# Lecture 1

**Role of system administrator is to maximise:**

- Reliability
    - Measure of percentage of time that the system is up and running
    - Goes hand in hand with service level agreement which is the user and administrator agreement on what is service
- Integrity
    - Degree to which data stored is trusted not to be lost or corrupted
    - Affected by hardware, backup, security
- Security
    - Degree to which data stored or in transit is trusted to not be altered, destroyed or disclosed to unauthorised party
    - Affected by procedures and policy (High security means low usability which affects workflow)
- Performance
    - Efficiency of system
    - Constraints are capital expenditures, procedures and policies, users
    - Need to train users on how to make use on resources
- Efficiency
    - System should be managed in a way which maximises the productivity of administrator
    - Centralising service may make it easier for the admins, but it may have detrimental effect on performance
- Ease of use
    - Degree which a system allows the user base to perform their task in the way the desire
    - Eg. Users wish to use easy to remember passwords.
    - System does not discriminate people with disability
- Order
    - Administrators need to understand the legal environment of the system and make sure users comply with all rules and regulations.
    - Company policies and ethics as well.

Administrators need to be able to code, strong knowledge of systems, and diagnose system problems.

They are expected to install hardware, maintain software and set/maintain configurations, capacity planning (hardware planning), performance tuning, monitor system, diagnose and fix problems, maintain local documents, write procedures and policy, enforce and educate user and management

**Devices**

CPU - Carries out instructions of program and performs basic arithmetic operation
- Eg. of architecture : Sparc, x86 and x86-64, PowerPC, MIPS, Alpha etc.
- PowerPC used in console, i5 and i7

Reduced Instruction Set Computing (RISC) vs Complex Instruction Set Computing (CISK)
RISC is better than CISK and is used in Servers. CISK is used in intel chips.

Parallelism done to make use of the CPU. Multiple programs can be run at once which is called time sharing. Uses context switching to make it smoothly. Uses pipeline to fetch jobs one after another to not waste resources
64 and 32 bit are representations of integer numbers. Using 64 bit means can refer to more memory addresses.

**Memory**
- SIMM, DIMM, SODIMM which holds memory for the CPU to access immediately.
- Volatile and nonvolatile memory (Volatile requires power to maintain data.)
    - Volatile (DRAM, SRAM)
    - Non volatile (ROM, PROM, EPROM, EEPROM)

**DDRS**
- RAM, Supports multiple memory access to occur simultaneously, compared to CPU not fast enough. Chip based memory makes retrieving data faster.

Don't need to know bus type
Northbridge - CPU, RAM, GPU etc
Southbridge - keyboard, mouse etc

**Disk**

Hard Disk Drive

- Disks are coated with electromagnetic material and paired with a head that is close to the surface but does not touch it. It is used to read and write data. The hand will move forward and backward as the disk spins to read from different tracks.

**Operating system**

**Consists User Command Interface of 4 essential managers**

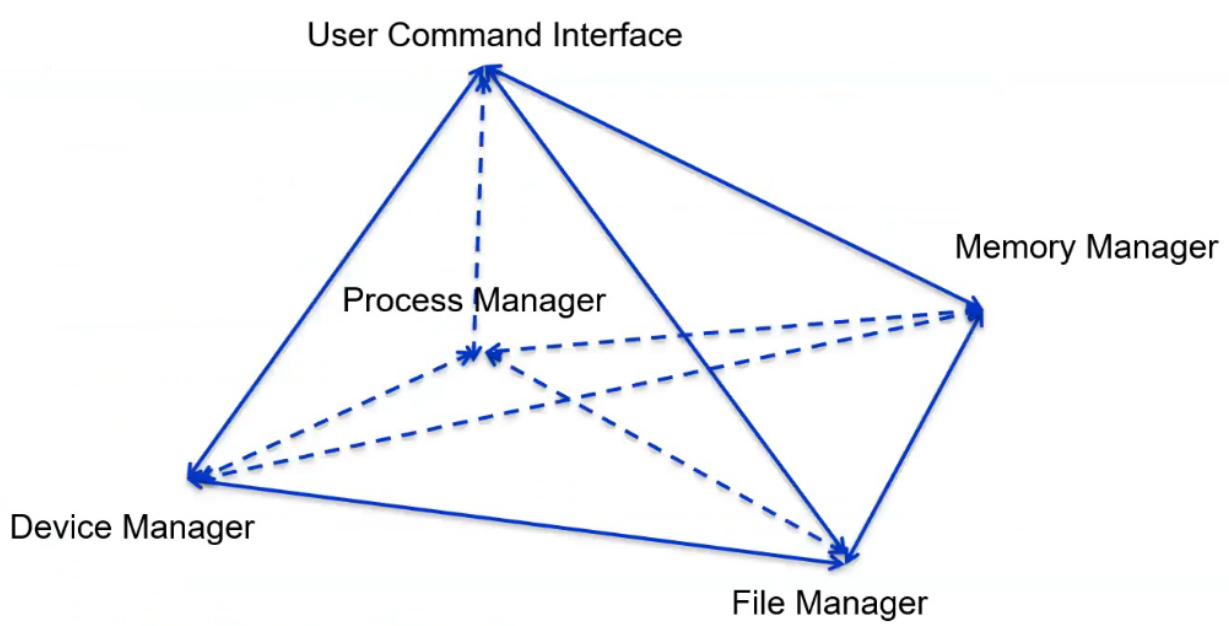
- Memory Manager
    - Check validity of request for memory space
    - Allocated a portion of unused memory space to legal request
    - Keeps track of who is using which section of memory in a multi -user environment
    - Deallocates memory when the time comes to reclaim the memory
    - It preserves the space in main memory occupied by the operating systems
- Processor Manager
    - Decides how to allocate the CPU
    - It keeps track of the status of each process
    - Once it allocate the processor, it sets up the necessary register and table
    - It reclaims the processor when the job is finished or when the time is up
        - Job scheduler accepts or rejects the incoming job
        - The Process Scheduler decides which process get the CPU and for how long
- Device Manager
    - It controls the user of devices
    - Monitors every device, channel, and control unit
    - Tracks the status of each device
    - It uses preset policies to determine which process will get a device and for how long
    - It allocates and deallocates the device
- File Manager
    - It keeps track of every file in the system
    - It uses predetermined access policies to enforce restrictions on who has access to which files
    - It controls what users are allowed to do with files

- It allocates they resource by opening the file and deallocates it by closing the file

**Network system have a fifth manager - Network Manager**

Let's say someone types a command to execute a program, what will happen?

