present in DVD then Anaconda write MBR programme and after OS install BIOS get MBR from HDD)

   MBR size 512 byte |----------446byte----------|----------64byte----------|--2byte-------|
   | Boot Sector | Partition Table | Magic no |
5. MBR Boot Sector contain only boot loader eg- ntldr(windows BootLoader), grub(Linux BootLoader) and partion table contain 4 programme which having size 16byte that why we can only create 4 No's of Primary Partition Magin no. Have two value yes or no whch check MBR status and if MBR fine then output is yes else no and MBR created by IBM company and MBR size 512byte why beause one Sector size is 512 byte.
6. BIOS load grub (rhel-6 grub version 0.97 & rhel-7 grub version 2.0)process called **Stage1**
7. **grub can understood ext filesystem that why didnot take help of CHS and that ext file system support called Stage 1.5**
8. **then grub refers -> vi /boot/grub/grub.conf file and load kernel and initramfs**

   |

   1. vi /boot/vmlinuz ---->load by grub

   2. vi /boot/initramfs ---->load by grub
9. **-> vi /boot/grub/grub.conf file contain**

default = 0 **(which OS you need when to start after timeout as default tittle)**

timout = -1 **(splash screen hold time)**

splashimage = (hd0 , 0)/grub/spash.xpm.gz

| |

Indicate load 1st HDD MBR |Locate /boot partin

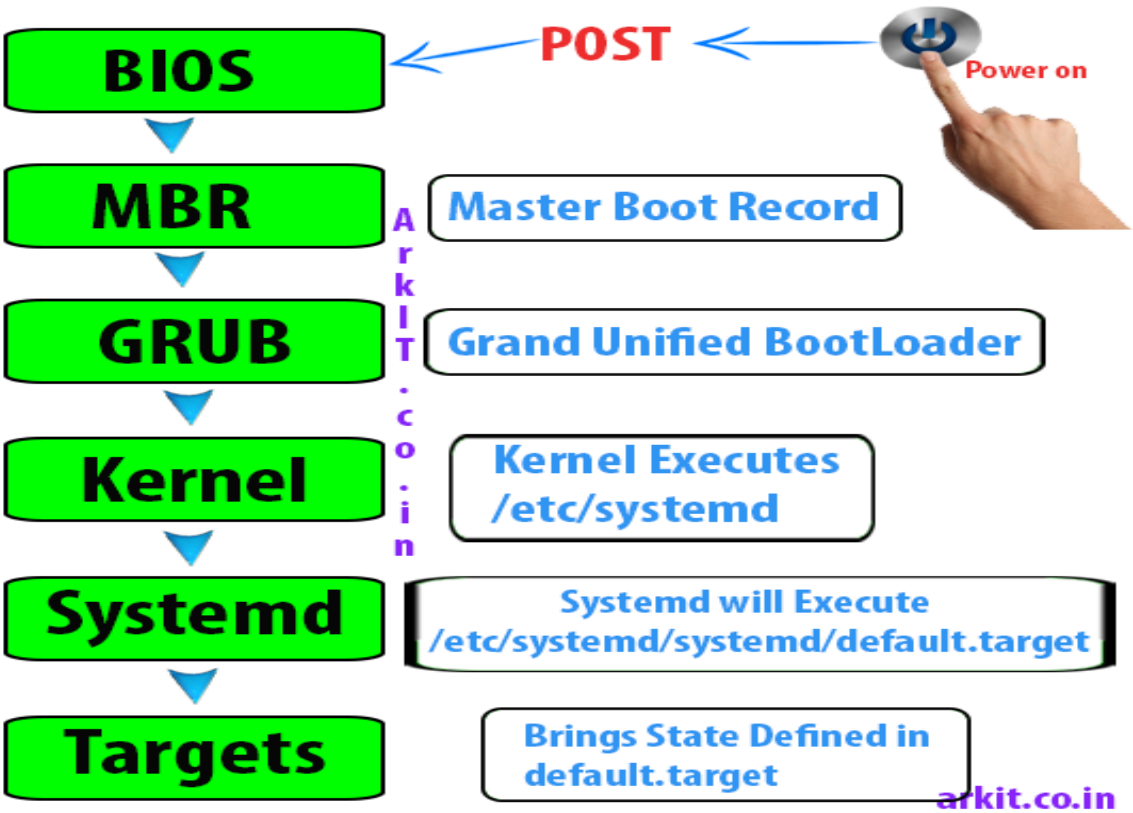
10. grub get Free after vmlinuz or linux kernels get load into RAM
11. vmlinuz file Load /boot/initramfs (initrd, dracut) file in RAM
12. initramfs file 1st mount "/" then load below content

