**Server Installation**

Bootup Process

* BIOS loads POST, hands over to MBR which loads & executes the GRUB boot loader; which loads and executes the KERNEL which mounts the File System, then executes the INIT system which identifies the RUN LEVEL by checking the /etc/inittab file.
* Config Files: GRUB - /boot/grub/grub.conf
* File System Mount: /etc/fstab
* Which services are available in the run level 5: /etc/rc.d/rc5.d
* Make run level permanent: chkconfig --level 35 on

**Configuration - Hardening**

* Modify root passwd level 1: /etc/sysconfig/init, shift g, then change /sbin/sushell to /sbin/sulogin
* Grub Passwd: # grub-crypt, then Copy to /boot/grub/grub.conf; insert under line 13:
* type: password --encripted, then paste, then reboot.
* # Setenforce 1 or moify /etc/Selinux/config to Enforcing
* Set password policy: modify /etc/login.defs and set password aging
* Deactivate root login remotely by: vi /etc/ssh/sshd\_config.
* Uncomment #PermitRootLogin and change 'yes' to 'no'
* Patch Server OS: yum update -y
* **Update Kernel**: wget link from kernel.org; # tar xvf link; # cd into pkg and then install using: # yum groupinstall "Development Tools"; then yum install openssl\*; then type # make menuconfig; and then type the # make command to compile dependencies
* Turn off unused services: chkconfig <service> off
* netstat -nlp | less to see listening ports
* ps -ax to see running processes; then kill -9 <process #>

**Configuration - Network**

* Use: system-config-network to Configure:
* ip address, hostname, DNS, gateway
* vi /etc/hosts
* cd /etc/sysconfig/network-scrpits; vi ifcg-<interface> service network start
* cat /etc/resolv.conf to verify dns; ifconfig; ping
* Samba: Communicate between Winows and Linux
* yum install samba; /etc/samba/smb.conf; service smbd start
* Firewall -To Open communication ports
* iptables -nL; /etc/sysconfig/iptables or system-config-firewall; service iptables restart
* NFS - Allows local access to remote files: yum install nfs-utils nfs-utils-lib; /etc/exports; service nfs start
* Rsyslog - Centralized logging system: rsyslog -v; /etc/rsyslog.conf; /etc/init.d/rsyslog/ restart
* Apache: - Webserver: yum install httpd -y; /etc/ http/conf/httpd.conf; vi /etc/sysconfig/iptables, -A INPUT -m state --state NEW -M tcp -p tcp --dport 80 -j ACCEPT; service iptables restart ; service httpd start.
* Mysql: yum install mysql-server -y; service mysqld start;
* Php: yum install php php-mysql -y; vi /var/www/html/info.php; <?php phpinfo(); ?>; service restart httpd
* LVM: pvcreate, vgcreate, lvcreate
* Ports: ftp: 21; ssh:22; telnet:23; dns:53; http: 80, https:443

**User & Group Management**

* user account file: /etc/passwd - 6 fields: 1. login name; 2. x - encripted passwd info stored in /etc/shadow; 3. unique user id; 4. GID - group ID; 5. user account full name; 6. Home directory.
* useradd <user>; useradd -u <user>; useradd -g <user>; useradd -G <user>; useradd -c <user>; useradd -M <user>; userad -e <date> <username>; userad -e <date> -f <# of days to expire> <username>; userad -s /sbin/nologin <username>; userad -m -d <homediriectory> -s /bin/bash -c <"comment"> -u <username>
* usermod <newname> <oldname>; usermod -s <newshell> ,username>userdel <username>; userdel -r <username>;
* groupadd <groupname>; groupadd -g <group#> <group>; groupoadd <username>; gpasswd -r <username>; gpasswd <username>;groupmod -n <newname> <oldname>; groupmod -g <group#> <group>; groupdel <groupname>; groupdel <username>;
* Change Group Ownership Of a file
* chown <oldgroupname>: <newgroupname> <filename>; or chgrp <newgroup> <filename>
* SET UID, GID, STICKY BIT
* uid = 4; chmod u+s <filename> or chmo 4755 <filename>
* gid = 2; chmo 2755 <directoryname> or g+s

**FILES & DIRECTORY PERMISSIONS**

* ls -l; ll
* -(file) rw-(owner) r--(group) r--(other) <#ofiles> root(owner) root(group) <size> <date> <filename>
* d(irectory) rw-(owner) r--(group) r--(other) <#ofiles> root(owner) root(group) <size> <date> <filename>
* r = read, w = write, x = execute.
* r =4, w = 2; x = 1.
* u = owner; g = group, o = other
* file: - rw- r-- r-- = 644
* - rwx -rw- r-- = 764
* -rwx r-x -r-x = 755
* chmod u + x <filename>; chmod 755 <file1> <file2> <file3> (for mulitiple files)
* ACCESS CONTROL LISTS (ACLs)
* getfacl <filename>
* setfacl -m u:<username>:<permission> <directory>

**INVENTORY COMMANDS**

**Display Memory:** cat /proc/meminfo, free –m

**Display Numbers of Processors (CPUs):** lscpu

**Display CPU type, speed etc:** cat /proc/cpuinfo, uname –p

**Display Kernel Bits type (64bits or 32 bits):** lscpu, uname –p, getconf LONG\_BIT

**Display Disk size, label, partitions etc**: cat /proc/partitions, ls /dev/sd\*, fdisk /dev/sd\*, fdisk -l

**Displays System release, platform, hostname etc**: uname –a, cat /etc/issue, cat /proc/release, lsb\_release –a

**Display Disk usage:** df –h

**Display Date:** date

**Change Date:** date MMDDhhmmyy

**IP Address:** ifconfig, nm-tool, ip –a,

**DNS:** cat /ete/resolve.conf, nm-tool

**Find How Long system has been running:** w, uptime

**Display all open ports on the server:** netstat – an

**Display the routing table:** netstat –r

**Display default run level:** who –r; cat /etc/inittab

**Display Network Interface**: netstat –r, netstat –i

**Display Server Type:** arch

**PROCESS MANAGEMENT**

|  |  |  |
| --- | --- | --- |
| **Command** | **Description** |  |
| **bg** | To send a process to the background |  |
| **fg** | To run a stopped process in the foreground | fg <jobname> |
| **top** | Details on all Active Processes | Press ‘q’ to get out |
| **ps** | Give the status of processes running for a user | ps ux, (display all processes running by a user)  ps –ef |
| **ps PID** | Gives the status of a particular process |  |
| **Pidof** | Gives the Process ID (PID) of a process | pidof <process name> |
| **kill PID** | Kills a process |  |
| **nice** | Starts a process with a given priority | nice -n <Nice value> <process name> |
| **renice** | Changes priority of an already running process | renice <nice value> -p <PID> |
| **df** | Gives free hard disk space on your system | df -h |

**PACKAGE MANAGEMENT**

**Check installed packages:** rpm –qa | grep <pkg>

**YUM – Yellow Dog Updater, Modified, located in**: /etc/yum.conf

**Repository info:** /etc/yum.repos.d

**List enabled yum repositories:** yum repolist

**Install package**: yum install <pkg> -y

**Remove package:** yum remove <pkg> -y

**Update package**: yum upate <pkg> -y

**Update System:** yum upate

**List Package**: yum list <pkg>

**List all installed packages:** yum list installed | less

**List all available packages:** yum list | less

**Search Package:** yum search <pkg>

**Create repository from a url or location**: yum-config-manager –add-repo=<url> or <file location>; then vi into: /etc/yum.repos.d and add gpgcheck=0

**Clean yum cache**: yum clean all

**Display group packages**: yum grouplist

**Install a group of packages:** yum group install

**OSI MODEL**

1. Physical: The [physical layer](https://en.wikipedia.org/wiki/Physical_layer) has the following major functions:

* It defines the [electrical](https://en.wikipedia.org/wiki/Electrical) and physical specifications of the data connection. It defines the relationship between a device and a physical [transmission medium](https://en.wikipedia.org/wiki/Transmission_medium) (Ethernet cable, switch, cat5 cable)

1. Data link At OSI Model, Layer 2, data packets are [encoded](http://www.webopedia.com/TERM/E/encoding.html) and decoded into bits. It furnishes [transmission protocol](http://www.webopedia.com/TERM/T/TCP_IP.html) knowledge and management and handles errors in the physical layer,
2. Network layer Layer 3 provides [switching](http://www.webopedia.com/TERM/P/packet_switching.html) and [routing](http://www.webopedia.com/TERM/R/routing.html) technologies, creating logical paths, known as [virtual circuits](http://www.webopedia.com/TERM/V/virtual_circuit.html), for transmitting data from [node](http://www.webopedia.com/TERM/N/node.html) to node. Routing and forwarding are functions of this layer, as well as [addressing](http://www.webopedia.com/DidYouKnow/Internet/IPaddressing.asp),[internet working](http://www.webopedia.com/TERM/I/internetworking.html), error handling, [congestion](http://www.webopedia.com/TERM/C/congestion.html) control and packet sequencing.
3. Transport layer OSI Model, Layer 4, provides transparent transfer of data between end systems, or [hosts](http://www.webopedia.com/TERM/H/host.html), and is responsible for end-to-end error recovery and [flow control](http://www.webopedia.com/TERM/F/flow_control.html). It ensures complete data transfer.

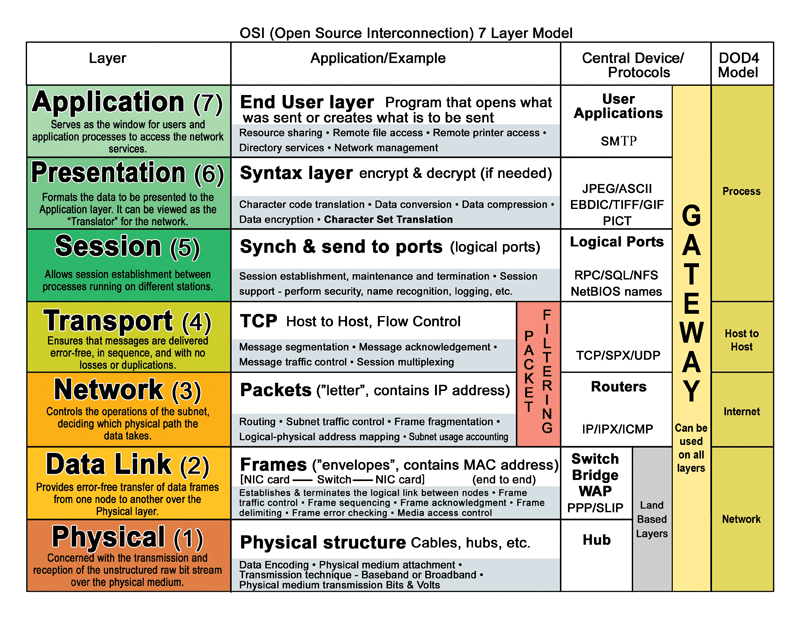
TCP or UDP

1. Session This layer establishes, manages and terminates connections between [applications](http://www.webopedia.com/TERM/A/application.html). The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. NFS Putty
2. PRESENTATION

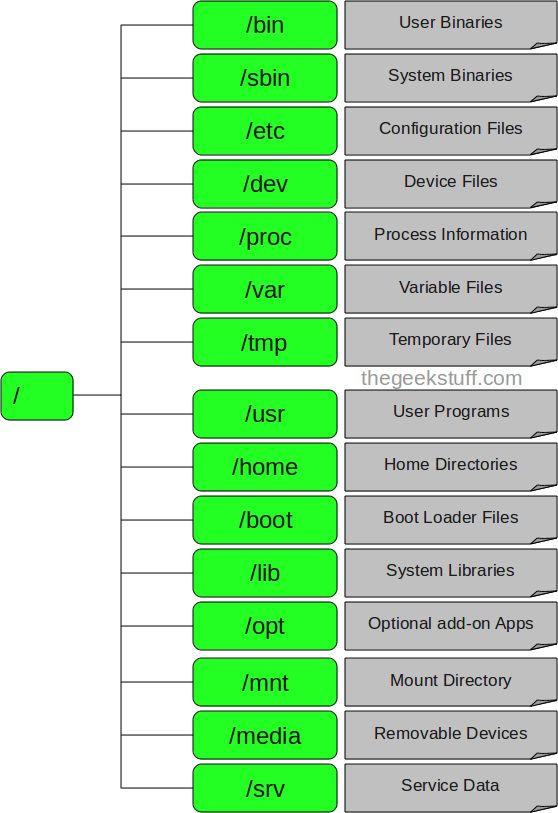
This layer provides independence from differences in data representation (e.g., [encryption](http://www.webopedia.com/TERM/E/encryption.html)) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a [network](http://www.webopedia.com/TERM/N/network.html)

1. APLICATION OSI Model, Layer 7, supports [application](http://www.webopedia.com/TERM/A/application.html) and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data [syntax](http://www.webopedia.com/TERM/S/syntax.html) are identified. Everything at this layer is application-specific. This layer provides application services for [file transfers](http://www.webopedia.com/Communications/File_Transfers/), [e-mail](http://www.webopedia.com/TERM/E/e_mail.html), and other [network](http://www.webopedia.com/TERM/N/network.html) [software](http://www.webopedia.com/TERM/S/software.html) services. [Telnet](http://www.webopedia.com/TERM/T/Telnet.html) and [FTP](http://www.webopedia.com/TERM/F/FTP.html) are applications that exist entirely in the application level.