Firstly, the device manager will receive the electrical impulse from the user. Then the command will be sent to the user command interface. It will then interact with the processor manager to validate if the command is valid. If valid, the process manager will send an acknowledgement to display through the device manager. Process manager will also need to determine if the data needs to be retrieved from the storage. If it is not in memory, then the file manager will locate and calculate the exact location of the file and then pass it to the device manager which will read and send it to the memory. The memory will then allocate memory and space for the program to be loaded into. The memory will also track the location and relevant data that is used by the program. For the program to execute, the process manager will manage CPU time to execute all the instructions contained in the program. If the data needs to be written back, it will interact with the memory manager to request additional space to store the results of that program execution. Once the program execution is complete, the processor manager will tell the memory manager that the program execution is done and the memory space can be released. The memory manager will release the memory space and at the same time, the data might need to be written on the disk storage so the memory manager will ask the device manager to allocate additional space to update the file.



# Lecture 2

**UNIX Operating System**

1. A portable operating system - can run even when the OS is stored in the USB stick
2. Multi tasking - support concurrent execution of multiple task and new process can interrupt existing process if it is higher priority
3. Multi user computer OS in a time sharing configuration - allow access by multiple user of a computer concurrently (Remote and local users can access the server at the same time)
4. Standard command line interface

Kernel is the core component and is loaded when the computer is first turned on . It loads all other components and serves to control activities centrally. User interacts with kernel using terminal

Shell Prompt

- # for root user
- $ for other user

Command:

- ls - a /user (ls is command name, -a is option and /user is the argument)
- Not all commands have options or take in arguments

Use command man to retrieve manual
Eg:
man date
man -k keyword

**Cut**

- cut -d ',' -f 1,3 filename.csv

In this example, -d ',' specifies that the delimiter is a comma, and -f 1,3 specifies that you want to extract the first and third fields.

**Sort**

- sort filename

**Shell (Create by user) and Environment (Set by system) Variables**
Use set or env to see list of environment variable and their values
Home - absolute pathname to home directory
PWD - directory u are working in
Path - contains a list of directories to search for an executable program (important cause used by malicious users that uses trojan horse. Attacker store it in path directory with same name as other program)
Shell - path name of current shell
Logname - username of current user
TZ - time zone of system

**UMASK -**
Used to reduce file permissions.

**Alias -**
Set in the shell like a shortcut. Eg. alias la = 'ls -A' then the next time u use la it will output that command

**Bash Scripting -**
Helps to automate things but it is powerful enough to run sophisticated commands
// Shebang - #!/bin/bash

vi to open text editor and create file (Vim) but pico works as well
To run the file -

- Use **'source'** when you want to execute a script within your current shell to set environment variables or define functions.
- Use **'bash'** when you want to use a new instance of Bash shell to run a script.
- Use **'sh'** when you want to ensure portability and compatibility with different shells and systems.

Using variables
$1, $2 - first and second argument provided
$0 - name by which the script was invoked
$# - no. of arguments that is supplied
$* - contains all arguments at once

Control Flow
if - then, if-then-else, fi (to terminate) elif for else if

Local and Global Variables

```
jyan@ubuntu:~$ cat scopetest
#!/bin/bash

function localiser {
  echo "In function localiser, a starts as '$a'"
  local a
  echo "After local declaration, a is '$a'"
  a="localiser version"
  echo "Leaving localiser, a is '$a'"
}

a="test"
echo "Before calling localiser, a is '$a'"
localiser
echo "After calling localiser, a is '$a'"
```

before function a is 'test'
in function, a starts as 'test'
after declare a is "
leave localiser a is 'localiser version'
after function a is 'test'

**Loops**
for ((i=0;i<9;i++)) do
for script in *script; do

exec 0<$1
while read line; do
^0 is standard file descriptor for standard import

**Arrays - (Values in bash array is all strings)**
Arrays are not often used in bash and they are delimited by parentheses and the elements are separated by whitespace
example=(aa bb cc dd)
Use bottom command to access array item
${example[1]}
Using @ and * prints out whole array but @ treats each element as individual while * treats array as string and can use IFS = , to change “ “ to “,” when printing. (use @ to preserve the element)
${#example[@]} - prints out length of array

**Shell Metacharacter Examples:**

```
jyan@ubuntu: ~
jyan@ubuntu:~$ echo My Shell is $SHELL
My Shell is /bin/bash
jyan@ubuntu:~$ echo 'My Shell is $SHELL'
My Shell is $SHELL
jyan@ubuntu:~$ echo "My Shell is $SHELL"
My Shell is /bin/bash
jyan@ubuntu:~$ echo My Shell is \$SHELL
My Shell is $SHELL
jyan@ubuntu:~$ echo Today is `date`
Today is Sun Feb 25 20:31:51 PST 2018
jyan@ubuntu:~$
```

```
jyan@ubuntu:~$ ls /etc/hosts /etc/h 1>goodoutput
ls: cannot access /etc/h: No such file or directory
jyan@ubuntu:~$ cat goodoutput
/etc/hosts
jyan@ubuntu:~$ ls /etc/hosts /etc/h 2>badoutput
/etc/hosts
jyan@ubuntu:~$ cat badoutput
ls: cannot access /etc/h: No such file or directory
jyan@ubuntu:~$ ls /etc/hosts /etc/h 1>goodoutput 2>&1
jyan@ubuntu:~$ cat goodoutput
ls: cannot access /etc/h: No such file or directory
/etc/hosts
jyan@ubuntu:~$ ls /etc/hosts /etc/h 1>>goodoutput 2>>&1
bash: syntax error near unexpected token `&'
jyan@ubuntu:~$ ls /etc/hosts /etc/h 1>>goodoutput 2>&1
jyan@ubuntu:~$ cat goodoutput
ls: cannot access /etc/h: No such file or directory
/etc/hosts
ls: cannot access /etc/h: No such file or directory
/etc/hosts
jyan@ubuntu:~$
```

```
jyan@ubuntu:~$ tr d D <file1 | sort | nl >file2
jyan@ubuntu:~$ cat file2

     1  DDD
     2  DDDDDDDDDDDD
     3  DDgfrgwlv
     4  DfDf
     5  DsDfDf
jyan@ubuntu:~$
```

tr translate d into D from file 1 and is sorted and then numbered list into file2

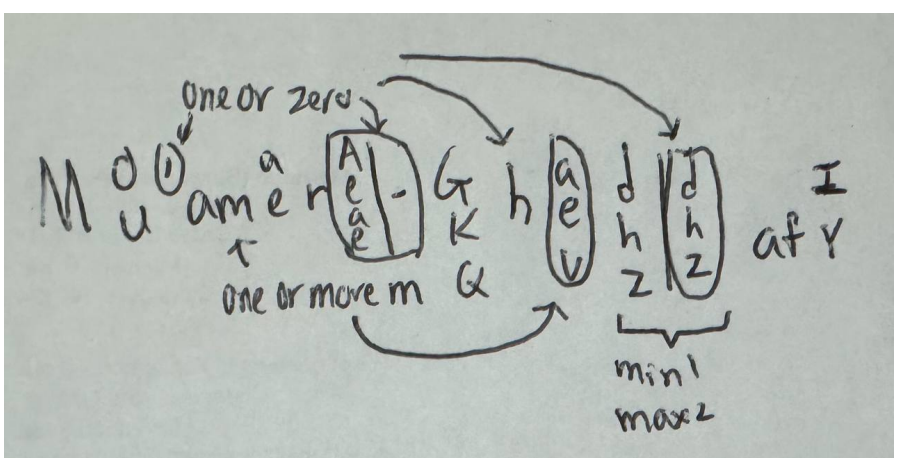
```
jyan@ubuntu:~$ tr l L </etc/hosts
127.0.0.1       LocaLhost
127.0.1.1       ubuntu

# The foLLowing Lines are desirabLe for IPv6 capabLe hosts
::1     ip6-LocaLhost ip6-Loopback
fe00::0 ip6-LocaLnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-aLLnodes
ff02::2 ip6-aLLrouters
```

tr changes the l to L in the list. < sends the output to the command tr
Will this work to edit the file?
tr 'l' 'L' < /etc/hosts > /tmp/hosts_temp && mv /tmp/hosts_temp /etc/hosts

- ^\d{4}$
- Letter[^1238]
- (mother|father)
- M[ou]'?am+[ae]r ([Aeae]|[-])?[GKQ]h?[aeu]+([dhz]|[dhz]?){1,2}af[iy]

Any consecutive 4 digits
Letter exclude anything that is 1238
Mother or father




grep - search for information using regular expression

# Lecture 3

Admin needs to select a unique and meaningful username and not give animal names to users

**Users**

Can belong to a set of groups but only have 1 primary group. Used for billing in the past but not important now.

Groups, especially primary groups, are mainly used to access permissions for files.

System does not enforce that owners or groups for files exist, so when a user creates a file, it is the owner of the file and if the user gets deleted, the file won't be deleted automatically and can still exist in the system which can be a potential security issue. If admin recycles user id and new user has the id of the deleted user, the new user will be the new owner of those files.

In UNIX, users are stored in '**/etc/passwd**'

Contains every user account and is represented in one line. There is several fields that are separated by column and there is :

1. Username
2. Encrypted password placeholder (usually "x", and encrypted password is stored in **'/etc/shadow'**
3. UID (UserID)
4. GID (GroupID)
5. GECOS information (Additional user information, such as user's full name)
6. Home directory
7. Login shell

Eg. jyan:x:1000:1000:Jun Yan, officenumber, phonenumber, homenumber:/home/jyan:/bin/bash

**/etc/shadow**

Contains -

1. Username
2. Encrypted Password
3. Time last change
4. Min time between change
5. Max time between change
6. Warn this many days before password expires
7. Max days of inactivity after expiry before disabled (Solaris inactivity after expiry)
8. Expire (set 0 for active users, set before Jan 1 1970 to disable it
9. Rsvd use sometimes to count failed attempts

//Username:passwd:last:may:must:warn:expire:disabled:rsvd

Uses crypt() to encrypt passwd
**/etc/login.defs**
In linux to change password policy through cmd, just have to edit the login.defs file and only the root user can edit. Once changed will be applied to every user account

**Password Selection**
Administrator must work within confines of human nature
- Cannot make passwords too hard, user will write them down
- Cannot make them change password too often, they will cycle them

**User Organization (Groups)**

- Do not use too complex structure. Now the purpose is to give access permissions to files. It usually represents the relationships between users.
- Can create a storage space and give it to a group instead of giving fixed space to each user
- User will have one primary group and other secondary groups enumerated in **'/etc/group'**
- If the passwd file and group file are not consistent, eg. the user is listed as staff in the passwd file but not in the staff group file, the passwd file will win the argument and the user will be a member of the staff.

Eg. of group which has
1. Name with a maximum of 8 characters
2. Password
3. GID
4. Member field indicates the list of users that are members of the group

//wheel:x:10:trent,bob,sam
cs-staff:*:100:john, tim
Password will be stored in **'/etc/gshadow'**
* Means no password

Commands -
'groups' - displays groups you are a member of
'id' - further display ids of all groups you belong to
'newgrp' - change primary group temporarily

**Home Directories**
Users will usually have their own directories which reflects user grouping structure

**Adding new users**
First thing is for them to accept the policy before the account is created.
Secondly edit etc/passwd, etc/shadow
Adding to etc/group is optional
Must set initial password. Never leave an account without password
Create user home directory and change the owner to the user
Copy startup file to user's home directory
Setup email and update LDAP database
Need to be done manually which is cumbersome

**Useradd command**
sudo useradd jyan - simple and all the perimeters will be configured by system automatically

sudo useradd -c "Jun Yan" -d /home/jyan -g faculty -G famous -m -s /bin/bash jyan
- -g is primary GID, -G is secondary

// sudo useradd -m -g staff -s /bin/bash jyan
sudo passwd jyan

**Adding user in bulk**
Linux can create multiple new users with newusers command but requires password to be stored in plaintext which should not be done.

**Modify user account**
Command "usermod"

**Disable Logins**
- Put a * or some other character in front of user's encrypted password in etc/shadow
- In linux, *usermod* -L *user* locks password and *usermod* -U *user* unlocks password
- Does not notify user of account suspension
- Write a script instead to allow users to login and instead of giving users their shell, this program will run a warning message

**Remove users**

- Remove from local database, phone list, aliases file or add a forward address
- Remove the user from **crontab** file and any pending at jobs or print jobs//
- Kill any of the user's processes that are still running
- Remove users from the passwd, shadow, group, and gshadow files
- Remove the user's home directory
- Remove the user's mail spool
- Duplicate documents that might be important, eg. mail and files before deleting them.
- *userdel* removes entries from both /etc/passwd and /etc/shadow
- -r option removes the home directory
- Any files that were previously owned by the user becomes owned by the number that represents the UID of the deleted user and any future user accounts with the same UID becomes the owner of those files.

**Managing groups**

Edit /etc/group file using text editor
Run *grpck* to check format of /etc/group and ensure that there are no structural errors
Command - groupadd, groupmod, groupdel

**chage will change /etc/passwd information**

- Like expiration date etc.

**Access control**

Root users can act as owner of any object and can perform certain sensitive administrative operations.
The owner can set permission of the file for

- Owner
- Group
- Everyone else

Permission - Read Write Execute (RWX)
Kernel and filesystem tracks users as numbers.

**Root account**

- Superuser and UID of 0
- Changing root directory of a process with *chroot*

Need to change root password regularly, avoid using it over the network

**Role based access control**
Similar to groups but can be used outside of the context of the filesystem.
Role can have hierarchical relationship to one another
su: substitute user identity
If invoked without arguments, it will prompt for root password and start up the root shell.
Root privilege remains in effect until termination of the shell.
*su* - username can substitute other identities
Cons -
Will still need to share root password, will not have records of operations, root will remain in effect until shell is terminated

**sudo - Limited su**
Edit using *visudo* (works like sudo pico but visudo helps to check for errors before admin can save the file)
Users use their own password to authenticate
sudo runs setuid root but consults file /etc/sudoers to see what permissions the users have with sudo.
sudo cannot be executed after 5 mins have elapsed with no further sudo activity
sudo keeps a log of sudo activities

**/etc/sudoers consists of**
- Users whom the line applies to
- Host on which the line should be heeded
- Commands that the specified users can run
- Users as whom the commands can be executed

//
ALL ALL = /dialup, /hangup
(host) (user) they can do (_____)
All users can execute the commands dialup and hangup

jim ALL = /dialup, /hangup
Jim can do dialup and hangup from all host

%admin ALL = (ALL) ALL
%admin means anyone that is in the group admin, the first ALL means any host, (ALL) means as anyone and the last ALL means any thing

jyan ALL = (root) ALL

Gives jyan root privileges and can run every command from any host.
File system
Purpose is to represent and organise the system storage. In windows is usually c, d, e drives and they are based on a fixed size and cannot be changed once created.
UNIX is more flexible which represents the requirements of multiuser multitask environment,
The structure is made up of many small file system and are attached to each other by the mount command

Eg. /usr/local might be another file system in another drive, but since it is mounted to its location, it becomes part of the file system structure
**Pathing**

- //Absolute pathing - Entire path to through file system to object. (/etc/passwd)
- //Relative pathing - Path from current directory to object wanted (start at /tmp/test and want to go to /bin, relative path is ../../bin)

/bin/su, /etc, /mnt, /var, /tmp, /usr

| Directory | Description |
|---|---|
| /bin | Binary commands for use by all users |
| /dev | Device files |
| /etc | System-specific configuration files |
| /home | Default location for user home directories |
| /lib | Shared program libraries |
| /mnt | Empty directory used for accessing disks such as floppy disks and CD-ROMs |
| /opt | Additional software programs |
| /proc | Process and kernel information |
| /root | Root user's home directory |
| /sbin | System binary commands (used for administration) |
| /tmp | Temporary files created by programs |
| /usr | System commands and utilities (/usr/bin, /usr/games/, /usr/include/, /usr/lib, /usr/local, /usr/sbin/, /usr/share/, /usr/src/, /usr/X11R6 |
| /var | Log files and spools |

**Filesystem Type**

Journaling file system means file system will keep track of the change that has not been committed to file system, writing it to a storage place which will be written to a data structure before the change is committed. The data structure is a journal.
It is important as the changes made to the file system often require a few steps. If directly committing the changes to a  file system and it crashes, the file system will enter an unstable state.
Eg.
When deleting a file, it takes a few steps. A file has 2 parts, information node (inode which contains owner, last changed, created by etc) and data node which stores the content of the file. When deleting the file and computer crashes, and when restarted the computer, the file is gone but the 2nd and 3rd step is not done yet and cant see the file but it still occupies the datanode and inode which cause the computer to be in unstable condition.
Journal is created to prevent this from happening. When users have written in the journal, they can execute what was in the journal. Purpose is to keep the file system stable.

File system can be

- Disk partition
- Logical Volume
- Network file server (mapping network drive to remote directory)
- Kernel component
- Memory-based disk emulator

File systems are attached to the tree with mount command and are usually mounted on /mnt folder.
Eg.
mount /dev/sda4 /users - /users file does not exist so sda4 will be located at, /mnt/users/dev/sda4.
If disk storage is not enough and you want to replace it, just unmount and mount the new filesystem and it will have the same path.

If don't want to mount in /mnt, mount /dev/sda4 /media/ will result the path to be /media/dev/sda4

File type

- Regular files (-)
- Directories (d)
- Character device files (c) not important
- Block device files (b) not important
- Local domain sockets (s) - process on one machine talk to another machine process
- Named pipes (p) - processes on  the same machine talk through pipes
- Symbolic links (l)

**File system structure**

Has a -

- Superblock which defines information about the filesystem in general
- Inode table which consist of several inode each describing file or directory for identification.
- Data that makes up content of the file are stored in data blocks that are referenced by inode.
- Inode table is also different in different file systems

**Hard Link and Symbolic Link**

**Hard linked file -**

- Direct copies of the original file share the same inode as well as data node. However when changes are made to either file, they will not modify the main file or the duplicated file. It will request for more data nodes to store the modified data from the file system
- Deleting one hard linked file does not delete all other files.
- If a hard linked file is in a different filesystem, it will just be like copying a file.
- Command - *ln file1 file2* will make hard link to file1 named file2

**Symbolic Link -**

- Like a shortcut but created mainly in cmd prompt and mainly used in the linux and unix environment.
- If you want to create links between different file systems, you should use symlink instead.
- Saves space as well as symlink does not hold data blocks
- Symlink will have different inode from main file as well
- Command - *ln -s file1 file2* will make symlink to file1 named file2

To display inode of file:

- “ls -i filename” or “stat filename”

**File Ownership**

When a user creates a file, the user's name and primary group becomes the owner and the group owner of the file.
Owner and root can change the ownership of the file (user1 and group1 is the name)

- chown user1 file1
- chgrp group1 file1

Usually need to change both

- chown user1:group1 file1

Permissions -

Divided in 3 sections

- Owner
- Group
- Others

// Regular permissions are

- Read (4):
    - Directory permission: I can see and list the file in the directory but not read the file
    - File permission: I can read the file contents
- Write (2):
    - Directory permission: I can create, delete, edit files in this directory
    - File permission: I can modify content of the file, including delete
    - Remove permission is granted if user has either write permissions of the file or the directory
- Execute (1):
    - Directory permission: I can navigate into the directory (cd/enter)
    - File permission: I can run the program or script. (does not have effect on text file)
- rwx = 4+2+1 = 7

**Changing permission**

- chmod u+w, g+r-w,o+r-x file1
    - Add write permission to owner, add read but minus write to group, add read but minus execute to others
- chmod u=rw, g=r, o=r file2
    - Give the owner read and write, group and others read.
- chmod a+x  file3
    - a refers to all, so give all execute permissions as well
- chmod +x file4
    - This gives everyone execute permissions as well

**Using numbers instead -**

- chmod 540 file1
    - Gives owner read and execute, group read and no permission to others
- chmod 644 file2
    - Gives owner read and write, group and others read permission
- chmod 777 file3
    - Gives everyone all permissions

**Default permission**
By default, files are given rw-rw-rw- and directories are given rwxrwxrwx

umask is a special variable that takes away permission on new files and directories immediately after they are created. Most common value is 022. 0 is for the owner, 2 is for the group and the last 2 is for others and it is to take away permission.
To set umask - umask 000 but it only affects the current session and when session ends, umask is removed. Can be set across all session by editing shell configuration file and system wide by editing /etc/profile

Changing Access Control List (ACL)
In addition to user, group and other, can change ACL with setfacl command to give specific user or group permission

- setfacl -m u:lisa:r file
    - M is modify, means lisa have read permission
- setfacl -x g:staff file
    - X is remove so remove all permission given to staff
- getfacl file1 | setfacl --set-file=- file2
    - Get acl from file 1 and give file 2 same permissions

**Special permissions**

- Set user ID (SUID) (4)
    - If set on file that is executable, the person that executed the file temporarily becomes the owner of the file while executing
- Set group ID (SGID) (2)
    - If set on file that is executable, the person that executed the file temporarily becomes a member of the group that is attached to the file while executing
- Sticky bit (1)
    - If set on a directory, in addition to the write permissions, the user may add files to the directory but can only delete the ones they added.

Login program that need root permission will have SUID to give users root permission to access etc/shadow and authenticate themself

Setting special permission -

- chmod 6755 file1
    - SUID, SGID, owner have read, write, execute, group and others have read and execute
- chmod 1777 dir1
    - Sticky bit, everyone have all permissions
- chmod 1770 dir1
    - Sticky bit, owner and group have all permission but others have none

If execute is not set in rwsrwsrwt, it will be 'S/T'. If execute is set, it will be 's/t'. First s represents owner, second s represents group and t represents sticky bit. (eg. rwsrwsrwt, rwSrwSrwT)

# Lecture 4

**Storage management-**
Hard disk - set of disk that is coated in magnetic material and stores data. A head will then move up and down to the right track while the disk spins forward or backward to allow the head to read and write data from the platter.

This manoeuvring takes time and if the data is spreaded in different sectors, it will take longer to read and write the data. So if the reading is random or not in sequence, it will take longer.

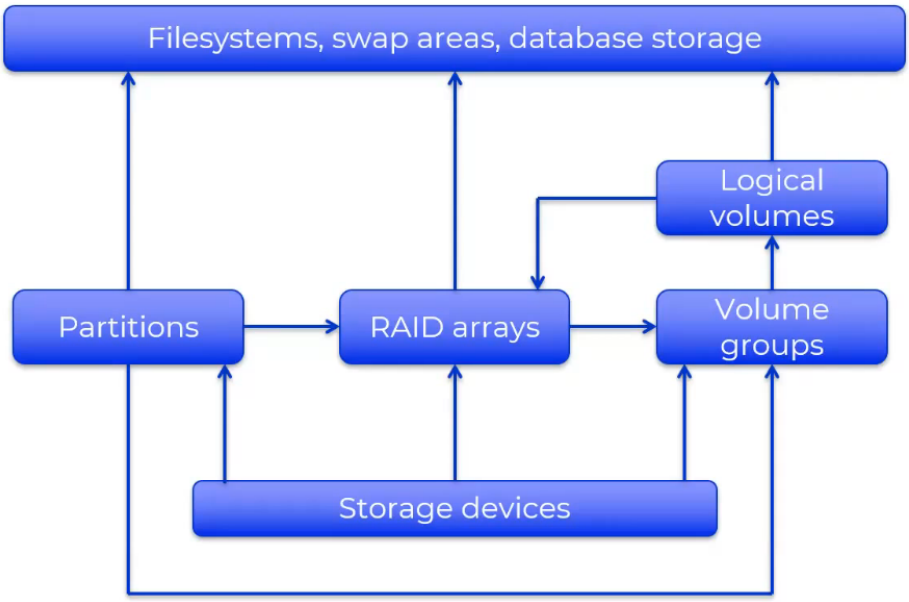
Storage management is independent of the disk used. It is a software to manage the storage software

Disks typically have surface defects which result in unusable sectors. So the disk will use alternate sectors for the bad location. When the disk is in use, they can frequently develop faults and there is no correlation between the operating temperature and the disk defects.

Once in operation, the disk may develop sectors and they will adjust such that bad sectors will not be used. However, in some cases, this might fail and the data might be corrupted.

**Focusing on software in this module**

//Software component mediate between storage device and file system hierarchy,



**Storage devices**

- Built into partitions, RAID arrays and volume groups.
- Eg. hard disk, solid state drive, flash drive, external raid array implemented in hardware, network service that provides block-level access to a remote device
- Device that allows random access, handles block I/O, and can be represented by a device file. Anything that is able to store data

**Partitions**

- Built into file systems or RAID arrays
- Fixed size subsection of a storage device
- Disk level management
- Once created, cannot be changed without damaging the data stored in it
- Each partition has its own device file and a few blocks at the beginning of the disk is reserved in order to store information about these partitions and it is known as master boot record (MBR) in windows. Windows will read the information and calculate the start and end of each partition

| Pros | Cons |
|---|---|
| Separates user data from os to prevent it from corrupting os | Fixed size |
| Backup partitions | If partition table data blocks are damaged, the disk becomes useless |

**RAID arrays (Redundant array of inexpensive/independent disks)**

- Built into file systems or volume groups
- Combines multiple storage devices into one virtualized device
- To increase performance, reliability

**Volume groups**

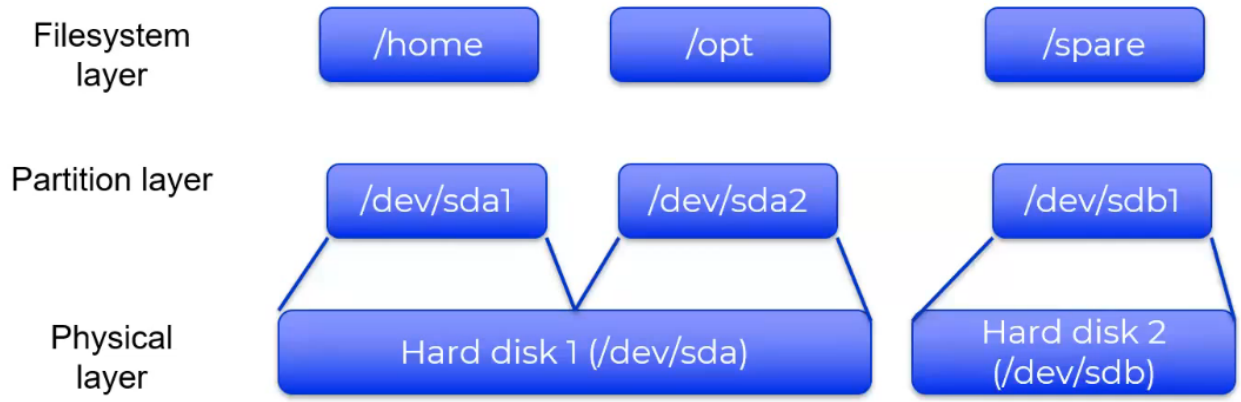
- Built into logical volumes
- Associated to logical volume managers
- Physical device are aggregated to form a volume group (a pool of storage data)

**Logical volumes**

- Built into file systems or RAID arrays
- Associated to logical volume managers
- Divided from volume groups to make logical volumes (similar to partition)

Eg. 750gb disk and a 250gb disk can be aggregated into a 1tb volume group and then split into two 500gb logical volumes

**Traditional data disk partitioning in linux**




But everytime the machine reboots, current disk A might be disk B and disk B will be the new disk A. It is very difficult to identify the disks
Disk devices files are shown as /dev/sda

- sda: first registered drive
- sda1: first partition of sda

Disk name are assigned in sequence as the kernel enumerates the various interfaces and devices on the subsystem
Use command fdisk (basic command line but not designed for large partitions) or parted (can move, resize, create, delete partitions) to partition disk

Root partition -
All systems have a root partition to store configuration files to start the operating system (includes "/" and most of the local host's configuration file).
Advised to keep root partition separate as once there are many processes running, it might corrupt or damage the data on root partition. It is also recommended to make a backup root partition on 2 different physical disks. Should have at least one swap area.
Rule of thumb is to be twice the size of a physical ram.
Put /tmp on a separate filesystem to limit temporary files to a finite size.
Put /var on a separate disk partition or filesystem as it contains log files and will be able to back up this data easily
Put user's home directory on separate partition or volume to isolate the data from other systems
Split swap space among several physical disk to enable parallel access to swap area and access to the virtual memory to improve performance of backup
Simplify backup by making partitions sizes to be able to fit inside backup media

**How to add disk to linux**

1. Attach disk
2. Run sudo fdisk -l to list system disks and identify new drive
3. Run fdisk to add new partitions
4. // Format partitions using mkfs (eg. mkfs -t ext4 /dev/sda4 (make file system type ext4 named /dev/sda4)
5. Mount file system using mount command
6. Set mount options by editing /etc/fstab

**fstab**

- Contains derivatives that tells OS at start up what file systems will be mounted at which location so that the file structure will be correct.
- // Eg. /dev/sda1 /mnt/mydisk ext4 defaults 0 0
- "/dev/sda1" is the name which can be replaced by UUID and is better.
- "/mnt/mydisk" is the mount point.
- "ext4" is the file system type.
- "defaults" is the mount option.
- First 0 is the order in which filesystem checks are performed at boot time. 0 is random, 1 is first, 2 is second and so on
- Second 0 is the order of whether it should be included in the dump backup (creating incremental backup). 0 is not considered for backup, 1 is considered for backup but lower priority than 2.

**Universally Unique Identifier (UUID)**

- Serial number of the file system that is unique and is generated when initializing the file system data structure.

**Mount options -**

- Defaults: read-write mode, enable device files, executables, setuid bit, and so on. Use this when don't want to give file system special options but want to fill in all fields in fstab file
- Errors: sets the kernel behaviour when the system has trouble mounting a file system. Default is normally error=continue but to have it try mount in read only, use errors=remount-ro and to halt it use errors=panic
- noauto: tells kernel to ignore entry. Use to prevent boot-time of removable-media devices. Eg cd-rom or floppy drive
- user: Allows unprivileged users to run mount on a particular entry, which can be handy for allowing access to cd-rom drives

**RAID Implementation -**
//Idea of using clusters of small disks as a group to simulate a larger device and at the same time provide a mechanism whereby a single disk failure does not result in the data becoming unavailable.

Improves performance by striping data across multiple drives, thus allowing drives to work simultaneously to supply or absorb a single data stream

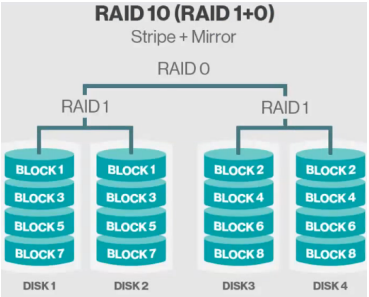
Improves reliability by mirroring (data blocks are reproduced bit by bit on a separate drive) or parity scheme (one or more drives contain error-checksum of block on remaining data drives to recover missing or damaged data. To recover from 2 bit or more error, more parity bit is needed).

**RAID Levels:**

**0 striped disk (no redundancy)**
- Requires 2 or more disk of the same size
- Strips the data alternately among the disks
- Gives best performance but 0 redundancy
- Reliability is worse compared to single disk as there is more disk, hence more chance of failure

**1 mirrored disk**
- Disk 2 is a duplicate of disk 1
- Read is improved but write is the same as need to write to both disks
- Reliability is better as there is a low chance of both disk failing at the same time

**0+1 mirrored and striped**
- Raid arrays can be nested
    - Raid 10 - one zero
        - Stripe first then mirror
    - Raid 01 - zero one
        - Mirror first then stripe



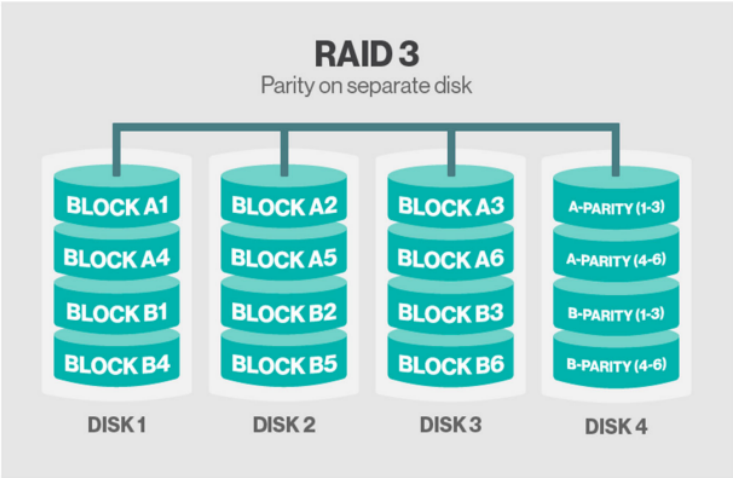

- The primary difference between RAID 10 and RAID 01 is in their layout. RAID 10 mirrors first and then stripes, while RAID 01 stripes first and then mirrors. RAID 10 provides better data redundancy, while RAID 01 may be slightly easier to implement in some cases. Both RAID levels offer good performance, but the choice between them depends on the specific requirements of your storage system and your tolerance for drive failures.

**Error Checking and Correcting - ECC:**
- Included in raid 2-6 to provide extra redundancy measures

- Parity data is used by some RAID levels to achieve redundancy. A certain checksum is calculated which then is written to a disk. If a drive in the array fails, remaining data on the other drives can be combined with the parity data (using boolean XOR function or Reed Solomon code) to reconstruct the missing data

**2 minor variation of 3 not used (skipped)**
**3 striping by byte/word with parity**

- Best for single user systems with long record applications such as streaming media, graphics and video editing
- At least have 3 disk




**4 striping by block with parity**

- Offers no advantage over RAID 5

**5 striping by block with rotating parity**

- Identical to RAID 4 but parity data is spread over all the disk drives
- This helps to increase reading speed
- Only can detect error when a disk fails and user tries to rebuild the drive

**6 striping by block with rotating parity in two parity disk**

- Like RAID 5 but requires more storage to store 2 sets of parity data

**Logical volume manager (LVM) -**

- // More flexible and powerful than disk partitions as it is based on the physical resources in the pool which allows it to expand and shrink on the fly. It is created from volume groups and it will be represented by a device and will act like a disk partition
    - Move logical volumes among different physical devices
    - Grow and shrink logical volumes on the fly
    - Take copy-on-write “snapshots” of logical volumes

    - Replace on-line drives without interrupting services
    - Incorporate mirroring and stripping in logical volume

**ZFS -Zetabytefile System**

- // Modern file system requirements providing redundancy, scalability, data integrity and other feature such as Snapshots, Clones and data compression
- Simple to implement LVM, RAID, Mirroring.
- Group devices in a pool then create formats, mirrors, RAID etc. It is automatically mounted and can change mount point anytime.
    - Create stripped pool using *sudo zpool create demo /dev/sdb /dev/sdc*
    - Create mirrored pool using *sudo zpool create demo mirror /dev/sdb /dev/sdc*
    - sudo zpool status
    - sudo zpool list demo
    - sudo zpool destroy demo
    - Create RAID-Z pool using *sudo zpool create demo raidz /dev/sdb /dev/sdc* (improved version of RAID 5)
- **Create file system**
    - sudo zfs create demo/fs1
    - sudo zfs list demo
    - zfs set quota=500m demo/fs1
    - zfs set reservation=200m
    - zfs set mountpoint=/test demo/fs1
- **Copy on Write**
    - When a user makes changes to the file, it does not write and update the content of the existing data. It will request for new data blocks to write and make changes there instead. Therefore having one additional block means that the system will keep two versions of the file, one old and one new.
    - This allows snapshots to not consume too much additional space as well.
- **Snapshot**
    - Uses the copy of the old data block to create a snapshot at a specific time in the file system whilst not using too much additional space
    - Snapshots are like backups of data, so users can recover from a snapshot if the original file is damaged
    - Have no effect to very little effect on space
    - Snapshot system are implemented per file system rather than per volume
    - Snapshots are read only file

    - zfs snapshot demo/fs1@version1 (demo/fs1 is the file system and version1 is the snapshot name.)
    - zfs rollback demo/fs1@version1 demo/subclone
    - Snapshots are stored in ./zfs directory
- **Clone**
    - A writable snapshot
    - By making a snapshot a clone, user will effectively have 2 file system
    - Share a set of blocks and when changes are made to any of the blocks, new data blocks will be created to reflect the changes but any unchanged blocks will continue to be shared no matter how many clones exist.
    - Clone is used in a scenario where everyday a snapshot is created and one day, the system gets hacked. Users can rollback to old snapshot but will lose all progress. So he should instead create a clone so that the file system can be used and the hacked version can be reviewed by the security team.
- **One filesystem per user**
    - They can do snapshot themselves
    - Can easily set the disc usage on individual user and the file system that contains all users (created from a pool)

**Process management -**

- Process identifies by process ID (PID)
- Each process can start an unlimited number of process called child process, therefore each process have a parent process ID (PPID)
- One process can only have one parent process
- PID is randomly generated from free entries in a process table used by the kernel
- View parent process by using ps -ef (f displays more information on process, e displays list of process across all terminals including daemons, u displays processes by a certain user
- To have a dynamic real time view of process, use the top command
- ps -l list all the processes, but not daemons
- pstree displays process tree
- NI is the nice value, used to affect priority. Can only lower priority value but cannot increase. Pri is the priority value.
- S is the process state. (S is sleeping, R is ready, O is currently running on processor, X is waiting for memory, I is being created, T is stopped or traced by another process, Z is zombie process)
- Zombie process means process should have been terminated and is trouble for administrator

- Terminating process using kill command. (kill -SIGHUP <pid>, SIGKILL kills all process immediately)
- Use & to run process in the background bash script.sh &
- Use bg or fg with pid to move process to background or foreground
- The lower the PRI value (0-127), the higher the priority
- Lower the nice value, the higher the priority
- nice -n <ni value> ./myscript.sh
- renice -n <ni value> -p <pid>

**Cron**
Schedules processes
cron -e to edit crontab
**Scheduling process -**
- at -t 05011200 (set task at 1 may 1200. After this command it will prompt and ask user what process to run)

//Cron - (min) (hour) (day of month) (month of year) (day of week) (absolute path of script or command)
Eg. 20 17 * 1,12 1-5 /myScript (at 1720 of any day in month of january or december from monday to friday run myScript)

# Lecture 5

**Layered Communication Models**
To communicate between 2 computers, there are a set of functions that needs to be done. So designers group functions that are relevant to each other together. Once they are grouped together, they create layers that are placed on top of each other to form the layered model. Functions in the later generations are then able to implement functions in different ways as long as they follow the same interfaces.
This is created to remove compatibility issues.

**OSI Reference Model**
Open systems interconnection model proposed by International Standard Organization. Aim is for people to understand data communication and become a standard practice. It never became an industry standard for data communication but it remained as a theoretical model that defines everything at an abstract level. TCP/IP protocol suite is also aligned with the OSI reference model

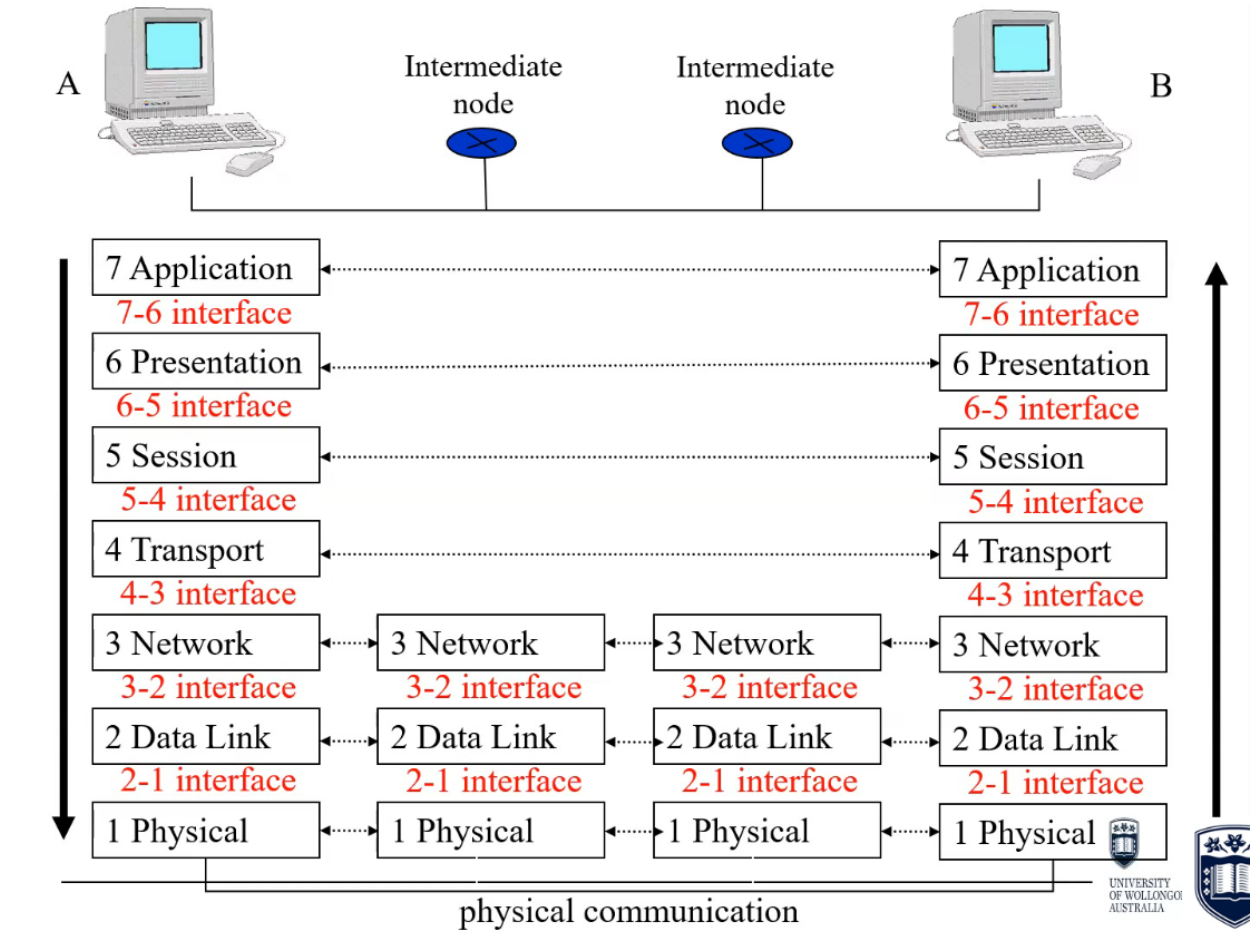
Please do not touch Sean Pnis Ah -
7 - Application - Allow access to network resource
6 - Presentation - Translate, encrypt and compress data
5 - Session - Establish, manage, terminate session. Control who is able to talk at what time, the order of who talks first and how they respond to different messages
4 - Transport - Provide reliable process-to-process message delivery and error recovery, delivers the message to the correct process
3 - Network - To move packets from source to destination, to provide internet working. Responsible transmission from host to host over the network. Handles the IP addressing and the routing
2 - Data Link - To organise bits into frames, to provide hop-to-hop delivery. Able to identify machines in the local area network by referencing MAC address
1 - Physical - To transmit bits over a medium to provide mechanical and electrical specs

Data goes from the sender's application layer down to the physical layer and then up the physical layer to the application layer of the receiver.

TCP/IP protocol suite was proposed before the OSI model was developed. It was proposed as a 4 layered model:
4 - Process/Application -> Session, Presentation, Application
3 - Host to host -> Transport
2 - Internet -> Network
1 - Network Access -> Physical, Data link

**Protocol Data Units PDU**

7 - Application - Data
6 - Presentation - Data
5 - Session - Data
4 - Transport - Segment (Data might be too big so is broken down into segments)
3 - Network - Packet
2 - Data Link - Frame
1 - Physical - Bit




Intermediate nodes are interconnecting devices, routers, switches and hubs. They are typically involved at the bottom 3 layers. At the physical layer, hubs will be involved as it will help to regenerate signals. One device that operates at the physical and data link layer is the switch. Device that has the function of all 3 layers is the router. The switch and router will read the data and decide whether the data is to be transferred within the local area network or does it need to be transferred over the internet by reading the ip address and routing table.

Physical Layer not important
Data link Layer also not very important other than physical address

**MAC Address / Physical Address**

- // 6 byte address (48 bits) in size (00-B0-D0-63-C2-26)
- Imprinted on network interface card when the card in manufactured
- Can create security control that only allow access to certain physical address

**Network Layer**

// Content of frame is a packet that generally has the source address, destination address, time (TTL - time to live (do not want the packet to stay within the internet for too long, everytime the router routes the packet, the TTL will be decreased by 1 and will be discarded when reaches 0)), options (define extra behaviour, not needed to know), checksums
// IP address will not be changed during transmission. The only exception is network address translation which translates the public ip to the private ip address.
There are other protocols as well like ICMP and will be discussed later
Routing is the notion of moving a packet from one network to another and ultimately its destination. Each packet is independently routed and some packets might arrive earlier than the others. Routing decisions are made based on the current status of the network. The network layer only cares that the packets all arrive. Transport layer will assemble the packets in correct order and if data is missing, the source will be informed to retransmit the missing data. If a packet cannot be assembled within a reasonable time, it will be discarded. IPs are used to uniquely identify hosts on the public internet.

**IPV4 - 32 bits**

Consist of 2 parts that makes up the 32 bits:

- Network Portion
- Host Portion

Network mask

- Made up of 32 bits as well
- Continuous 1s followed by continuous 0s
- Used to identify network address and host of ip address

IP has a predetermined class, mask and network address.
Class A to Class E
Class A (255.0.0.0/8, First bit is 0 remaining 7 bit is network, 24 bits for host)

- Maximum network 127
- Maximum host, 2^24 - 2

Class B (255.255.0.0/16, First two bit is 10 remaining 14 bit is network, 16 bits for host)

- Maximum network 2^14

- Maximum host, 2^16 - 2

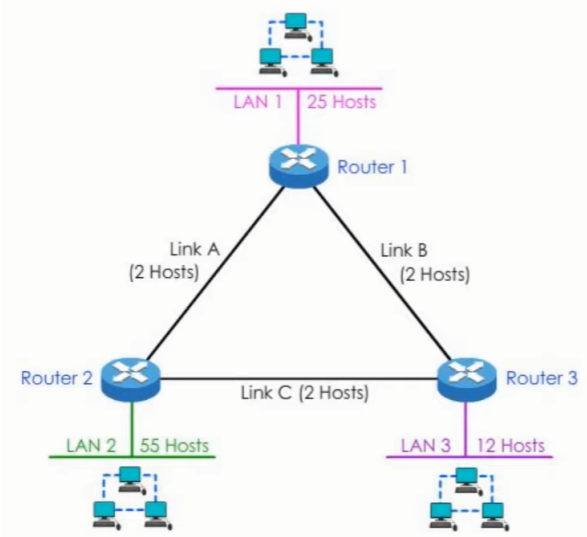
Class C (255.255.255.0/24, First three bit is 110 remaining 21 bit is network, 8 bits for host)

- Maximum network 2^21
- