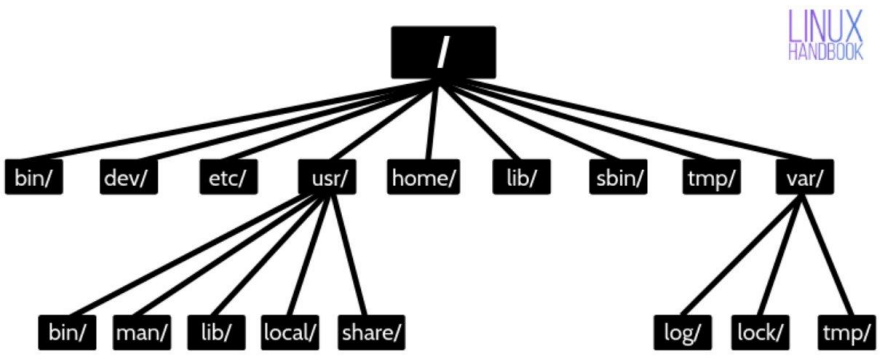
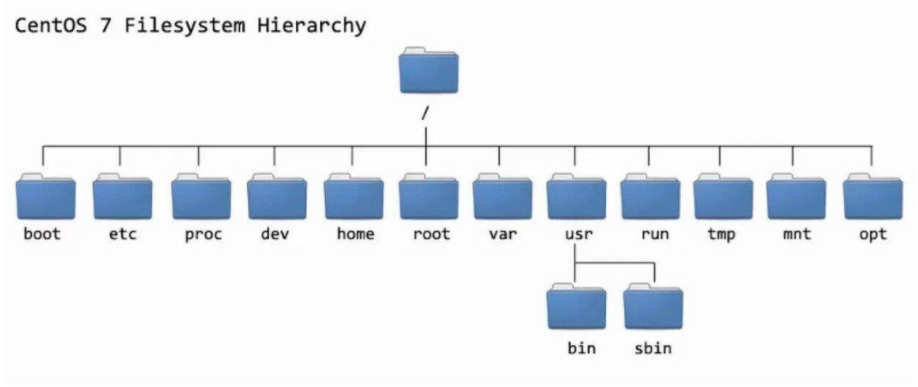
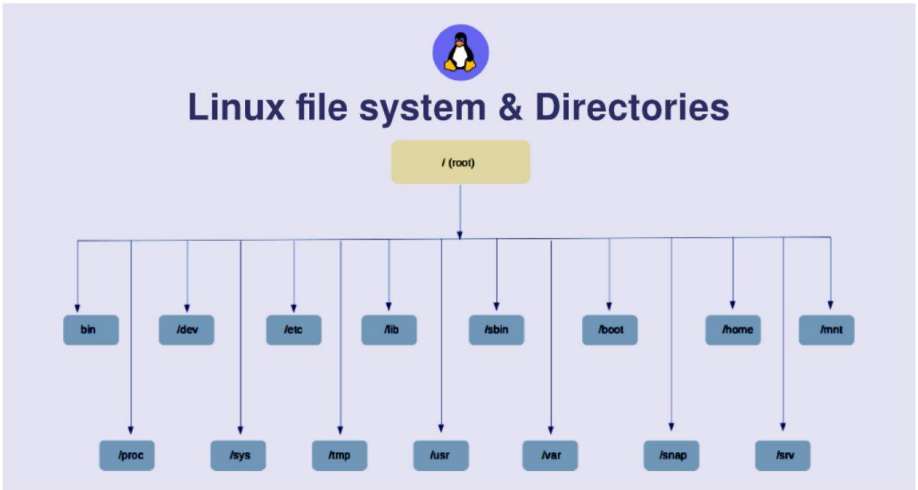
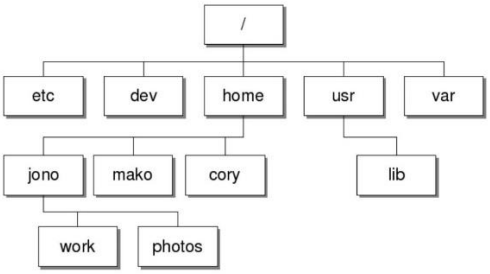
For NotePad : https://www.notion.so/

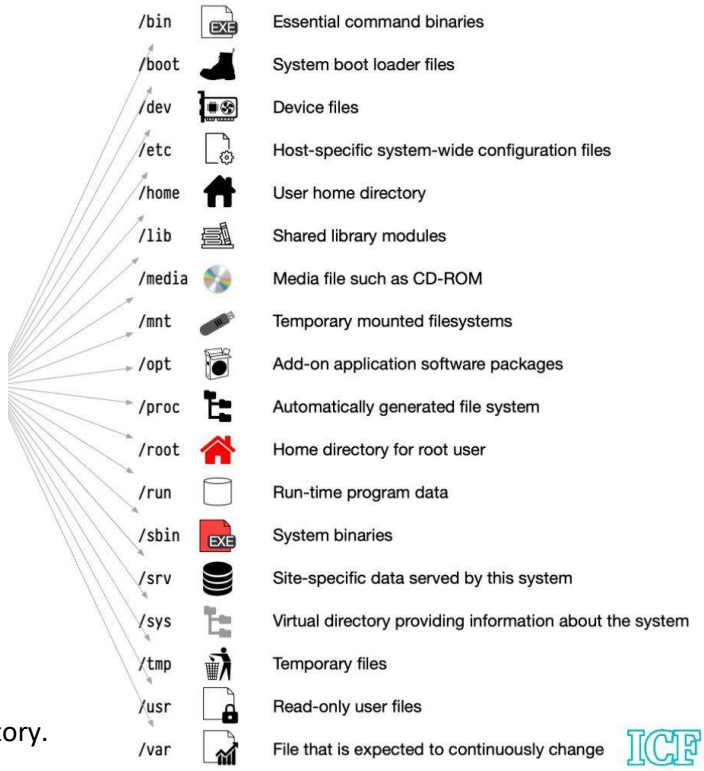
**Linux Directory History**






**Linux directory structure :** [link]

**. / – Root**
Every single file and directory starts from the root directory.
Only root user has write privilege under this directory.
Please note that /root is root user's home directory, which is not same as /.

**2. /bin – User Binaries**
Contains binary executables.
Common linux commands you need to use in single-user modes are located under this directory.
Commands used by all the users of the system are located here.
For example: ps, ls, ping, grep, cp.

**3. /sbin – System Binaries**
Just like /bin, /sbin also contains binary executables.
But, the linux commands located under this directory are used typically by system aministrator, for system maintenance purpose.
For example: iptables, reboot, fdisk, ifconfig, swapon

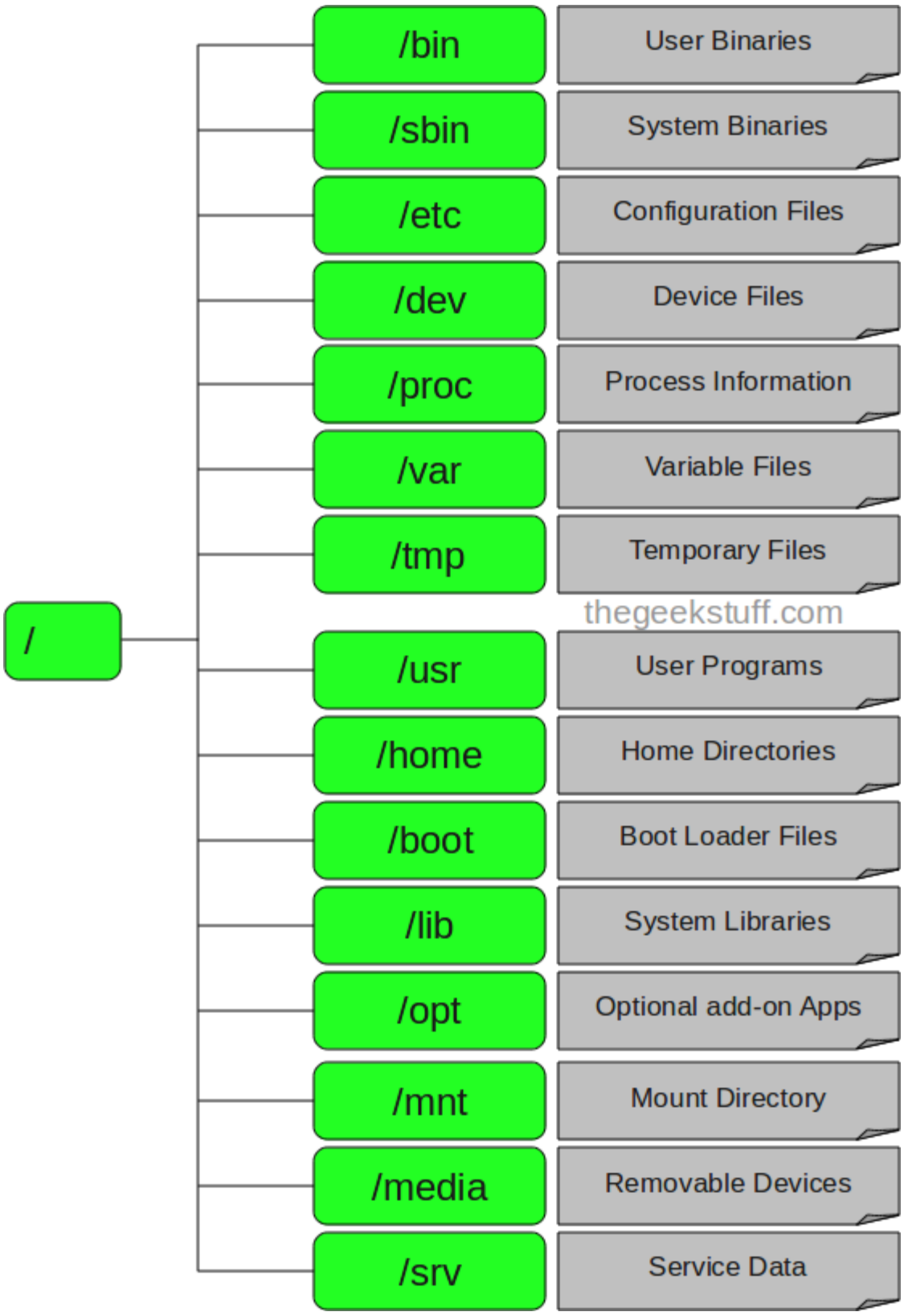
**4. /etc – Configuration Files**
Contains configuration files required by all programs.
This also contains startup and shutdown shell scripts used to start/stop individual programs.
For example: /etc/resolv.conf, /etc/logrotate.conf

**5. /dev – Device Files**
Contains device files.
These include terminal devices, usb, or any device attached to the system.
For example: /dev/tty1, /dev/usbmon0

**6. /proc – Process Information**
Contains information about system process.
This is a pseudo filesystem contains information about running process. For example: /proc/{pid} directory contains information about the process with that particular pid.
This is a virtual filesystem with text information about system resources. For example: /proc/uptime

**7. /var – Variable Files**
var stands for variable files.
Content of the files that are expected to grow can be found under this directory.
This includes — system 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);

**8. /tmp – Temporary Files**
Directory that contains temporary files created by system and users.
Files under this directory are deleted when system is rebooted.
**9. /usr – User Programs**
Contains binaries, libraries, documentation, and source-code for second level programs.
/usr/bin contains binary files for user programs. If you can't find a user binary under /bin, look under /usr/bin. For example: at, awk, cc, less, scp
/usr/sbin contains binary files for system administrators. If you can't find a system binary under /sbin, look under /usr/sbin. For example: atd, cron, sshd, useradd, userdel
/usr/lib contains libraries for /usr/bin and /usr/sbin
/usr/local contains users programs that you install from source. For example, when you install apache from source, it goes under /usr/local/apache2
**10. /home – Home Directories**
Home directories for all users to store their personal files.
For example: /home/john, /home/nikita
**11. /boot – Boot Loader Files**
Contains boot loader related files.
Kernel initrd, vmlinux, grub files are located under /boot
For example: initrd.img-2.6.32-24-generic, vmlinuz-2.6.32-24-generic
**12. /lib – System Libraries**
Contains library files that supports the binaries located under /bin and /sbin
Library filenames are either ld* or lib*.so.*
For example: ld-2.11.1.so, libncurses.so.5.7
**13. /opt – Optional add-on Applications**
opt stands for optional.
Contains add-on applications from individual vendors.
add-on applications should be installed under either /opt/ or /opt/ sub-directory.
**14. /mnt – Mount Directory**
Temporary mount directory where sysadmins can mount filesystems.
**15. /media – Removable Media Devices**
Temporary mount directory for removable devices.
For examples, /media/cdrom for CD-ROM; /media/floppy for floppy drives; /media/cdrecorder for CD writer
**16. /srv – Service Data**
srv stands for service.
Contains server specific services related data.
For example, /srv/cvs contains CVS related data.


/
/bin
User Binaries
/sbin
System Binaries
/etc
Configuration Files
/dev
Device Files
/proc
Process Information
/var
Variable Files
/tmp
Temporary Files
thegeekstuff.com
/usr
User Programs
/home
Home Directories
/boot
Boot Loader Files
/lib
System Libraries
/opt
Optional add-on Apps
/mnt
Mount Directory
/media
Removable Devices
/srv
Service Data

**Linux Common Commands**

# Top 50 Linux Commands you must know

| | | | | |
|---|---|---|---|---|
| 1. is | 1. clear | 1. diff | 1. kill and killall | 1. apt, pacman, yum, rpm |
| 2. pwd | 2. echo | 2. cmp | 2. df | 2. sudo |
| 3. cd | 3. less | 3. comm | 3. mount | 3. cal |
| 4. mkdir | 4. man | 4. sort | 4. chmod | 4. alias |
| 5. mv | 5. unman | 5. export | 5. chown | 5. dd |
| 6. cp | 6. whoami | 6. zip | 6. ifconfig | 6. whereis |
| 7. rm | 7. tar | 7. unzip | 7. traceroute | 7. whatis |
| 8. touch | 8. grep | 8. ssh | 8. wget | 8. top |
| 9. in | 9. head | 9. service | 9. ufw | 9. useradd |
| 10. cat | 10. tail | 10. ps | 10. iptables | 10. passwd |

## Common Linux Commands

| command | description | command | description | command | description |
|---|---|---|---|---|---|
| cd | change directories | find | find something | pwd | present working directory (where am I) |
| chmod | change read, write, execute (rwx) permissions | grep | find something | rm | remove |
| chown | change owner | history | history | scp | secure copy |
| clear | clear | man | manual | ssh | secure shell (remote login) |
| cp | copy | mkdir | make directory | su | swith users |
| crontab | cronological listing of jobs | mv | move/ rename | sudo | super user do (override) |
| df | disk free | netstat | check ports | tar | compress/extract directory |
| du | disk usage | nslookup | lookup ip address or hostname | touch | Create a file |
| exit | exit | | | | |

# Most Used Linux Commands

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | ls | 22 | ifconfig | 43 | lsof | 64 | parted |
| 2 | pwd | 23 | ip | 44 | dig | 65 | wc |
| 3 | cd | 24 | wget | 45 | nslookup | 66 | ls |
| 4 | clear | 25 | curl | 46 | du | 67 | nmap |
| 5 | mkdir | 26 | apt | 47 | tree | 68 | dmesg |
| 6 | mv | 27 | apt-get | 48 | ss | 69 | chattr |
| 7 | cp | 28 | yum | 49 | partx | 70 | usermod |
| 8 | rmdir | 29 | dnf | 50 | uptime | 71 | free |
| 9 | touch | 30 | rpm | 51 | tr | 72 | cron |
| 10 | cat | 31 | alias | 52 | ping | 73 | mysql |
| 11 | echo | 32 | dd | 53 | zcat | 74 | sdiff |
| 12 | less | 33 | top | 54 | xargs | 75 | history |
| 13 | tar | 34 | useradd | 55 | rm | 76 | netstat |
| 14 | grep | 35 | sleep | 56 | stat | 77 | sftp |
| 15 | head | 36 | screen | 57 | who | 78 | tcpdump |
| 16 | tail | 37 | pv | 58 | locate | 79 | scp |
| 17 | sort | 38 | fgrep | 59 | host | 80 | rsync |
| 18 | ps | 39 | dir | 60 | find | 81 | fsck |
| 19 | kill | 40 | egrep | 61 | fuser | 82 | bc |
| 20 | df | 41 | ssh | 62 | at | 83 | chage |
| 21 | chown | 42 | fd | 63 | fdisk | 84 | ffmpeg |

| File Commands | | |
|---|---|---|
| 1. | ls | Directory listing |
| 2. | ls -al | Formatted listing with hidden files |
| 3. | ls -lt | Sorting the Formatted listing by time modification |
| 4. | cd dir | Change directory to dir |
| 5. | cd | Change to home directory |
| 6. | pwd | Show current working directory |
| 7. | mkdir dir | Creating a directory dir |
| 8. | cat >file | Places the standard input into the file |
| 9. | more file | Output the contents of the file |
| 10. | head file | Output the first 10 lines of the file |
| 11. | tail file | Output the last 10 lines of the file |
| 12. | tail -f file | Output the contents of file as it grows,starting with the last 10 lines |
| 13. | touch file | Create or update file |
| 14. | rm file | Deleting the file |
| 15. | rm -r dir | Deleting the directory |
| 16. | rm -f file | Force to remove the file |
| 17. | rm -rf dir | Force to remove the directory dir |
| 18. | cp file1 file2 | Copy the contents of file1 to file2 |
| 19. | cp -r dir1 dir2 | Copy dir1 to dir2;create dir2 if not present |
| 20. | mv file1 file2 | Rename or move file1 to file2,if file2 is an existing Directory |
| 21. | ln -s file link | Create symbolic link link to file |
| Process management | | |
| 1. | ps | To display the currently working processes |
| 2. | top | Display all running process |
| | | |

| | | |
|---|---|---|
| 3. | kill pid | Kill the process with given pid |
| 4. | killall proc | Kill all the process named proc |
| 5. | pkill pattern | Will kill all processes matching the pattern |
| 6. | bg | List stopped or background jobs,resume a stopped job in the background |
| 7. | fg | Brings the most recent job to foreground |
| 8. | fg n | Brings job n to the foreground |

File permission

| | | |
|---|---|---|
| 1. | chmod octal file | Change the permission of file to octal,which can be found separately for user,group,world by adding,<br>• 4-read(r)<br>• 2-write(w)<br>• 1-execute(x) |

Searching

| | | |
|---|---|---|
| 1. | grep pattern file | Search for pattern in file |
| 2. | grep -r pattern dir | Search recursively for pattern in dir |
| 3. | command \| grep pattern | Search pattern in the output of a command |
| 4. | locate file | Find all instances of file |
| 5. | find . -name filename | Searches in the current directory (represented by a period) and below it, for files and directories with names starting with filename |
| 6. | pgrep pattern | Searches for all the named processes , that matches with the pattern and, by default, returns their ID |

System Info

| | | |
|---|---|---|
| 1. | date | Show the current date and time |
| 2. | cal | Show this month's calender |
| 3. | uptime | Show current uptime |
| 4. | w | Display who is on line |
| 5. | whoami | Who you are logged in as |

| | | |
|---|---|---|
| 6. | finger user | Display information about user |
| 7. | uname -a | Show kernel information |
| 8. | cat /proc/cpuinfo | Cpu information |
| 9. | cat proc/meminfo | Memory information |
| 10. | man command | Show the manual for command |
| 11. | df | Show the disk usage |
| 12. | du | Show directory space usage |
| 13. | free | Show memory and swap usage |
| 14. | whereis app | Show possible locations of app |
| 15. | which app | Show which applications will be run by default |

Compression

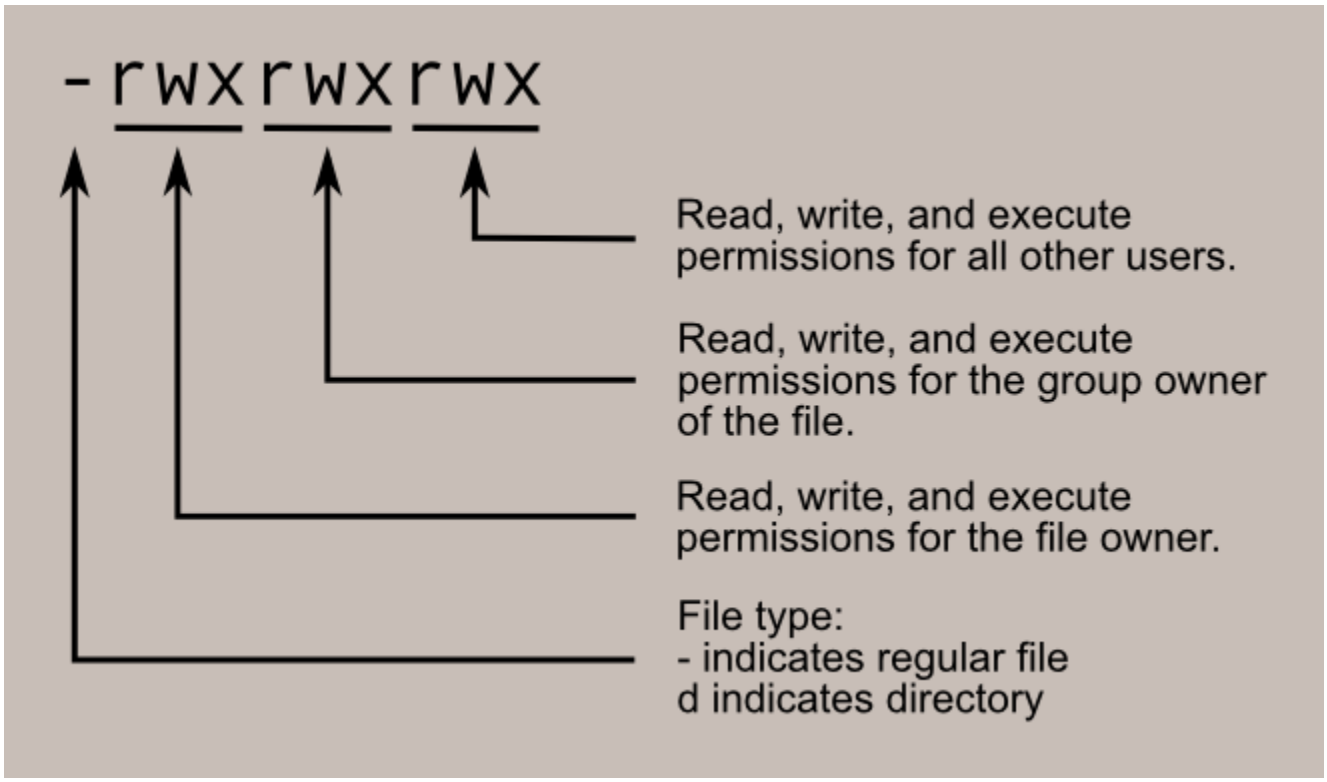
| | | |
|---|---|---|
| 1. | tar cf file.tar file | Create tar named file.tar containing file |
| 2. | tar xf file.tar | Extract the files from file.tar |
| 3. | tar czf file.tar.gz files | Create a tar with Gzip compression |
| 4. | tar xzf file.tar.gz | Extract a tar using Gzip |
| 5. | tar cjf file.tar.bz2 | Create tar with Bzip2 compression |
| 6. | tar xjf file.tar.bz2 | Extract a tar using Bzip2 |
| 7. | gzip file | Compresses file and renames it to file.gz |
| 8. | gzip -d file.gz | Decompresses file.gz back to file |

Network

| | | |
|---|---|---|
| 1. | ping host | Ping host and output results |
| 2. | whois domain | Get whois information for domains |
| 3. | dig domain | Get DNS information for domain |
| 4. | dig -x host | Reverse lookup host |
| 5. | wget file | Download file |
| 6. | wget -c file | Continue a stopped download |

| Shortcuts | | |
|---|---|---|
| 1. | ctrl+c | Halts the current command |
| 2. | ctrl+z | Stops the current command, resume with fg in the foreground or bg in the background |
| 3. | ctrl+d | Logout the current session, similar to exit |
| 4. | ctrl+w | Erases one word in the current line |
| 5. | ctrl+u | Erases the whole line |
| 6. | ctrl+r | Type to bring up a recent command |
| 7. | !! | Repeats the last command |
| 8. | exit | Logout the current session |
| | | |

**Linux Permission Mode**



drwxrwxrwx

d = Directory
r = Read
w = Write
x = Execute

chmod 777

rwx | rwx | rwx
Owner | Group | Others

| | | |
|---|---|---|
| 7 | rwx | 111 |
| 6 | rw- | 110 |
| 5 | r-x | 101 |
| 4 | r-- | 100 |
| 3 | -wx | 011 |
| 2 | -w- | 010 |
| 1 | --x | 001 |
| 0 | --- | 000 |

| Octal | Decimal | Permission | Representation |
|---|---|---|---|
| 000 | 0 (0+0+0) | No Permission | --- |
| 001 | 1 (0+0+1) | Execute | --x |
| 010 | 2 (0+2+0) | Write | -w- |
| 011 | 3 (0+2+1) | Write + Execute | -wx |
| 100 | 4 (4+0+0) | Read | r-- |
| 101 | 5 (4+0+1) | Read + Execute | r-x |
| 110 | 6 (4+2+0) | Read + Write | rw- |
| 111 | 7 (4+2+1) | Read + Write + Execute | rwx |

| | | |
|---|---|---|
| ———- | 0000 | no permissions |
| -rwx—— | 0700 | **read, write, & execute only for owner** |
| -rwxrwx— | 0770 | read, write, & execute for owner and group |
| -rwxrwxrwx | 0777 | read, write, & execute for owner, group and others |
| —x–x–x | 0111 | execute |
| –w–w–w- | 0222 | write |
| –wx-wx-wx | 0333 | write & execute |
| -r–r–r– | 0444 | read |
| -r-xr-xr-x | 0555 | read & execute |
| -rw-rw-rw- | 0666 | read & write |
| -rwxr—– | 0740 | owner can read, write, & execute; group can only read; others have no permissions |

# Basic Linux Command

File and Directory Manipulation
pwd: Display path of current directory you're in
ls: List all files and folders in the current directory
ls -la: List detailed list of files and folders, including hidden ones
Change to a specific directory
cd: Change to home directory
cd /user/Desktop: Change to a specific directory called Desktop
cd .. : Move back a directory
Create a directory/folder
mkdir <dir>: Create a new directory
mkdir /home/Desktop/dir: Create a directory in a specific location
Create and edit files
touch <file>: Create an empty file
nano <file>: Edit an existing file or create it if it doesn't exist.
Alternatives to nano text editor: vim, emacs
Copy, move and rename files and directories
cp <file1> <file2>: Create a copy of a file
cp -r <dir1> <dir2>: Create a copy of a directory and everything in it
cp <file> /home/Desktop/file2: Create a copy of a file in a different directory and name it file2.
mv <file> /home/Desktop: Move a file to a specific directory (overwrites any existing file with the same name)
mv <dir> /home/Desktop: Move a directory to another location
mv <dir1> <dir2>: Rename a file OR directory (dir1 -> dir2)
Delete files
rm <file>: Delete a file
rm -f <file>: Force delete a file
Careful now..
rm -r <dir>: Delete a directory and its contents
rm -rf <dir>: Force delete a directory and its contents
Careful when using this command as it will delete everything inside the directory
Output and analyze files
cat <file>: Display/output the contents of a file
less <file>: Display the contents of a file with scroll (paginate) ability (press q to quit)
head <file>: Display the first ten lines in a file
head -20 <file>: Display the first 20 lines in a file
tail <file>: Display the last ten lines in a file
tail -20 <file>: Display the last 20 lines in a file
diff <file1> <file2>: Check the difference between two files (file1 and file2)

Basic linux command
System & User Information
cal: Display monthly calendar
date: Check date and time
uptime: Check system uptime and currently logged in users
uname -a: Display system information.
dmesg: Display kernel ring buffer
poweroff: Shutdown system
reboot: Reboot system
View disk and memory usage
df -h: Display disk space usage

fdisk -l: List disk partition tables
free: Display memory usage
cat /proc/meminfo: Display memory information
cat /proc/cpuinfo: Display cpu information
View user information
whoami: Output your username
w: Check who's online
history: View a list of your previously executed commands
View last logged in users and information
last: Display last login info of users
last <user>: Display last login info of a specific user
finger <user>: Display user information

Basic linux command
Installing & Upgrading Packages
Search for packages
apt-cache pkgnames: List all available packages
apt search <name>: Search for a package and its description
apt show <name>: Check detailed description of a package
Install packages
apt-get install <name>: Install a package
apt-get install <name1> <name2>: Install multiple packages
Update, upgrade & cleanup
apt-get update: Update list of available packages
apt-get upgrade: Install the newest version of available packages
apt-get dist-upgrade: Force upgrade packages.
apt-get autoremove: Remove installed packages that are no longer needed
apt-get clean: Free up disk space by removing archived packages
Delete packages
apt-get remove: Uninstall a package
apt-get remove --purge: Uninstall a package and remove its configuration files

Basic linux command
Processes & Job Management
kill <PID>: Kill a processes by PID #.
killall <processes>: Kill all processes with specified name.
Start, stop, resume jobs
jobs: Display the status of current jobs
jobs -l: Display detailed info about each job
jobs -r: Display only running jobs
bg: View stopped background jobs or resume job in the background
fg: Resume recent job in the foreground
fg <job>: Bring specific job to the foreground.

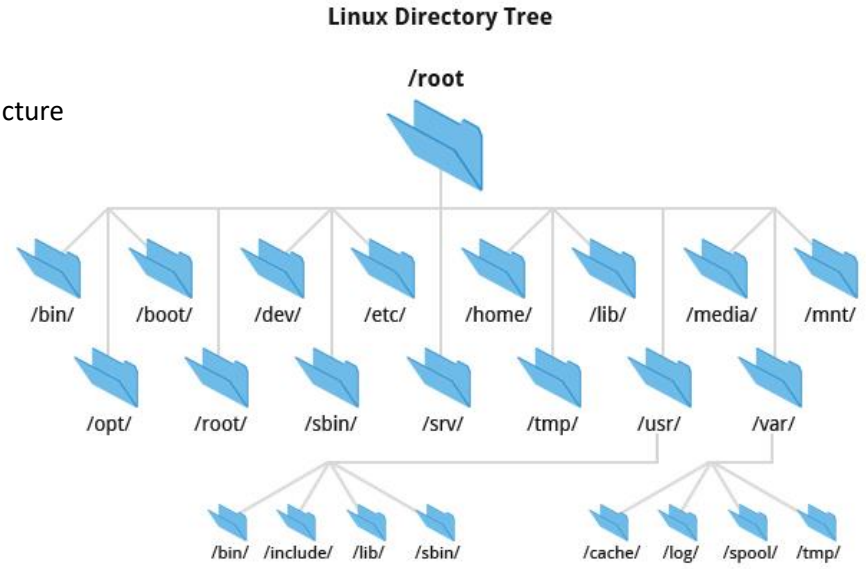
Basic linux command
Networking Utilities
ping <host>: Ping a host
whois <domain/IP>: Get whois information about a domain or IP.

dig <domain/IP>: Get DNS information
nslookup: <NS>: Get nameserver information
ifconfig: Configure/display network interfaces
iwconfig: Configure/display wireless network interfaces
netstat -r: Display kernel IP routing tables
netstat -antp: Check for established and listening ports/connections
arp -a: Display ARP cache tables for all interfaces

Basic linux command
Keyboard Shortcuts

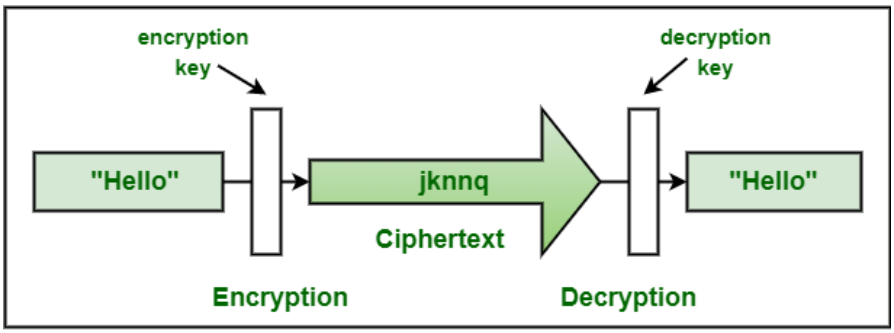
| | |
|---|---|
| CTRL + L | Clear terminal screen |
| CTRL + D | Log out of current session |
| CTRL + C | Stop (halt) currently running command/processes |
| CTRL + Z | Suspend (pause) currently running command/processes |
| CTRL + W | Delete the last word/argument |
| CTRL + E | Jump (skip) to the very LAST line |
| CTRL + A | Jump (skip) to the very FIRST line |
| CTRL + F | Move cursor one letter forward |
| CTRL + B | Move cursor one letter backward |
| CTRL + U | Cut (copy) everything BEFORE the cursor |
| CTRL + K | Cut (copy) everything AFTER the cursor |
| CTRL + Y | Paste previously copied text |
| clear | Clear terminal screen |
| reset | Fix display errors |
| exit | Exit (log out) current session |
| tab | Auto-complete |
| man <cmd> | Read the manual page of a command |
| which <cmd> | Locate the path name of a command |
| !! | Repeat last command |
| sudo !! | Repeat last command as sudo (admin/root) user |

Kali linux Directory Structure
Linux Directory Tree



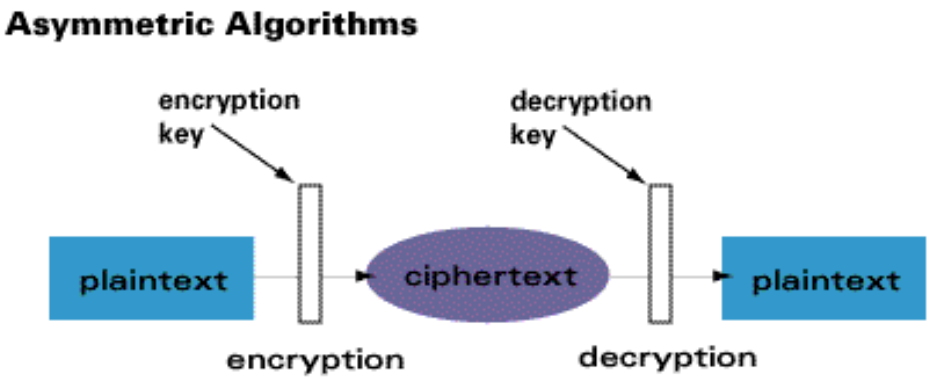

HACKERS ROCKS

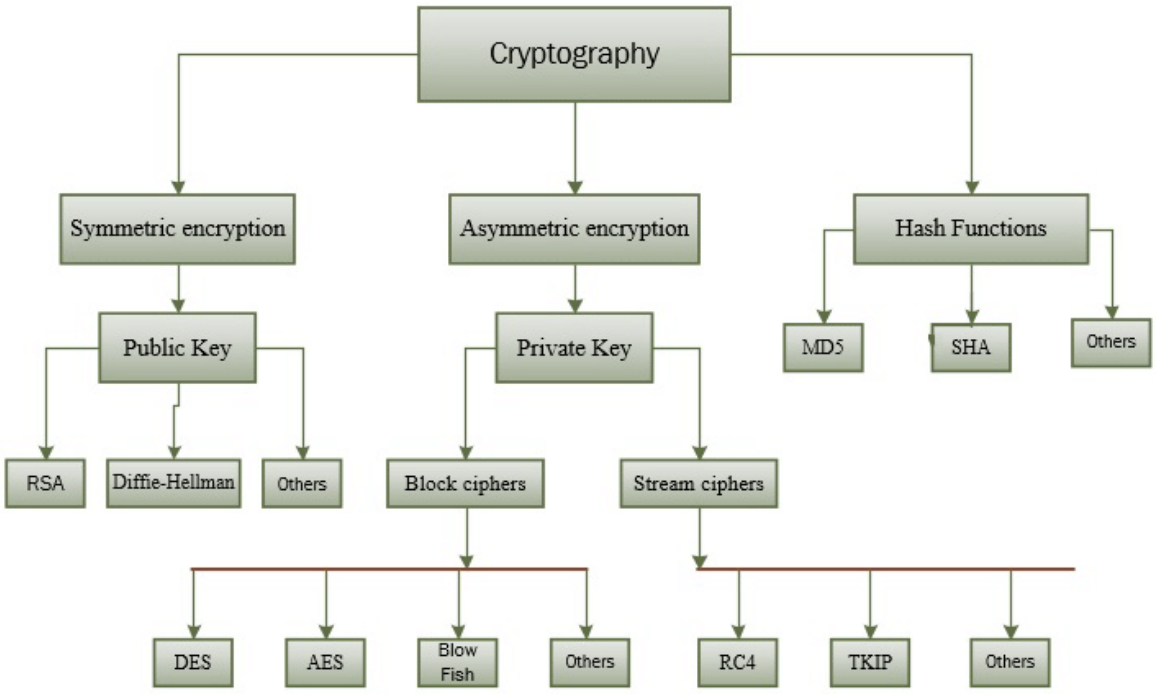
**Cryptography:** Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages




Cryptography

| Name | Description |
|---|---|
| Plain Text | Readable Text |
| Cipher Text | Unreadable Text |
| Keys | Use for create Cipher Text |
| Encrypt | Convert Plain text to Cipher Text |
| Decrypt | Convert Cipher text to Plain Text |
| Hash | Cipher text after using Hashing Algorithm |






**Type of Crypto**

There are 3 types of Crypto:
Symmetric-Key Cryptography, Asymmetric-Key Cryptography, Hash Function Cryptography

**Symmetric-Key Cryptography:** Symmetric Cryptography is type of cryptography where both sender and receiver use same private key.

**Example:**

Plain Text: Hacker
Cypher Text: Ohjrly
Key: 7

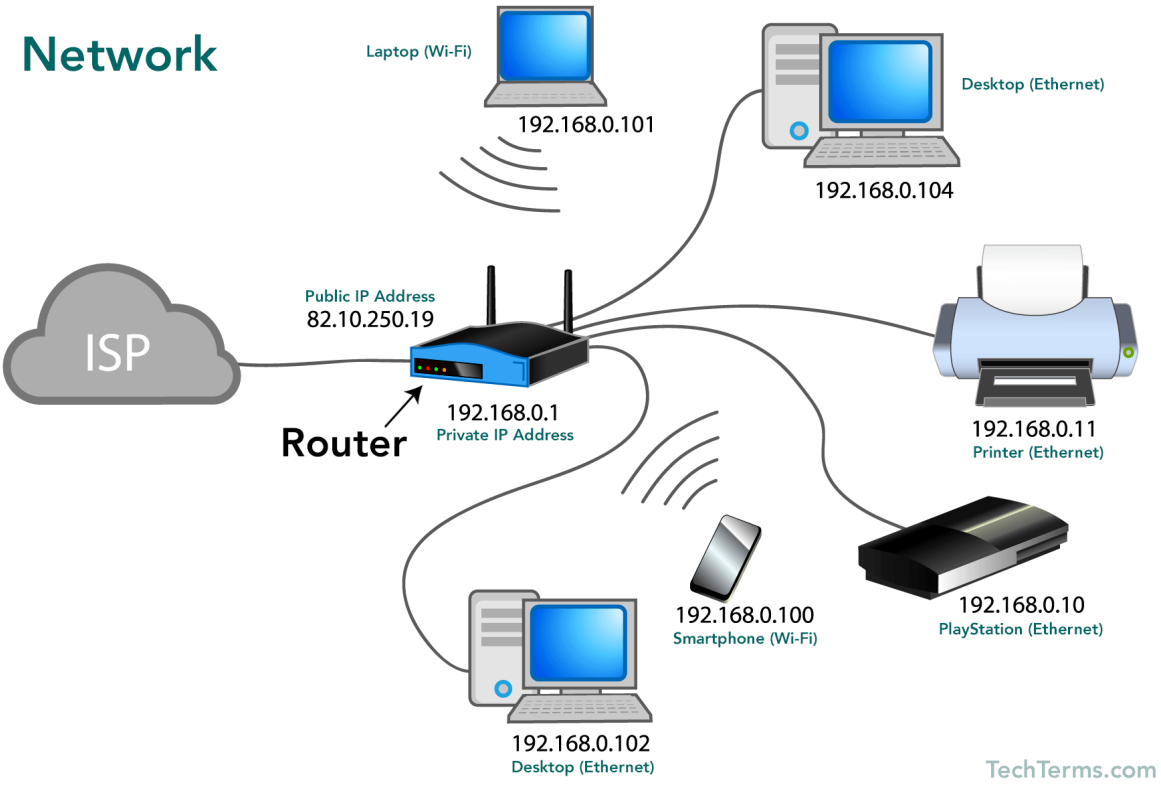
Symmetric Cryptography: Caesar Cipher, ROT13, Vigenere Cipher, Morse Code, Bacon Cypher, Alphabetical Substitution, MD5, Sha-1, Sha-256,Whirpool,Shake,Has-160

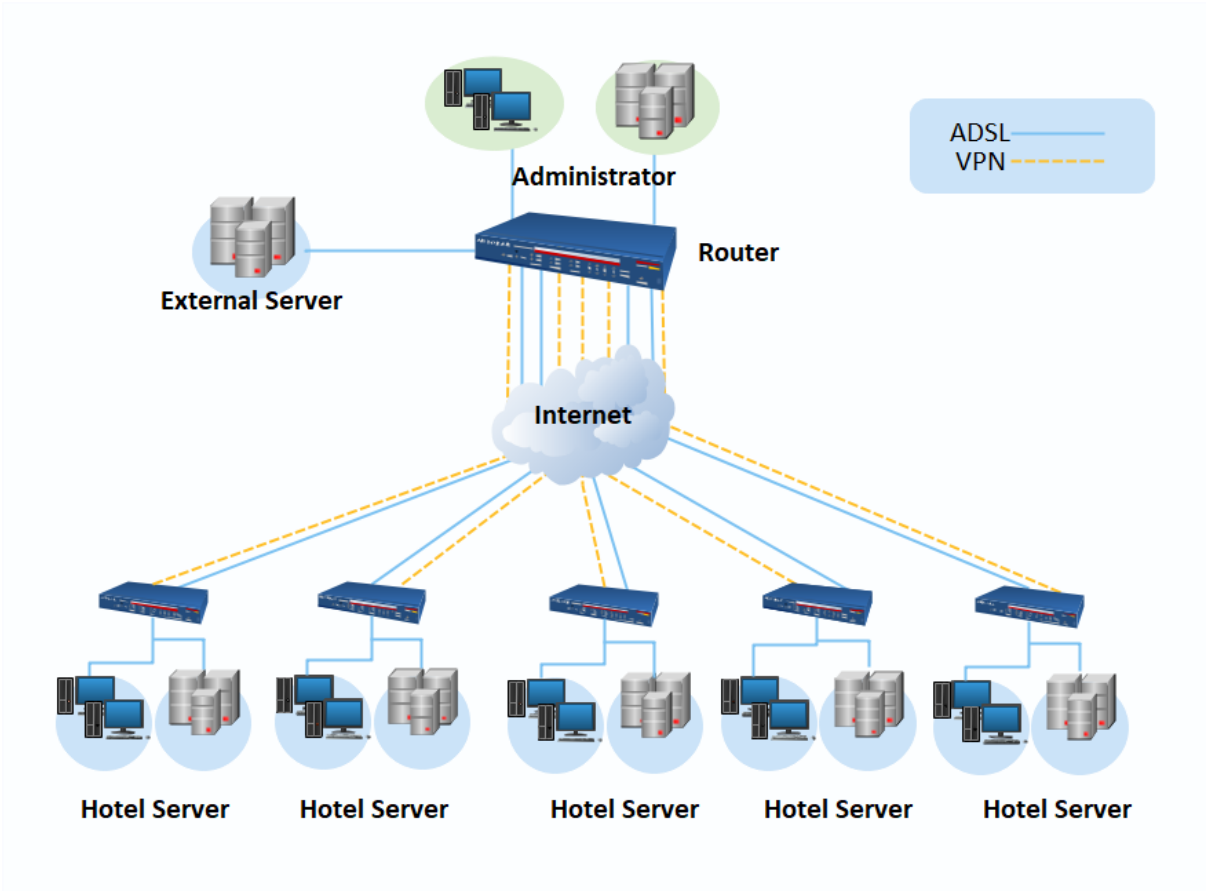
Tools: CypherChef, Cryprii, Hashcat, John The Ripper, Online Tools,,Hashid, Haiti

**There are 3 Type of CTF**: Jeopardy CTF, Attack and Defense, Mixed
**Example:** Google CTF, Defcon CTF, Plaid CTF, Inter-University Cyber Drill, National Cyber Drill

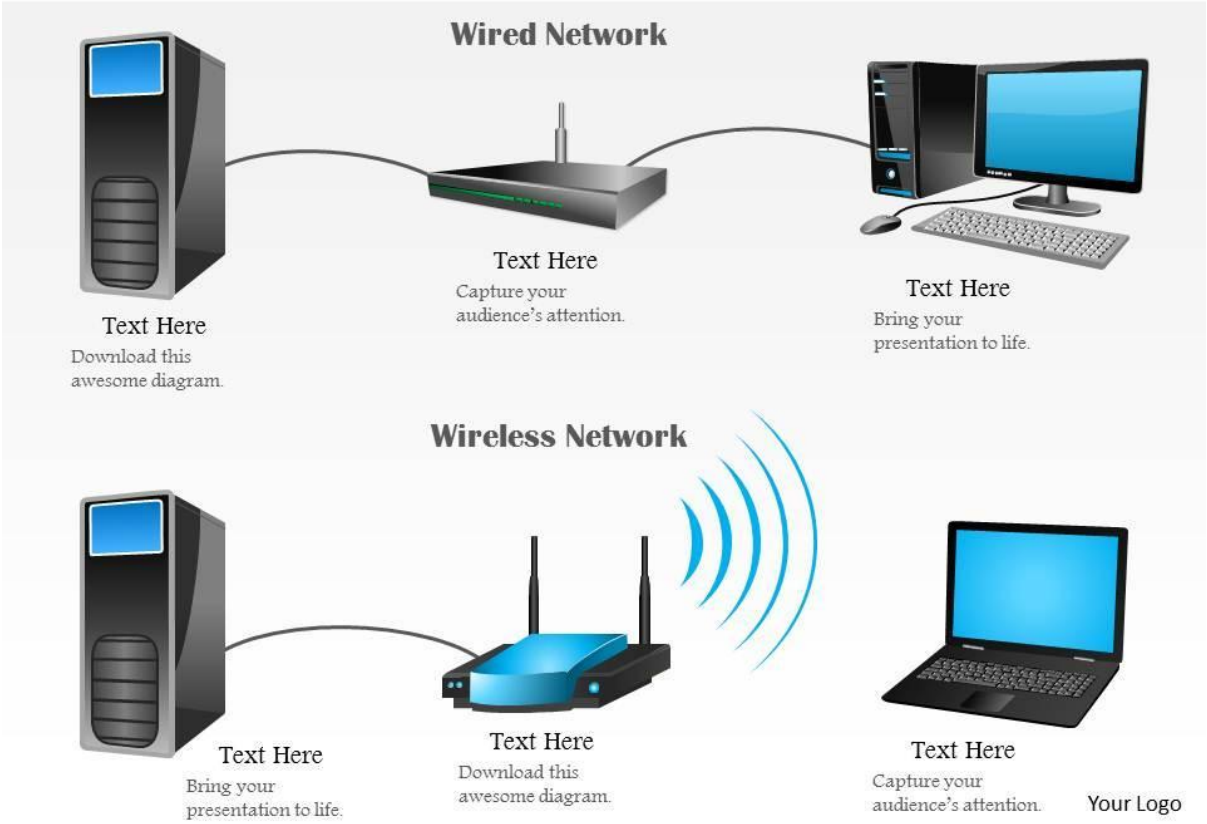
**Online All Tools:** Ctypii Cybershef Dcode Salty CipherIdentifier CipherIdentifier

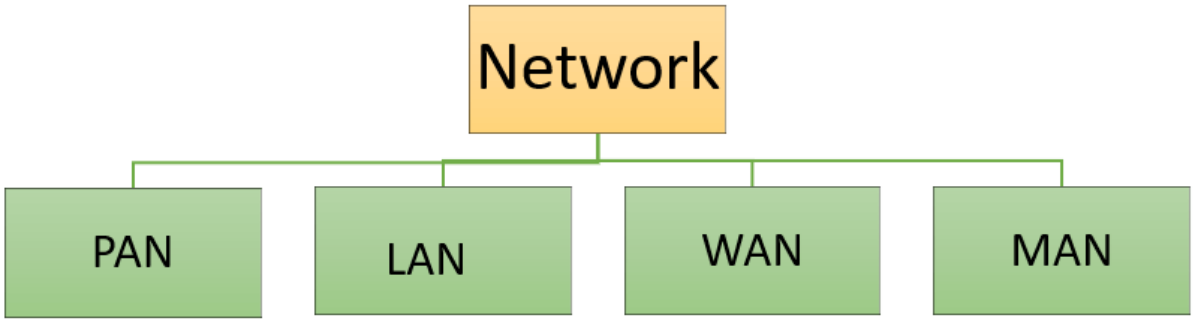
**Networking:**


Network
Laptop (Wi-Fi)
192.168.0.101
Desktop (Ethernet)
192.168.0.104
ISP
Public IP Address
82.10.250.19
Router
192.168.0.1
Private IP Address
192.168.0.11
Printer (Ethernet)
192.168.0.100
Smartphone (Wi-Fi)
192.168.0.10
PlayStation (Ethernet)
192.168.0.102
Desktop (Ethernet)
TechTerms.com

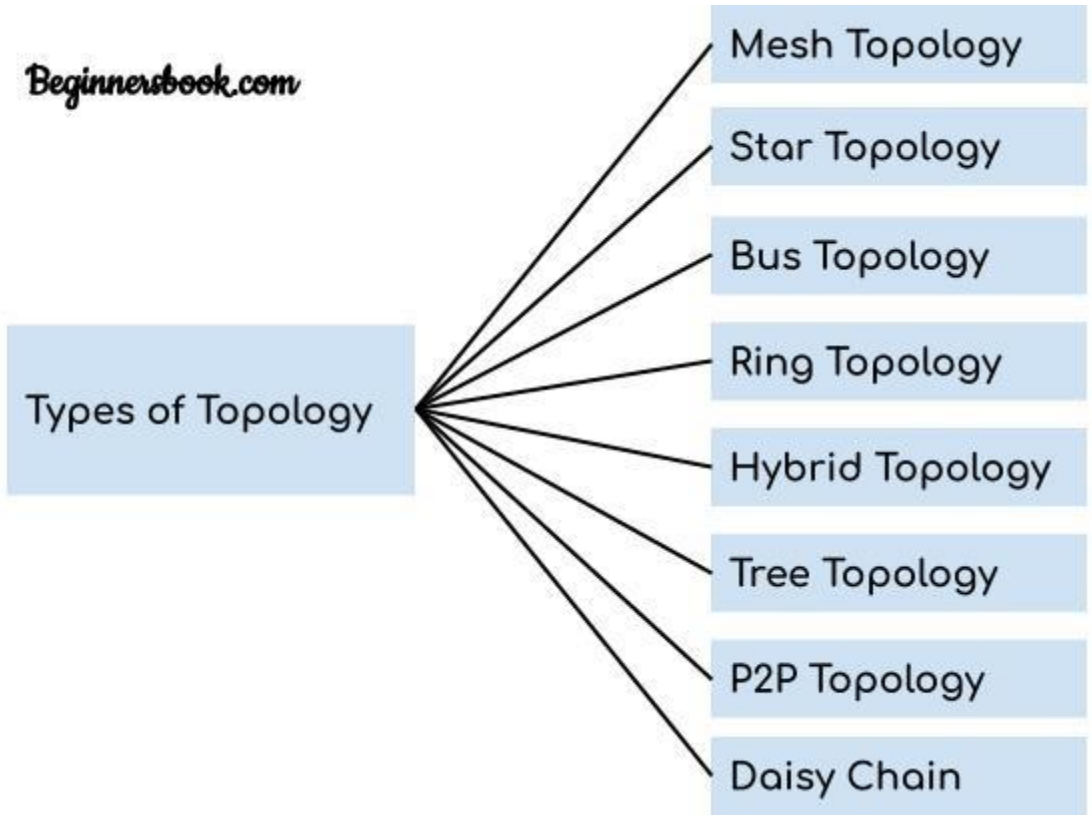

ADSL
VPN
Administrator
Router
External Server
Internet
Hotel Server
Hotel Server
Hotel Server
Hotel Server
Hotel Server

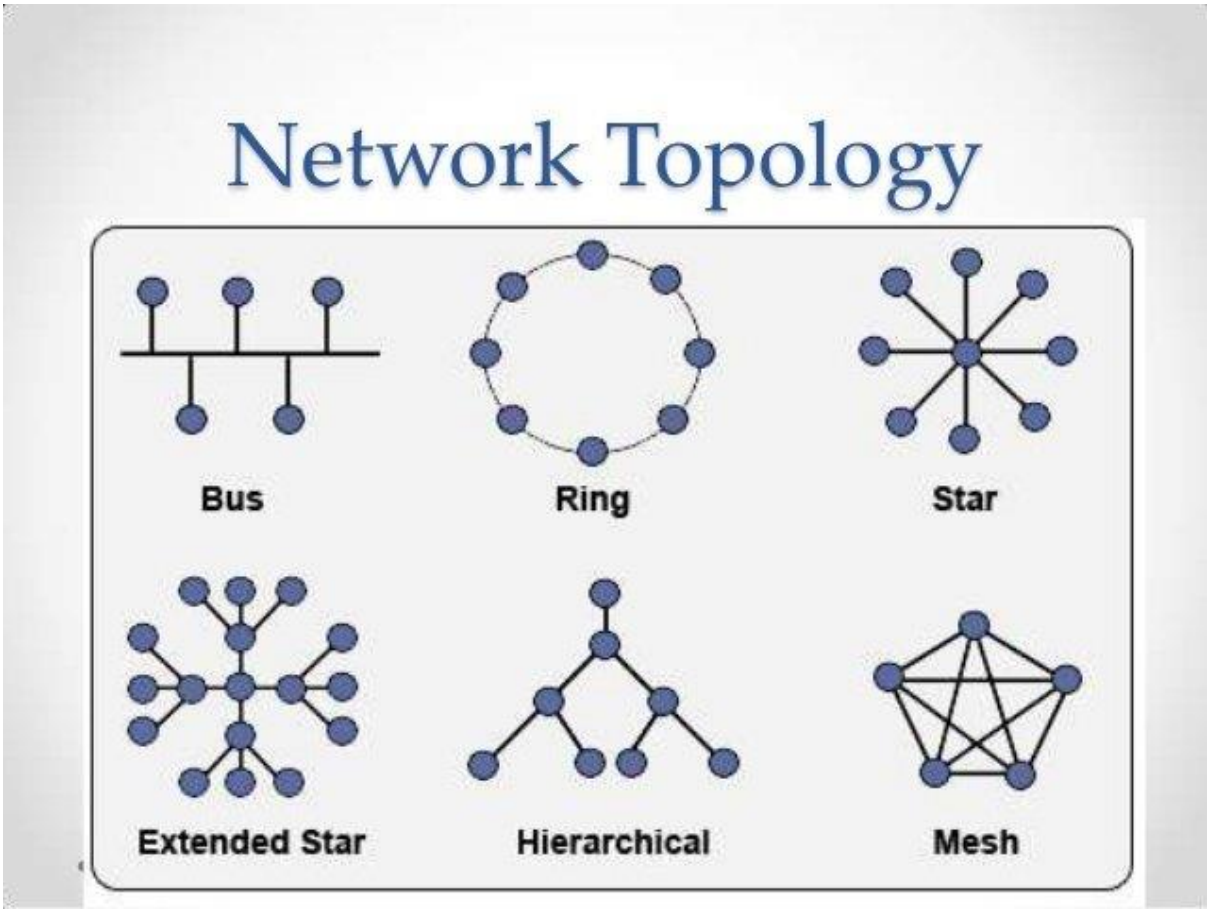
# Wired & Wireless Networking

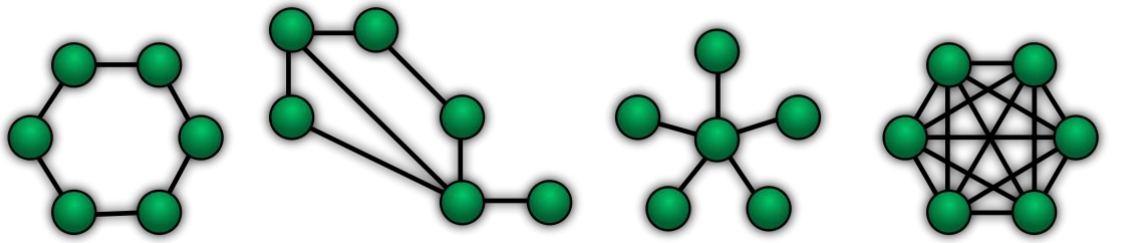


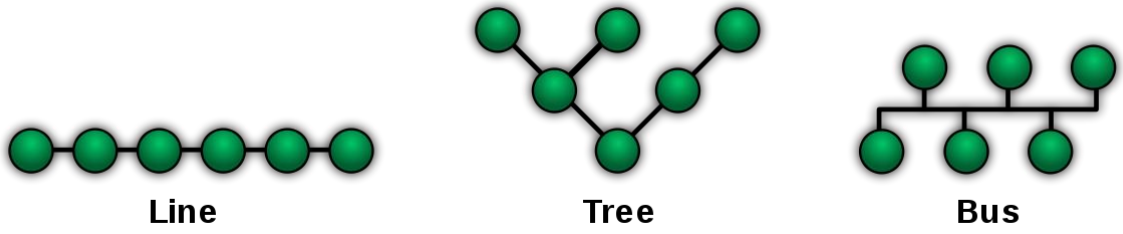


Network
PAN
LAN
WAN
MAN

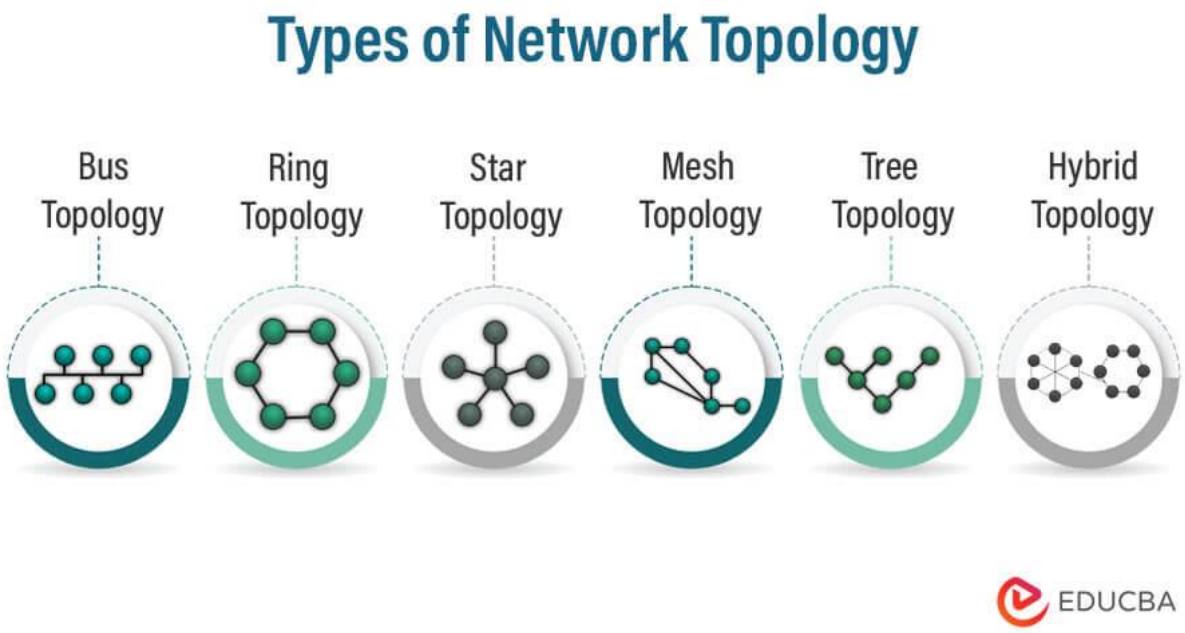



Beginnersbook.com
Types of Topology
Mesh Topology
Star Topology
Bus Topology
Ring Topology
Hybrid Topology
Tree Topology
P2P Topology
Daisy Chain


Network Topology
Bus
Ring
Star
Extended Star
Hierarchical
Mesh


Ring
Mesh
Star
Fully Connected


Line
Tree
Bus




**IP Address:** An Internet Protocol address is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification and location addressing.

**There is 2 Type of IP:** Public IP and Private IP

| Private IP | Public IP |
|---|---|
| Used with LAN or Network | Used on Public Network |
| Not recognized over Internet | Recognized over Internet |
| Assigned by LAN administrator | Assigned by Service provider / IANA |
| Unique only in LAN | Unique Globally |
| Free of charge | Cost associated with using Public IP |
| Range –<br>Class A -10.0.0.0 to 10.255.255.255<br>Class B – 172.16.0.0 to 172.31.255.255<br>Class C – 192.168.0.0 – 192.168.255.255 | Range –<br>Class A -1.0.0.0 to 9.255.255.255<br>11.0.0.0 – 126.255.255.255<br>Class B -128.0.0.0 to 172.15.255.255<br>172.32.0.0 to 191.255.255.255<br>Class C -192.0.0.0 – 192.167.255.255<br>192.169.0.0 to 223.255.255.255 |

**There is 2 Version of IP:** IPv4, IPv6

| IPv4 | IPv6 |
| --- | --- |
| Deployed 1981 | Deployed 1998 |
| 32-bit IP address | 128-bit IP address |
| 4.3 billion addresses<br>Addresses must be reused and masked | $7.9 \times 10^{28}$ addresses<br>Every device can have a unique address |
| Numeric dot-decimal notation<br>192.168.5.18 | Alphanumeric hexadecimal notation<br>50b2:6400:0000:0000:6c3a:b17d:0000:10a9<br>(Simplified - 50b2:6400::6c3a:b17d:0:10a9) |
| DHCP or manual configuration | Supports autoconfiguration |

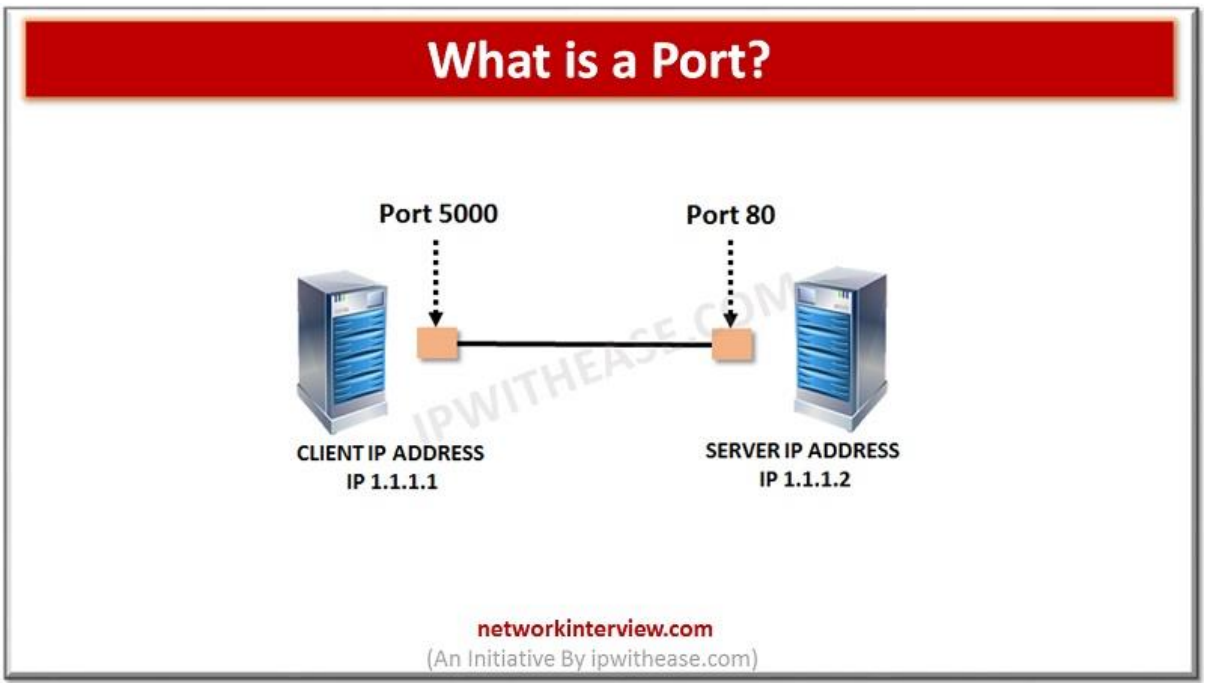
## IPv4 Address Types

| Type | Purpose | Example |
| --- | --- | --- |
| Unicast | send to a single host | 192.168.1.100 |
| Multicast | send to a group of hosts | 224.0.0.1 |
| Broadcast | sending to every host | 192.168.1.255 |
| Loopback | send to self | 127.0.0.1 |
| Link-local | local link(subnet) only - not routable | 169.254.0.0 |
| Unspecified | unknown network - quad-zero | 0.0.0.0 |
| All-hosts broadcast | broadcast to all hosts on local link | 255.255.255.255 |
| Directed broadcast | broadcast to a specific network (remote) | 192.168.2.255 |

| IPv6 address | Meaning |
|---|---|
| 0:0:0:0:0:0:0:0 OR :: | This address is equivalent to 0.0.0. IPv4 address. |
| 0:0:0:0:0:0:0:1 Equals ::1 | This is equivalent to the 127.0.01 |
| 0:0:0:0:0:0:192.168.1.1 | IPv4 and IPv6 addresses in mix mode. |
| 2000::/3 | The global unicast address range. |
| FC00::/7 | The unique local unicast range. |
| FE80::/10 | The link-local unicast range. |
| FF00::/8 | The multicast range. |
| 3FFF:FFFF::/32 | Reserved for examples and documentation. |
| 2002::/16 | This range allowed IPv6 packets to transmitted on an IPv4 network. |
| 2001:0DB8::/32 | Also reserved for examples and documentation. |



**Port:** In computer networking, a port or port number is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service. 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.



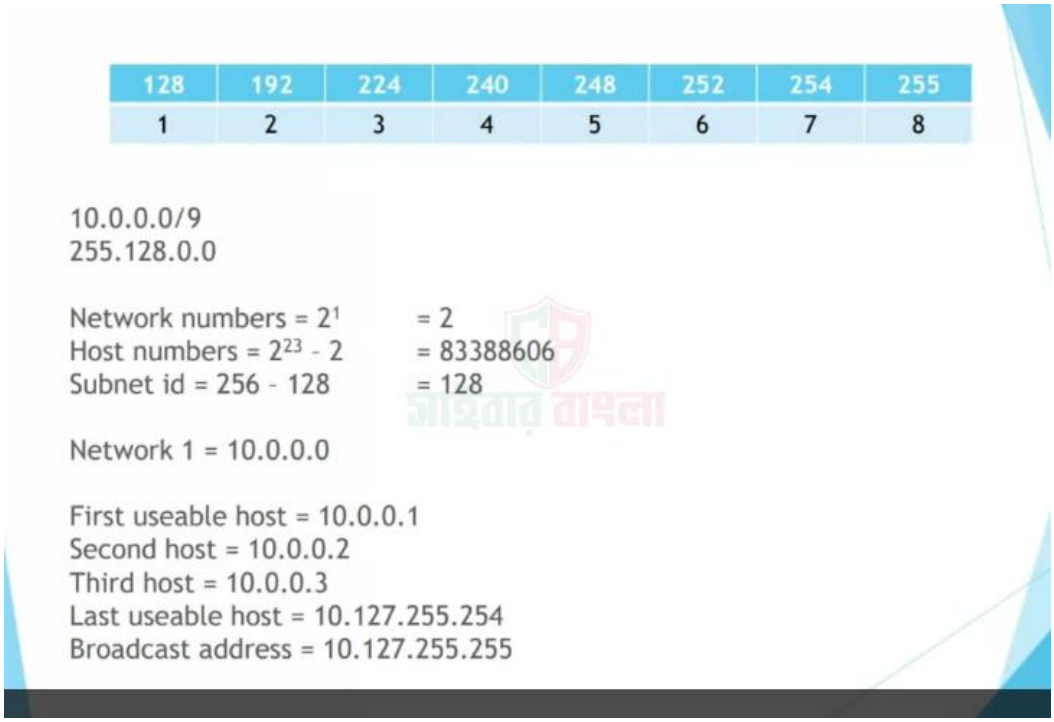
**Network protocols** are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely. Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.

FTP(20/21)
SMTP(25)
HTTP(80)
HTTPS(443)
DNS(53)
SSH(22)

**Class**:

| CLASS | LEADING BITS | NET ID BITS | HOST ID BITS | NO. OF NETWORKS | ADDRESSES PER NETWORK | START ADDRESS | END ADDRESS |
|---|---|---|---|---|---|---|---|
| CLASS A | 0 | 8 | 24 | $2^7$ ( 128 ) | $2^{24}$ (16,777,216) | 0.0.0.0 | 127.255.255.255 |
| CLASS B | 10 | 16 | 16 | $2^{14}$ ( 16,384 ) | $2^{16}$ ( 65,536 ) | 128.0.0.0 | 191.255.255.255 |
| CLASS C | 110 | 24 | 8 | $2^{21}$ ( 2,097,152 ) | $2^8$ ( 256 ) | 192.0.0.0 | 223.255.255.255 |
| CLASS D | 1110 | NOT DEFINED | NOT DEFINED | NOT DEFINED | NOT DEFINED | 224.0.0.0 | 239.255.255.255 |
| CLASS E | 1111 | NOT DEFINED | NOT DEFINED | NOT DEFINED | NOT DEFINED | 240.0.0.0 | 255.255.255.255 |

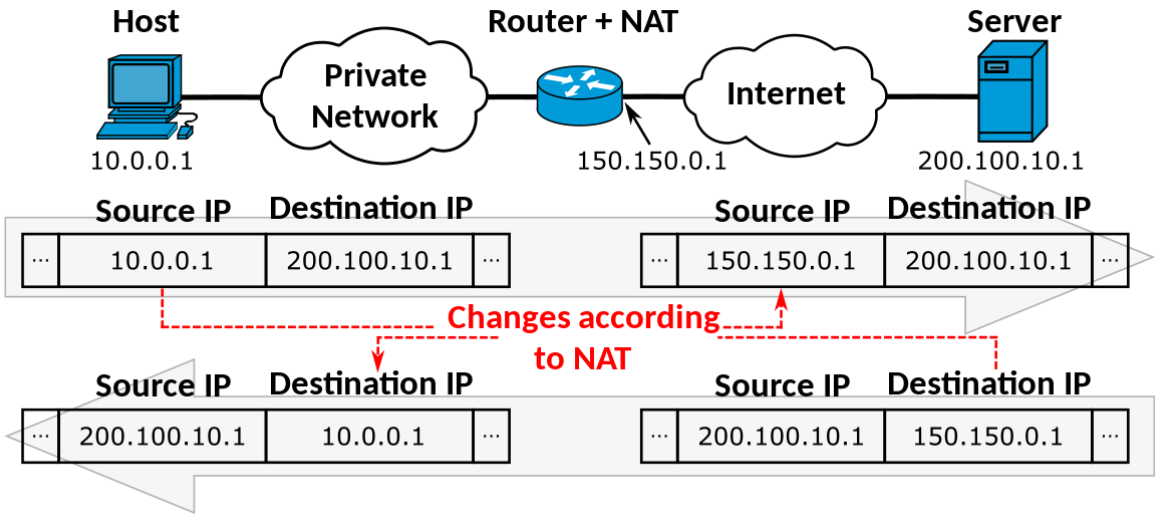
**Subnet Mask:**

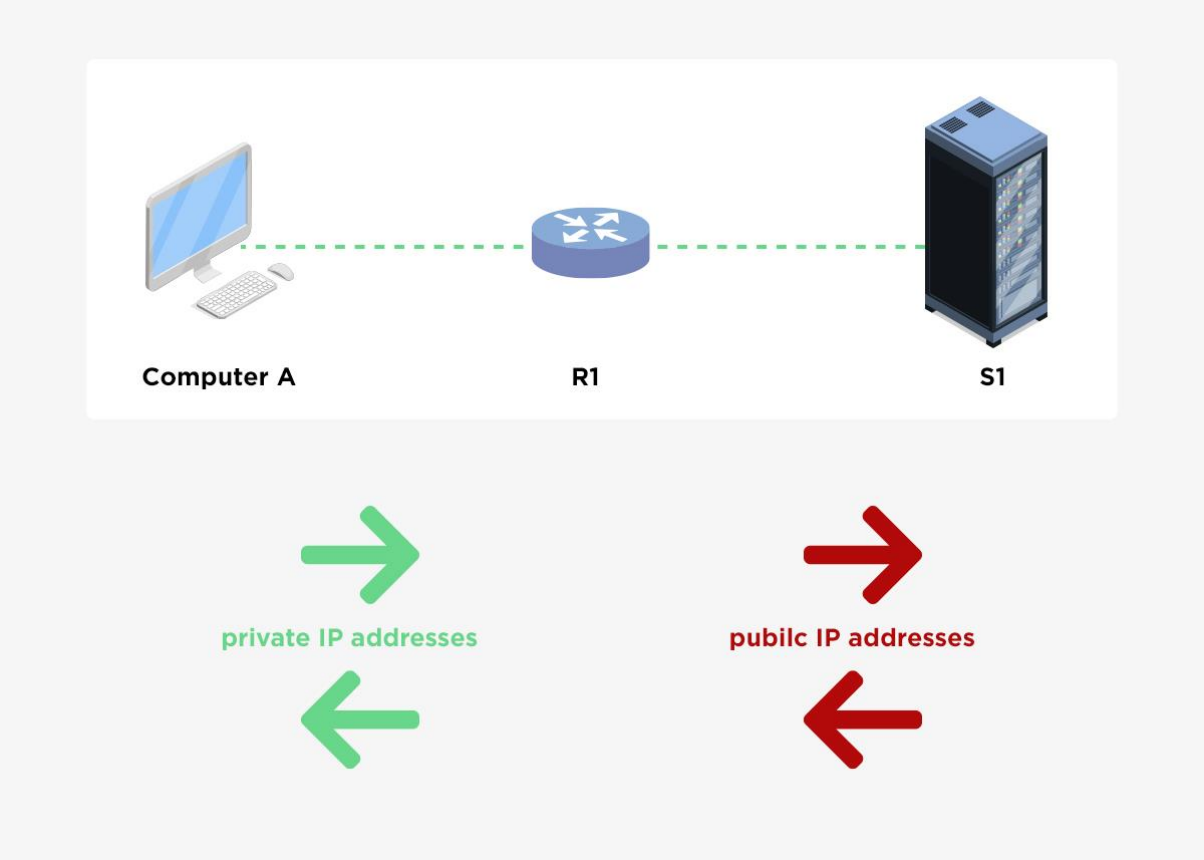


# Subnet Mask

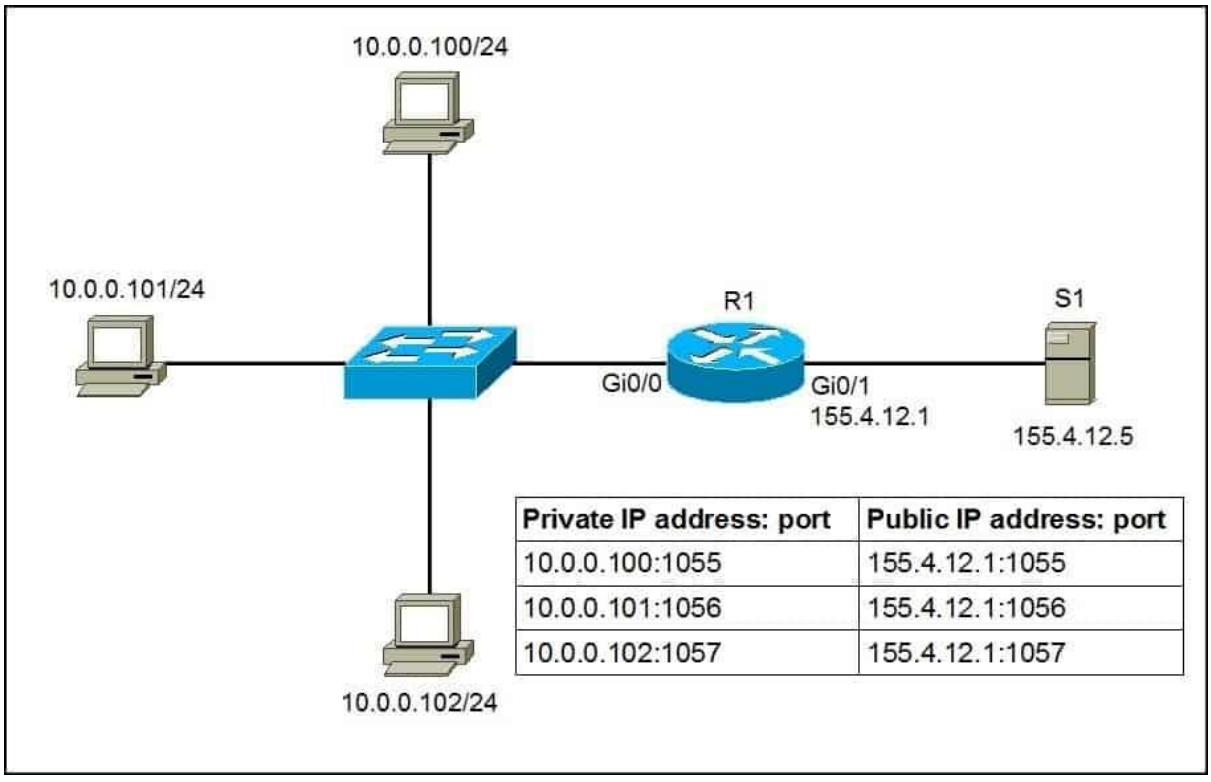
| Suffix | Hosts | 32-Borrowed=CIDR | 2^Borrowed = Hosts | Binary=> dec = Suffix |
|---|---|---|---|---|
| .255 | 1 | /32 | 0 | 11111111 |
| .254 | 2 | /31 | 1 | 11111110 |
| .252 | 4 | /30 | 2 | 11111100 |
| .248 | 8 | /29 | 3 | 11111000 |
| .240 | 16 | /28 | 4 | 11110000 |
| .224 | 32 | /27 | 5 | 11100000 |
| .192 | 64 | /26 | 6 | 11000000 |
| .128 | 128 | /25 | 7 | 10000000 |

**Network Address Translation (NAT)**



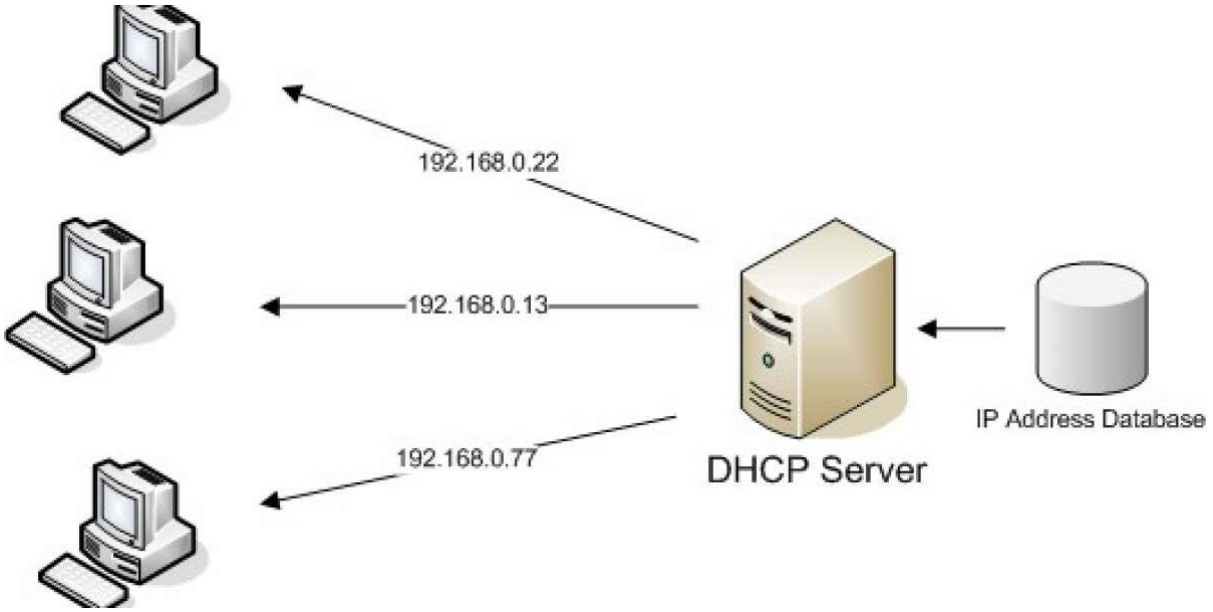


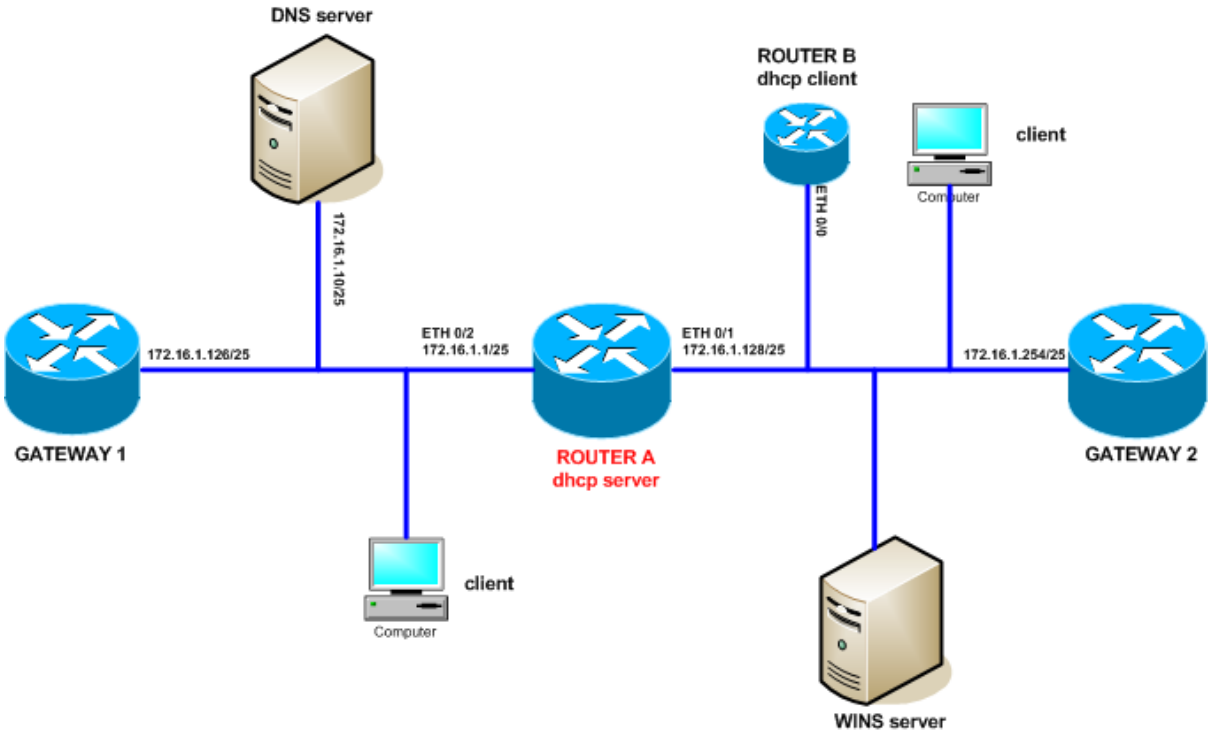

**Process analytical technology (PAT):**

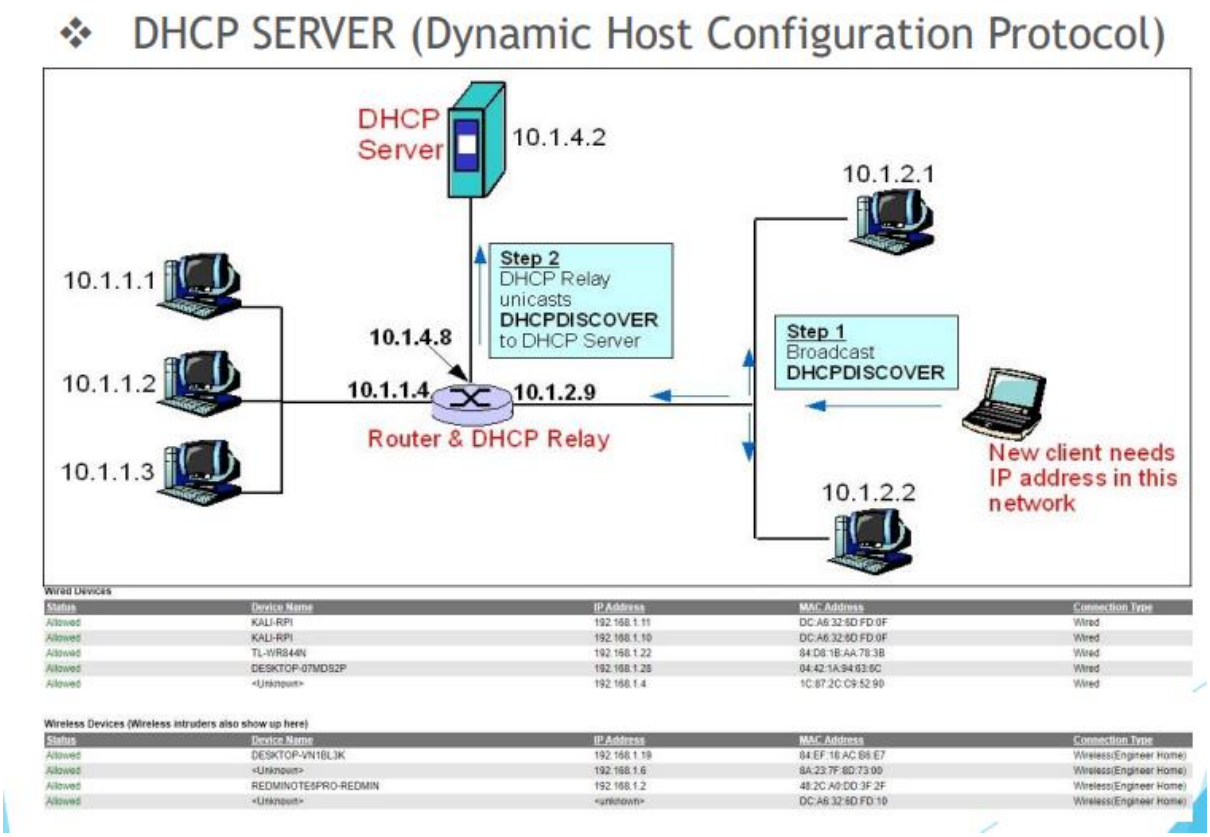



| Private IP address: port | Public IP address: port |
|---|---|
| 10.0.0.100:1055 | 155.4.12.1:1055 |
| 10.0.0.101:1056 | 155.4.12.1:1056 |
| 10.0.0.102:1057 | 155.4.12.1:1057 |

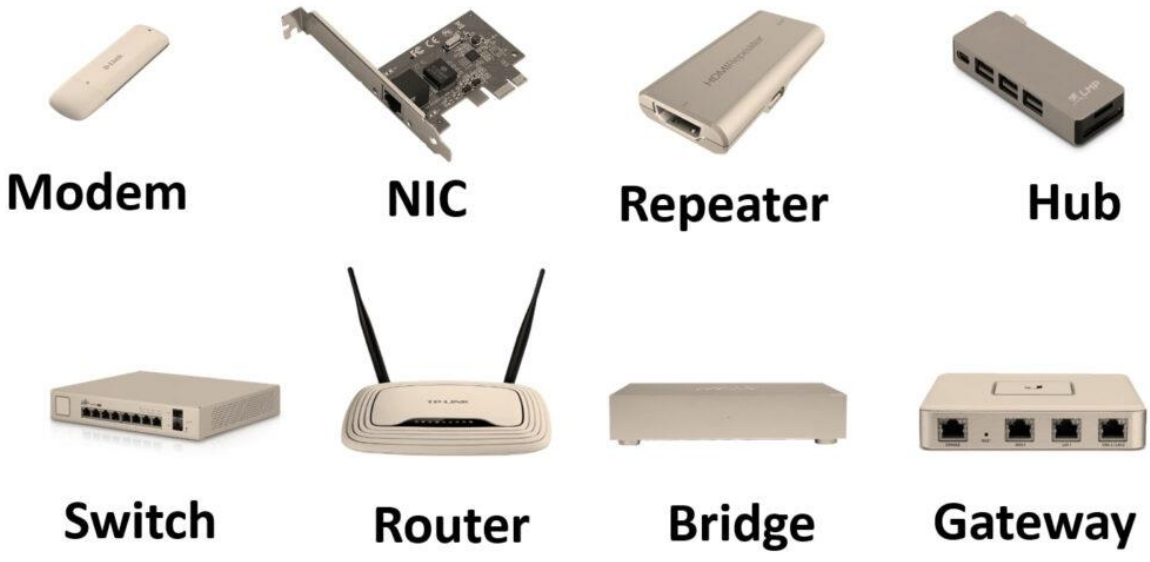
**A DHCP Server** is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.





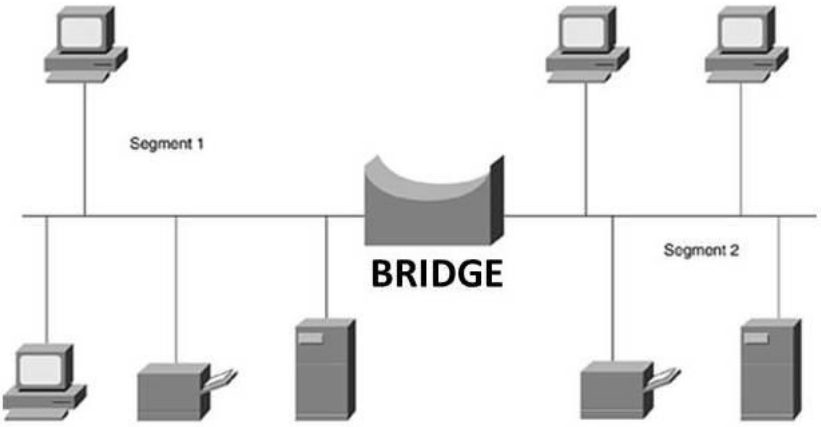

**Some Network Device:**



NIC CARD

HUB

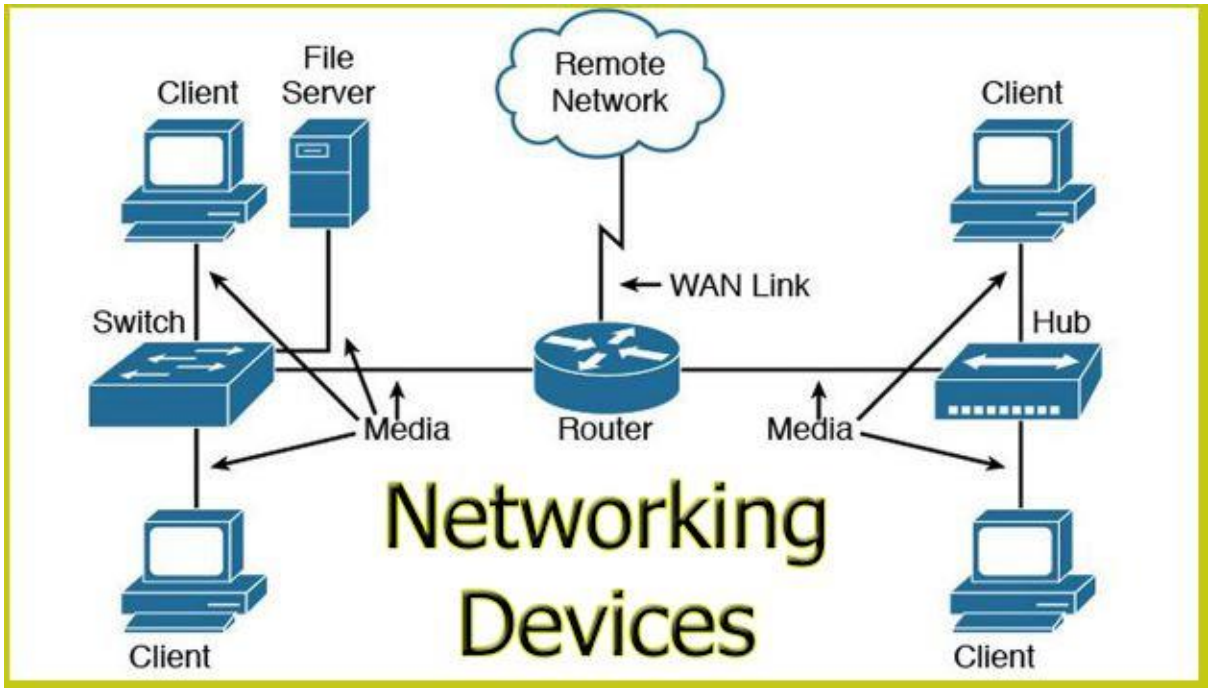
REPEATER

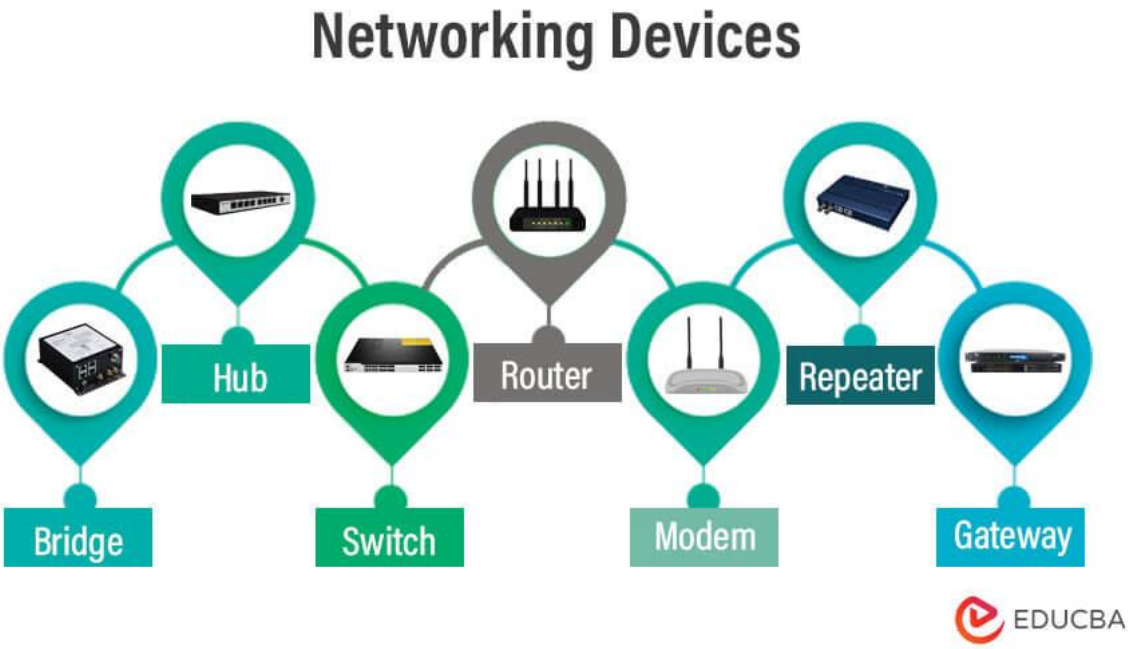



BRIDGE

ROUTER

ETHERNET SWITCH





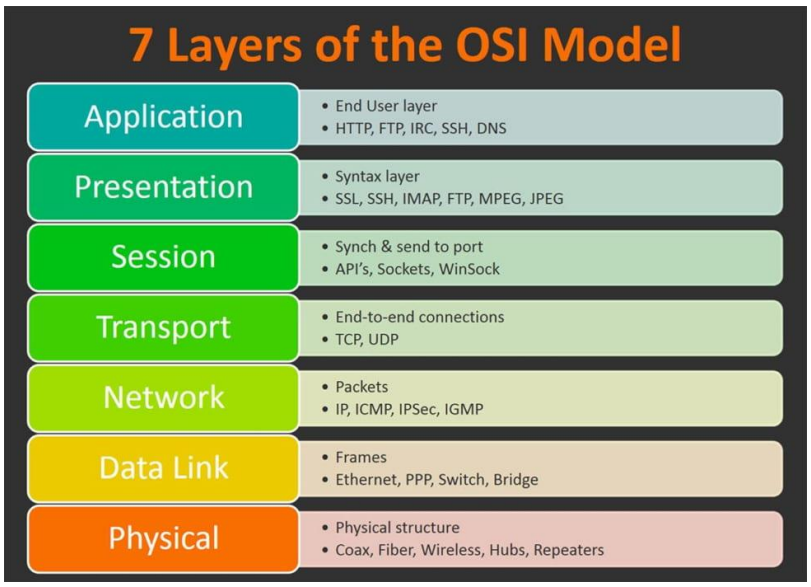

**Repeater** – A repeater can extend the signal.
**Hub** - A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it.
**Bridge** – A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN

**Switch** – Switches are networking devices operating at layer 2 or a data link layer of the OSI mode. Two types of switch.

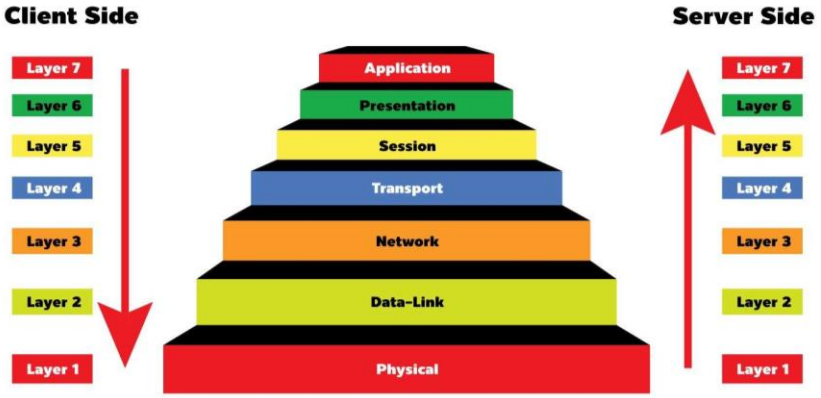
- Layer 2
- Layer 3

**Router**– Routers are networking devices operating at layer 3 or a network layer of the OSI model.

**OSI Model:**



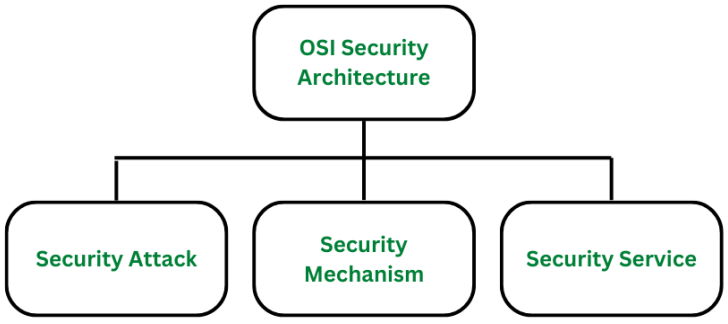
# OSI MODEL

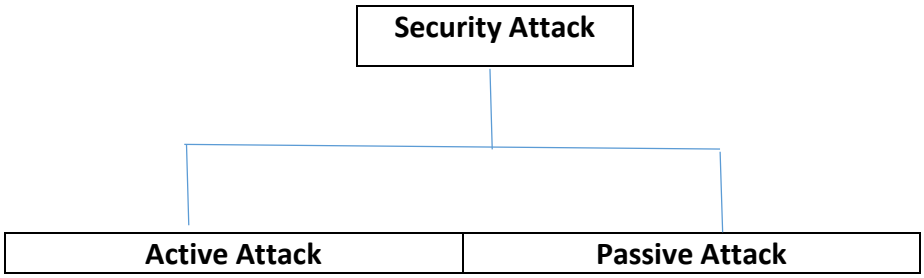



**What is the threat?**
A potential for violation of security, which exists when there is a circumstance, capability,action or event that could breach security and cause harm.That is a threat is a possible danger that might exploit a vulnerability

**What is Attack:** An assault on system security that derives from an intelligence threat, that is an intelligence act that is a deliberate attempt to evade security services and violate the security policy of a system

**OSI Security Architecture**






| | |
|---|---|
| **There are 2 Types**<br>**Masquerade**(using another credential to login,steal the password)<br>**Reply:** attacker divided the big message and sent again andagain( ex: hi how are you : **reply attack > hi > how> are>you**<br>**Modification of message:** attacker sends the message with modification.<br>**Denial of Service ( DoS)** | Release of message contents<br><br>**Traffic analysis**: Observe the pattern of messages Because he(attacker) don't know which message they are sending because of encryption.But still not attacker knock the location, content type , content length of the targeted person |

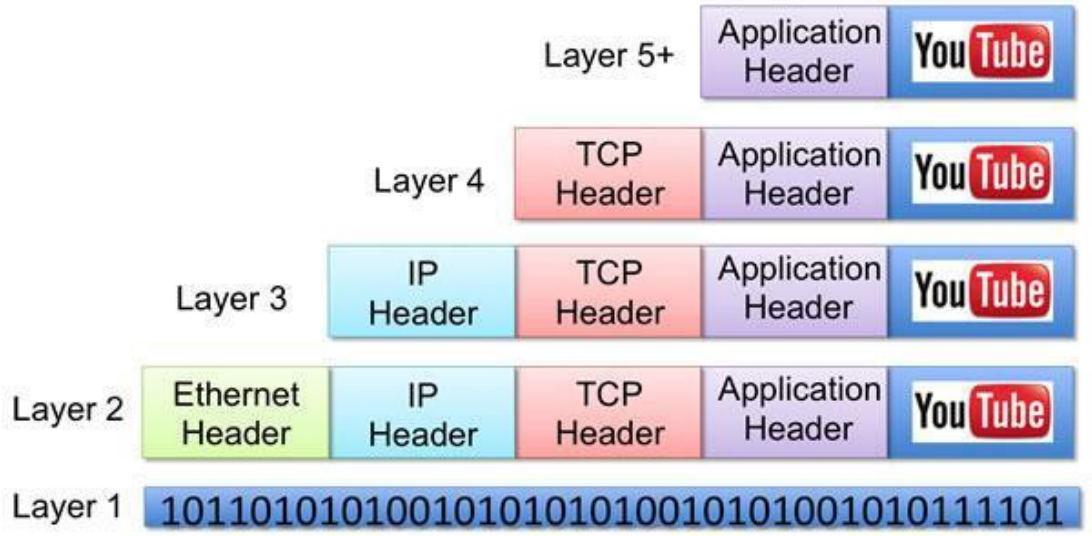
## Security Mechanism:

Detect ,prevent or recover from a security attack.
=> **Encipherment** ( convert plaintext to ciphertext)
=> **Digital Signature**( To prove the identity of the source also provide data integrity )
=> **Access control** ( Control access level,that means user level control kora ,kon user koto tuku access neta parbe )
=> Data Integrity
=>Authentication Exchange ( then send small piece of information exchange between to router just for authentication)
=> Traffic Padding ( Send the dummy data between sender and receiver to confuse the attacker, it not impact on sender and receiver )
=>Routing control
=> Notarization( SSL certicicate )

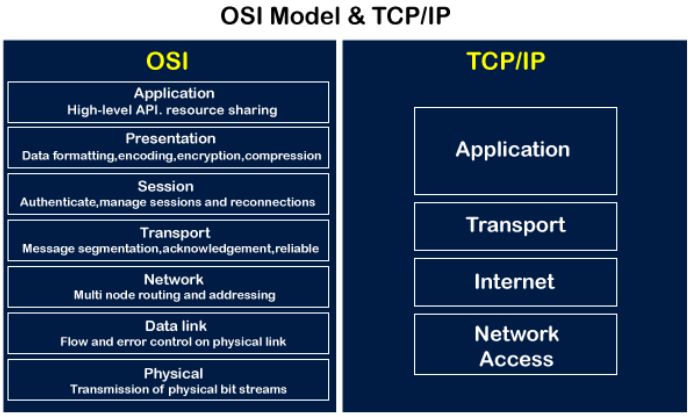
## Security Service:

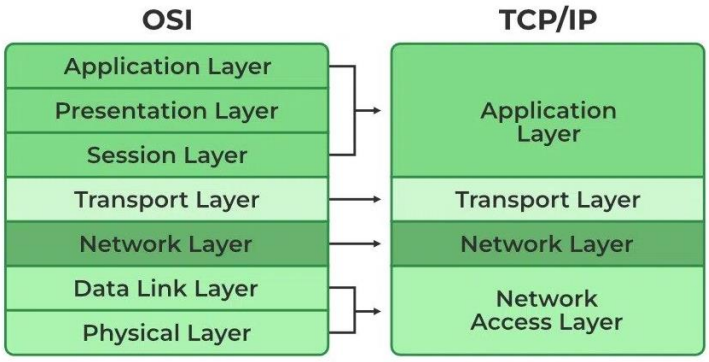
Enhances the security ,counter security attacks , and provides the service.
**=> Authentication**( confirm the source and destination)
**=> Access control** ( labels of access,user access)
**=> Data confidentiality**( protect unauthorized access to see the message)
**=> Data integrity**( Send message = Receive message )
**=> Nonrepudiation** ( Message send and receive howar por security system k ensure korte hobe j sa message ta send and receive korasa )

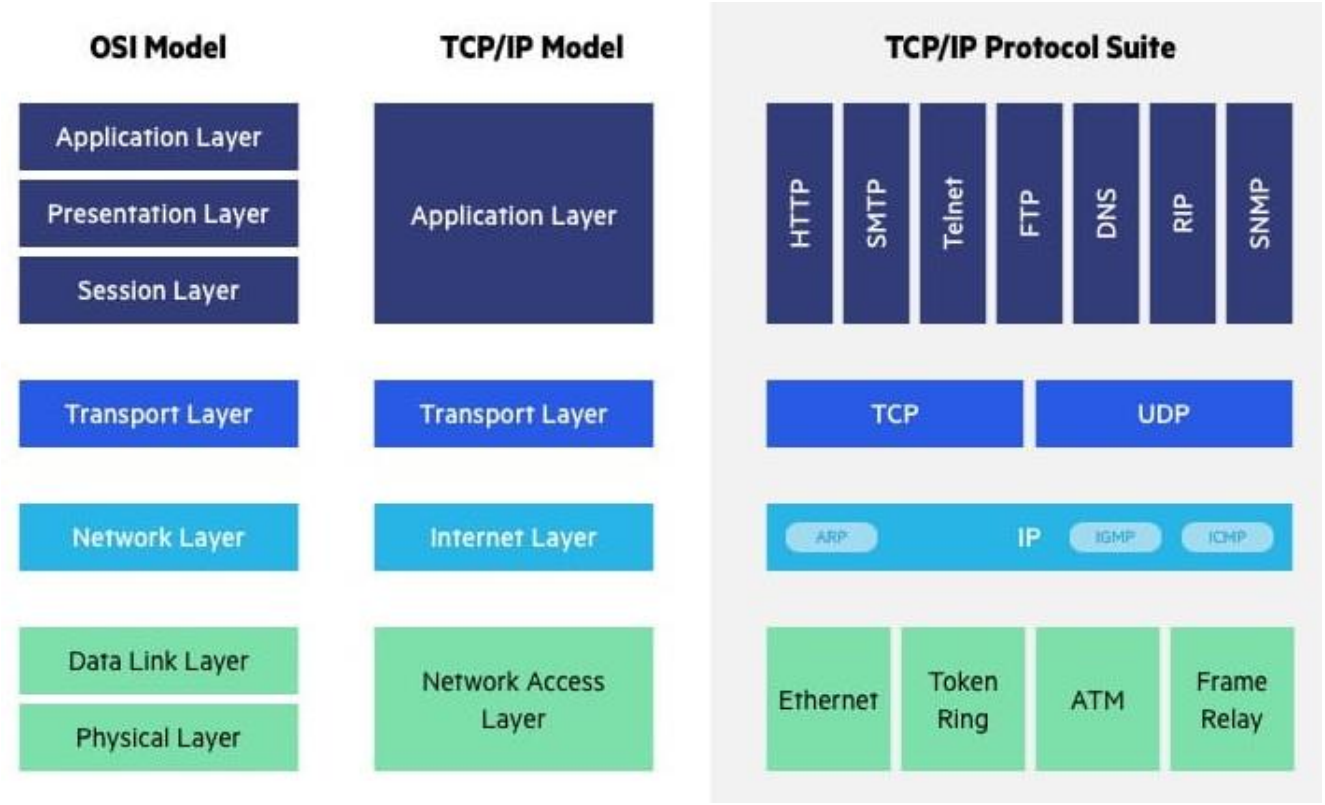
| Layer | Device / Protocols | Function | Cyberattack / Threat Examples |
|---|---|---|---|
| 7. Application | FTP, HTTP, IMAP, SMTP | User interface | Ransomware, Viruses, Worms, Malware, Botnets, Keyloggers, Rootkits, ARP Spoofing, Man-in-the-Middle attack, Spyware, Cache Poisoning, DNS-redirecting |
| 6. Presentation | JPG, MPEG, PNG | Data format; encryption | |
| 5. Session | SQL, RPC, NFS | Process to process communication | |
| 4. Transport | TCP, UDP | End-to-end communication maintenance | RIP Attacks, SYN Flooding |
| 3. Network | L3 Switches, Routers | Routing data, logical addressing, WAN delivery | IP Smurfing, Address spoofing, Misconfigured devices, Vulnerable old firmwares, Default passwords |
| 2. Data Link | L2 Switches, Bridges | Physical addressing, LAN delivery | |
| 1. Physical | Physical cabling | Transmitting bits | Environmental and physical threats: Dust, Water, Rodents |

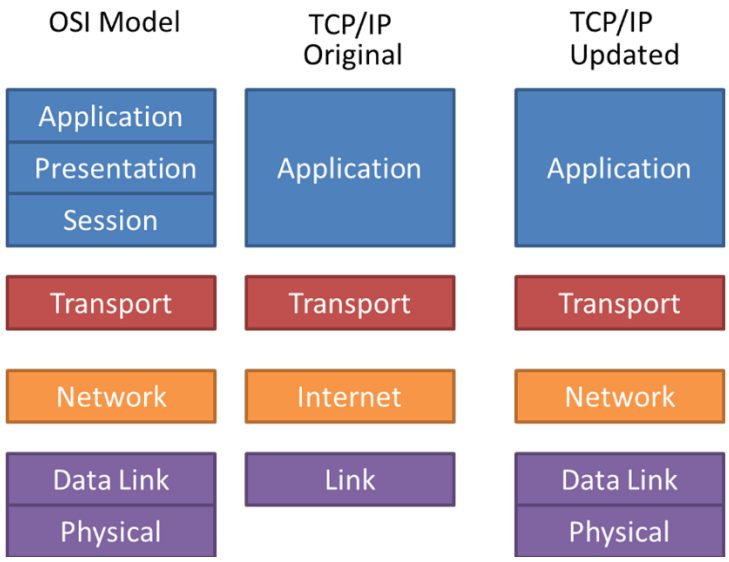


# OSI and TCP/IP






## Steganography

Tools: Xiao, Cryture, Steghide, Zsteg, Openstego, Foremost, Binwalk, Setgsolve
File: Image File Check

File to HEX : File To HEX List of File SIgnature

**EXIFTOOL**
file name.extention
exiftool name.extention
exiftool -comment="this is a test" test.jpg
exiftool -flag="flag.flag" test.jpg
exiftool -H name.ext
exiftool -v name.ext

strings a.jpg

sudo apt-get install steghide [jpeg, bmp, wav and au]
steghide embed -cf <imagename> -ef <filename>  abc
steghide extract -sf <imagename>

zsteg name.png

stegsolver:
wget http://www.caesum.com/handbook/Stegsolve.jar -O stegsolve.jar
chmod +x stegsolve.jar
mkdir bin
mv stegsolve.jar bin/

Run:
  java -jar stegsolve.jar

https://stegonline.georgeom.net/upload

Stegseek:

go to link and download https://github.com/RickdeJager/stegseek
Install the .deb file using sudo apt install ./stegseek_0.4-1.deb
stegseek [image name] rockyou.txt

locate rockyou.txt

Binwalk:
Install https://github.com/ReFirmLabs/binwalk
Run : binwalk [image name]
Extract : binwalk -e <image name>
binwalk --dd=".*" name.png -e

ForeMost:
Install : sudo apt-get install -y foremost
Run : foremost [fileName]

gmic <pic1> <pic2> -blend xor

● Download deep sound
Link ~ https://deepsound.en.uptodown.com/windows

● Download Coagula
Link ~ https://ccm.net/download/download-14504-coagula

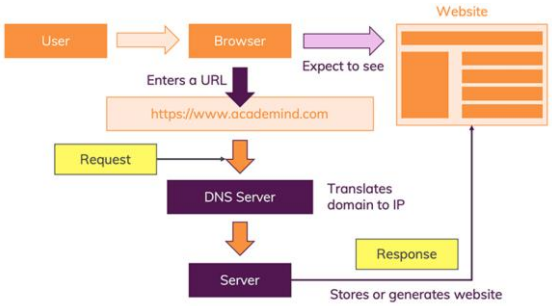
● Download Sonic
Link ~ https://www.sonicvisualiser.org/download.html

● PCRT Tool
Link ~ https://github.com/sherlly/PCRT
Run ~ python PCRT -v -i [imageName]

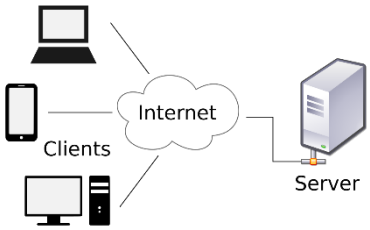
# Web Pentesting

## How Internet Works :

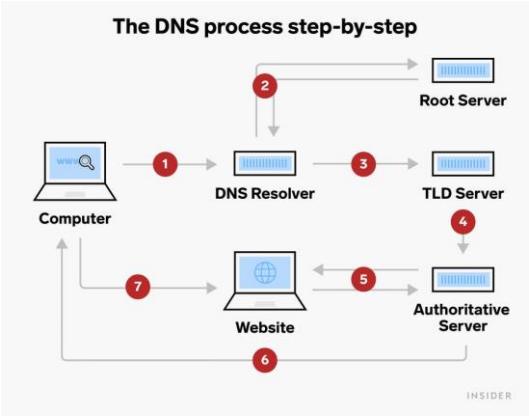
**Domain:** In the Internet, a domain name is a string that identifies a realm of administrative autonomy, authority or control. Domain names are often used to identify services provided through the Internet, such as websites, email services and more. As of 2017, 330.6 million domain names had been registered

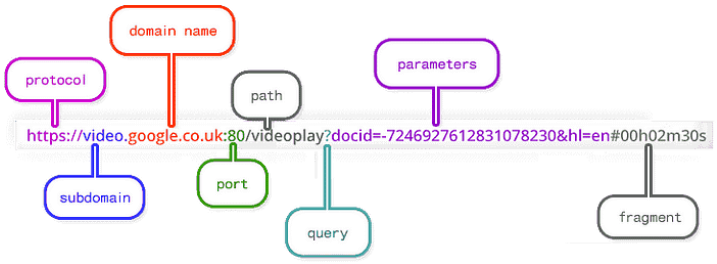


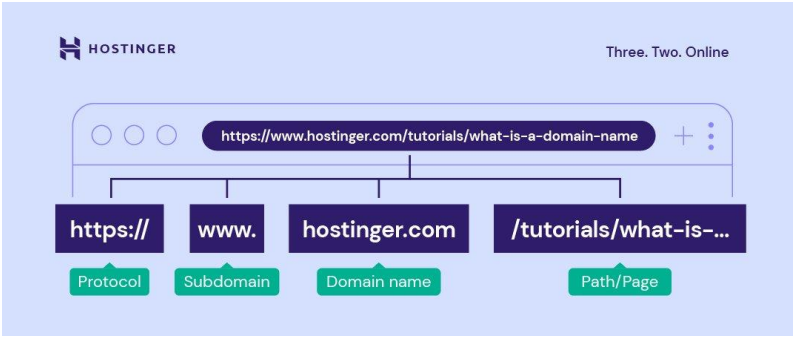

**Server:** In computing, a server is a piece of computer hardware or software that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model.

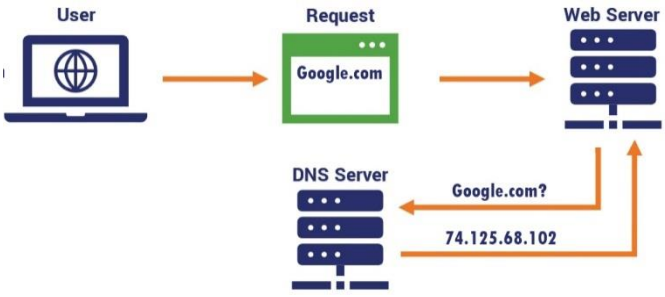



DNS: The Domain Name System is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol networks. It associates various information with domain names assigned to each of the associated entities

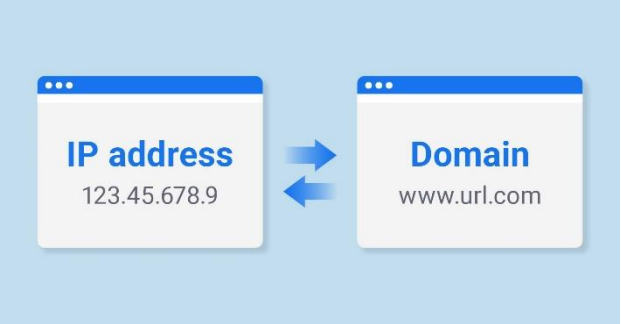


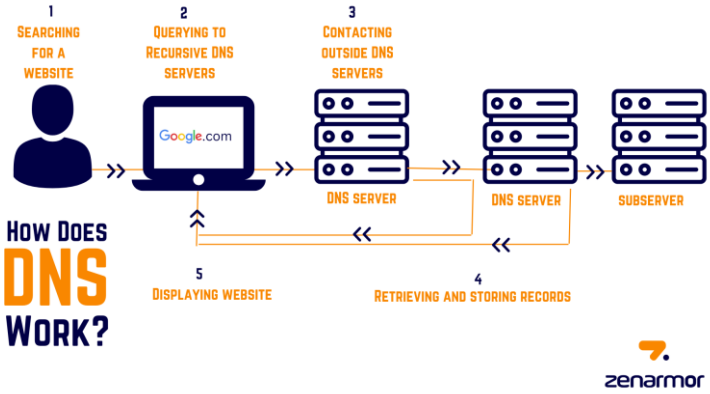



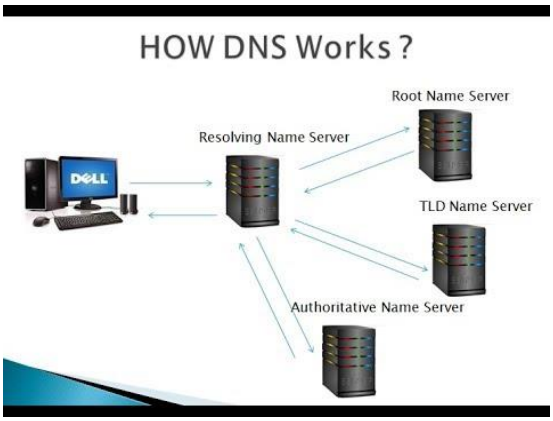



**Domain to IP::**




**How DNS Works:**




A **root name server** is a name server for the root zone of the Domain Name System of the Internet. It directly answers requests for records in the root zone and answers other requests by returning a list of the authoritative name servers for the appropriate top-level domain