**OSI MODEL**



**THE ROOT FILE SYSTEM**



**BOOT UP PROCESS & UNIX RUN LEVELS**

1. BIOS

Performs some system integrity checks. Searches, loads, and executes the boot loader program. Once the boot loader program is detected and loaded into the memory, BIOS gives the control to it. So, in simple terms BIOS loads and executes the MBR boot loader.

2. MBR

* MBR stands for Master Boot Record. It is located in the 1st sector of the bootable disk. Typically /dev/hda, or /dev/sda. It contains information about GRUB (or LILO in old systems). So, in simple terms, the MBR loads and executes the GRUB boot loader.

3. GRUB

* GRUB stands for Grand Unified Bootloader. If you have multiple kernel images installed on your system, you can choose which one to be executed. GRUB displays a splash screen, waits for few seconds, if you don’t enter anything, it loads the default kernel image as specified in the grub configuration file. Grub configuration file is /boot/grub/grub.conf. So, in simple terms GRUB just loads and executes Kernel and initrd images.

4. Kernel

* Mounts the root file system as specified in the “root=” in grub.conf. Kernel executes the /sbin/init program. initrd stands for Initial RAM Disk. initrd is used by kernel as temporary root file system until kernel is booted and the real root file system is mounted. It also contains necessary drivers compiled inside, which helps it to access the hard drive partitions, and other hardware.

5. Init

* Looks at the /etc/inittab file to decide the Linux run level.
* Following are the available run levels
  + 0 – halt
  + 1 – Single user mode
  + 2 – Multiuser, without NFS
  + 3 – Full multiuser mode
  + 4 – unused
  + 5 – X11
  + 6 – reboot
* Init identifies the default init level from /etc/inittab and uses that to load all appropriate program. Typically you would set the default run level to either 3 or 5.

6. Runlevel programs

* When the Linux system is booting up, you might see various services getting started. For example, it might say “starting sendmail …. OK”. Those are the runlevel programs, executed from the run level directory as defined by your run level.
* Depending on your default init level setting, the system will execute the programs from one of the following directories.
  + Run level 0 – /etc/rc.d/rc0.d/
  + Run level 1 – /etc/rc.d/rc1.d/
  + Run level 2 – /etc/rc.d/rc2.d/
  + Run level 3 – /etc/rc.d/rc3.d/
  + Run level 4 – /etc/rc.d/rc4.d/
  + Run level 5 – /etc/rc.d/rc5.d/
  + Run level 6 – /etc/rc.d/rc6.d/
* Please note that there are also symbolic links available for these directory under /etc directly. So, /etc/rc0.d is linked to /etc/rc.d/rc0.d.
* Under the /etc/rc.d/rc\*.d/ directories, you would see programs that start with S and K.
* Programs starts with S are used during startup. S for startup.
* Programs starts with K are used during shutdown. K for kill.
* There are numbers right next to S and K in the program names. Those are the sequence number in which the programs should be started or killed.
* For example, S12syslog is to start the syslog deamon, which has the sequence number of 12. S80sendmail is to start the sendmail daemon, which has the sequence number of 80. So, syslog program will be started before sendmail.

**Some Linux Admin Tools**

**Exit or return code**: echo $?

**Display in sequence**: seq <range>

**Display a page at a time**: more; less

**Change file contents without vi**: sed. Eg, sed –i `s/<string to be replaced>/<replacement>/g` <filename>

**Sort file alphabetically**: sort –n <filename>

**Filter specific output or string from a file:** awk eg, awk –F”.” `{print $1}` <filename>

**Copy file (same with scp)**:

cp <source> <destination>

cp <option> <source> <destination>

**Preserve file options:** cp –p <source> <destination>

**Copy recursively:** cp –R source> <destination>

**Copy all files in a directory to a new directory**: cp \* <old dir> <new dir>

**The Find Command**

find <source location> -<name> -exec <command> {} <new-test-file-name> \;