    |

    1. JBD.ko (HDD Driver)
    2. ext4.ko (file system friver)
    3. nash (minimum shell)
    4. mount /dev/root / ro (setup root in "/")
    5. **mount /dev/sdax / ro (switch root "/" with readonly permission)**

Load in RAM and Access the partion called mounting.

RHEL7 Boot Process



Step 1 – 4 : All steps Same till grub load in RAM from MBR as per RHEL6 grub boot process

Step 5 : GRUB

(Grand Unified Boot Loader) configuration file located in /boot/grub2/grub.cfg which actually points to **initramfs** is initial RAM disk, initial root file system will be mounted before real root file system.

Basically initramfs will load block device drivers such as SATA, RAID .. Etc. The initramfs is bound to the kernel and the kernel mounts this initramfs as part of a two-stage boot process.

Step 6 : KERNEL

GRUB2 config file will invoke boot menu when boot is processed, kernel will load. When kernel loading completes it immediately look forward to start processes / Services.

Step 7 : Starting Systemd the first system process

After that, the systemd process takes over to initialize the system and start all the system services. How systemd will start.

As we know before systemd there is no process / service exists. Systemd will be started by a system call fork( ); fork system call have an option to specify PID, that why systemd always hold PID 1.

As there is no sequence to start processes / Services, based on **default.target**will start. If lot many services enabled in default.target boot process will become slow.

Step 8 : User Interface (UI)

Once that's done, the "Wants" entry tells systemd to start the **display-manager.service service** (/etc/systemd/system/display-manager.service), which runs the GNOME display manager.

Your User interface start and prompt you for credential to login.

*****shell Scripting*****

-> vi pravin (write a script)

```
clear
echo “Welcome to Linux”
echo “which Distributer you refer in linux”
read os
case $os in
redhat ) tput cup 10 10  ; echo “Red Hat is good Distributer but very expensive”
;;
centos ) tput cup 10 10  ; echo “Centos very good option as compare with Red Hat”
;;
fedora ) tput cup 10 10  ; echo “Fedora also good but as compare above two....”
;;
* ) tput cup 10 10  ; echo “This is not valid distributor....”
;;
esac
sleep 2
clear
echo “Enter any num.....”
read num
if test $num -le 5
#(-le ,-lt .-gt ,-ge ,-eq ,-ne)
then
tput cup 10 10  ;echo “you enter small value than 5”
else
tput cup 10 10  ;echo “you enter bigger value than 5”
fi
```

service	systemctl	Description
service name_service start	systemctl start name.service	Starts a service.
service name_service stop	systemctl stop name.service	Stops a service.
service name_service restart	systemctl restart name.service	Restarts a service.
service name_cond restart	systemctl try-restartname.service	Restarts a service only if it is running.
service name reload	systemctl reload name.service	Reloads configuration.
service name status	systemctl status name.service systemctl is-active name.service	Checks if a service is running.

*****Crontab*****

In every 1 minute system goto /var/spool/cron and match job time to system time and system time linked with NTP and we can't run cronjob within Second but we can used sleep command to run cronjob scheduler.

There is three type of scheduler in the linux

1. cronjob schduler

2. anacron schduler- this scheduler userd to run those which cronjob missed or could not run on schdule time those are run in anacron scheduler.

3. atd - /etc/ini.d/atd this scheduler used when we need only onece time to run any cronjob that time we used atd file to run one time cronjob -> atd -f /opt/myscriptname 10AM

-> vi /etc/crontab

* Minute (hold values between 0-59)

* Hour (hold values between0-23)

* Day of Month (hold values between 1-31)

* Month of the year (hold values between 1-12 or Jan-Dec)

* Day of week (hold values between 0-6 or Sun-Sat)

-> vi /etc/cron.deny (In that file we can add user name which did not allow to set, write, and execute cronjob)

-> vi /etc/cron.allow (In that file we can add user name which allow to set ,write and execute cronjob)

System administrator can use predefine cron directory as shown below.

1./etc/cron.d
2./etc/cron.daily
3./etc/cron.hourly
4./etc/cron.monthly
5./etc/cron.weekly

-> crontab -l (" l "Shown all List of cronshceduler)

-> crontab -r (" r "Remove cron sheduler)

-> crontab -i -r (" i "given prompt you confirmation from user before deleting user's crontab)

-> crontab -e (" e "Edit crontab entries)

1. **Every Day Delete all empty file after 12.30AM or 00.30AM**

-> crontab -e

30 0 * * * root find / -type f -empty -delete

2. **Every Sunday backup of /home after 2.30AM and backup stored in /var/backup folder.**

-> crontab -e

30 2 * * 7 or 6 root tar -zcvf /var/backup/ /home **or** /root/backup.sh

| |

UserName /path **or** command – Script or command name to schedule

Important Notes Related to Linux OS

Note1.

Each hard linked file is assigned the same Inode value as the original, but Softlink or symbolic link shown differnce number of Inode value becuse softlink is pointer of orignal link and hard link is achual orignal link.

Link validation, when the original or parent file deleted in softlink which is not Valid but that is Valid in hardlink.

If link count is more than 1 that is hard link else it's softlink

ln -s /home/core/pravin.txt /opt/pravin (can create softlink Cross partition)

ln /home/core/pravin.txt /home/core/dj/pravin.txt (only create same partition)

Note2.

Total Runlevel's in Linux is 7 which is 0 to 6

init0 - shutdown or poweroff

init1 - Boot with single user mode and no Network, no GUI, no Login credential, only "/" mounted, only minimal drivers and services.

Init2 - Multiuser Mode without Network and No NFS and No GUI

init3 - Multiuser Mode with all possibility but only No GUI and **when No GUI there No Processor Load.**

Init4 - same as runlevel 3 but reserved for developer to development.

Init5 - Bydefault runlevel all possibility and GUI also present.

Init6 - Reboot or Restart again again.

Note3.

***How to secured Single user Mode**

->vi /etc/sysconfig/init (entry)

SINGLE=/sbin/sushell (replace with) SINGLE=/sbin/sulogin

after Reboot machine enter root credential on login page.

Note4.

In Logical volume manager (LVM) we can't extented regular partition if that partition is lvm partition then only then we can extend that partion and LVM is file system on partition.

File system id eg. 83 – ext2, ext3, ext4. 8E – linux LVM

Note 4

***How to find Machine Hardware and motherboard information.**

-> uname -a (view linux system information and architechture details)

-> lshw -short (information all system hw related with short table)

->dmesg | grep -i pci

->dmidecode

->biosdecode

Note 5.

Daemons always run after system start

application daemons means No impact on system which kill by user

system daemons means system will crach after kill this daemons.

Note6

File System Hierarchy

/	-	**Primary hierarchy** root and root directory of the entire file system hierarchy
/bin	-	This stands for binaries and contains the fundamental utilities that are needed by all users also for Essential command example: ps, ls, ping, grep, cp.
/sbin	-	This stands for System Binaries, and contains the fundamental utilities needed to start, maintain and recover the system and also system binaries **used typically by system aministrator, for system maintenance purpose e**g.iptables, reboot, fdisk, ifconfig, swapon
/root	-	This is the home location for the system administrator root.
/srv	-	This one is server data which is data for services provided by the system.
/sys	-	This contains a sysfs virtual filesystem which holds information related to the hardware.
/etc	-	This contains configuration files for the system and system databases.
		For example: /etc/resolv.conf, /etc/logrotate.conf
/opt	-	Contains add-on software, larger programs may install here rather than in /usr /opt stands for optional and contain third party application files.
/boot	-	This contains all the files needed for the booting process like GRUB boot loader's files and Linux kernels **eg. /boot/**initrd.img-2.6.32-24-generic, /boot/vmlinuz-2.6.32-24-generic, /boot/grub/grub.conf
/dev	-	This stands for devices, which contains files for peripheral devices and pseudo devices. Eg - /dev/sda, /dev/sr0
/lib	-	This is the system libraries and has files like the kernel modules and device drivers for 64bit systems.
/media	-	This is default mount point for removable devices like USB drives and media players, etc.
/proc	-	This contains virtual filesystems describing the processes information as files. eg-/proc/uptime
/tmp	-	This is a place for temporary files. tmpfs mounted on it or scripts on start up usually clear this at boot.
/mnt	-	This stands for mount, and contains filesystem mount points. Used for multiple hard drives, multiple partitions, network filesystems and CD ROMs.
/home	-	This holds all the home directories for the users.
/usr	-	This holds the executables and shared resources that are not system critical and **Secondary hierarchy** for read-only user data.
/var	-	This stands for variable and is a place for files that are in a changeable state. Such as size going up and down and var stands for variable files.
		log files(/var/log); packages and database files (/var/lib); emails (/var/mail); print queues (/var/spool); lock files(/var/lock); temp files needed across reboots (/var/tmp);

Note 7.

Top command used for collect and display all information from proc which loaded in ram

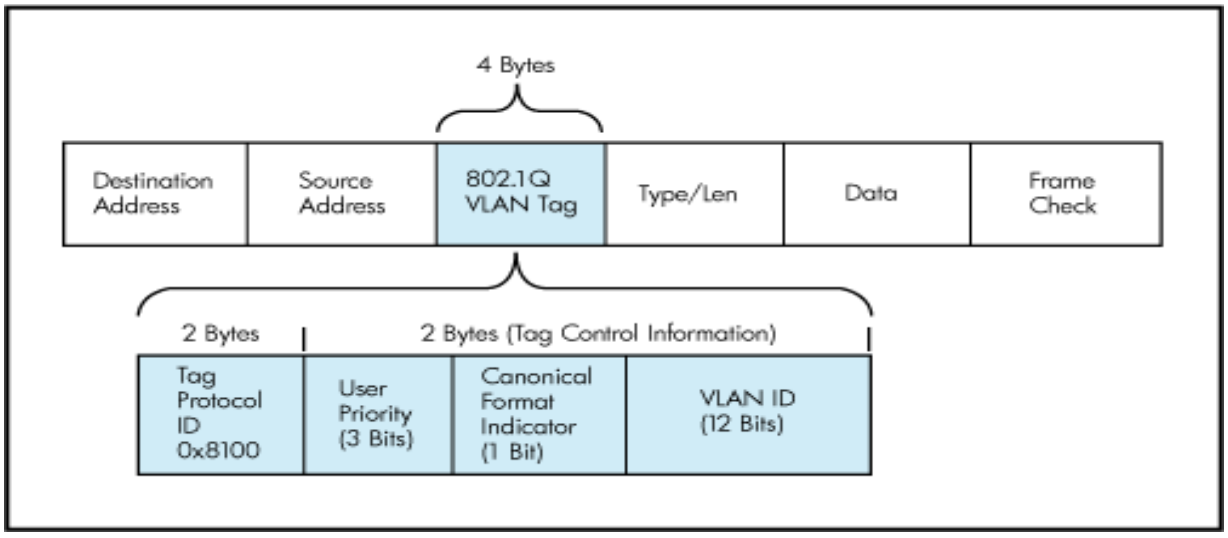
1st row contain	–uptime—how many user login—load average with 1min 5min 15min
2nd row contain	--total task—running task—sleeping task—stopped task—zombie task
3rd row contain	--how many % CPU used by User process, System process—nice value—CPU ideal Status value
4th row contain	--RAM total Memory Size—free size—used size—cache and buffer memory
5th row contain	--swap total memory size--free size—used size—available memory
6th row contain	--process ID—user name—nice value--% cpu--% memory—time—--command name

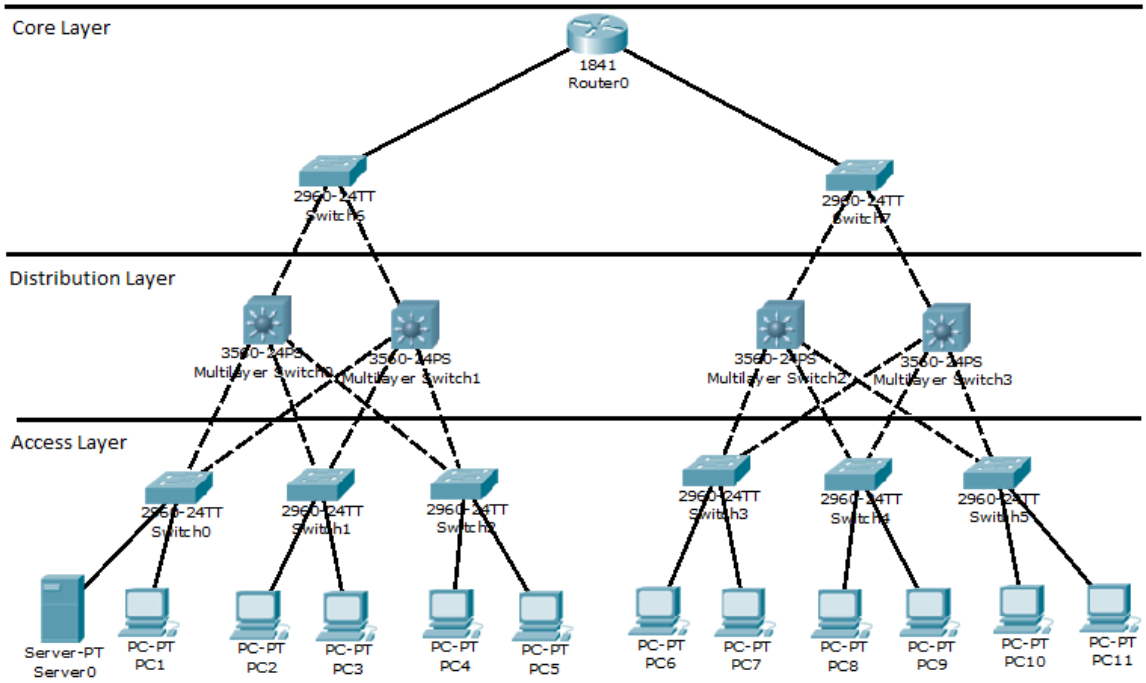
Note 8.

VLAN- A Virtual Local Area Network (VLAN) is a network technology used to logically separate large broadcast domains using layer 2 devices.

How do VLANs work ?

The virtual networks work by tagging the packets while they travel. Each port on a switch is associated with a VLAN. When a frame comes, the switch decomposes it and inserts a VLAN tag, specifying the ID of the VLAN configured on that specific port.





Data VLAN- This is the main type of virtual network. It is designed to carry user-defined data. The link connected to your computer is assigned to a data VLAN.

Default VLAN- This is the VLAN assigned by default to all ports. For Cisco switches this is VLAN1. That's why if you don't configure any virtual networks, your network will still reside in a VLAN

Native VLAN-The native VLAN is the VLAN assigned to untagged packets, which have not yet travelled through a VLAN marked port. The native VLAN must be configured on all switches. From a security perspective, it's not a good practice to leave it unchanged.

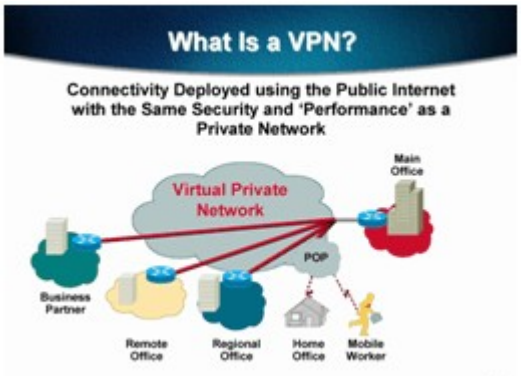
Management VLAN -VLAN used for switch management. It's a good practice to change it so it differs from the default one, although sometimes the Management VLAN is also set to be the native one.

Voice VLAN -This is a special type of VLAN used with VoIP devices. I'll discuss that later in detail.

Note9.

VPN (virtual private network) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g. a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common though not an inherent part of a VPN connection.

VPN Allows you to be at home and access your company's computers in the same way as if you were sitting at work. Almost impossible for someone to tap or interfer with data in the VPN tunnel. If you have VPN client software on a laptop, you can connect to your company from anywhere in the world.



Note 10.

POP- Post Office Protocol version 3 (POP3) is a standard mail protocol used to receiveemails from a remote server to a local email client. POP3 allows you to downloademail messages on your local computer and read them even when you are offline.POP is an application layer protocol.

Note11.

LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying items in directory service providers like Active Directory, which supports a form of LDAP. Short answer: AD is a directory services database, and LDAP is one of the protocols you can use to talk to it. In Windows Server LDAP is a protocol which is used for access Active Directory object, user authentication, authorization. LDAP is also used to store your credentials in a network security system and retrieve it with your password anddecrypted key giving youaccess to the services

Note14

Port's - In computer networking, a port is an endpoint of communication. Physical as well as wireless connections are terminated at ports of hardware devices. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.It is a 16-bit number (0 to 65535)

1.0-1023 – the Well Known Ports, also referred to as System Ports.
2.1024-49151 – the Registered Ports, also known as User Ports.
3.49152-65535 – the Dynamic Ports, also referred to as the Private Ports.

-> cat /etc/services | grep -i <port no.> **(all port information and Service Port Match Here)**

******* n**etstat** is a powerful tool for monitoring network connections and statistics.

-> netstat -tulap (a-all ,t-tcp listening ports, u- udp listening ports, l- listening sockets, n-port number, p-shown PID/Program Name)

***** nmap** used to find out all open ports, services and MAC address on the system.

-> nmap -v <server or machine IP> (shwon open ports v- with more details)

-> nmap -v <server or machine IP> <server or machine IP>(used for multiple IP)

-> nmap -v 192.168.1.* (used with wildcard)

***** lsof** -i (to display all open ports)

***** telnet** <domain name or ip address> <port>

Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name System (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP

110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP
123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP
3389	Remote Desktop Protocol	TCP and UDP

Note13.

Desktop Installation, Troubleshooting and outlook configuration

Patch updates, drivers installation, configure and enable services like FTP,SAMBA,SMTP,backup services, application services at desk/Low-end servers etc
Networking concept (OSI,TCP/IP,Topology etc)
Anti Virus support at client site
Windows support, DNS, DHCP, Lotus notes, Client side Outlook
VLAN VPN POP PROXY SERVER SAMBA ALL SMTP SNTP

EPEL(Extra Packages for Enterprise Linux)

- EPEL repository for RHEL 7 / RHEL 6/ RHEL 5 and Centos 7/ Centos 6/ Centos 5.
- EPEL repository (Extra Packages for Enterprise Linux) EPEL is a open source package building project which is owned and maintained by fedora.
- All the packages created by EPEL project is highly qualified and tested.
- Manual installation of packages in Linux it's time taking process and we have to download all the packages and it's dependencies one by one by using EPEL repo we can just install a packages using in yum command.
- EPEL Resolve dependencies and install them automatically.
- Just install EPEL RPM it will automatically configures YUM for you
- Required Internet access to install packages
- It does not provide duplicate core packages

-> wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm

-> rpm -ivh epel-release-7-7.noarch.rpm

-> vi /etc/yum.repos.d/epel.repo

-> yum repolist (check repolist is working or not)

-> yum list all

-> yum --enablerepo=epel install nagios (install nagios with using epel)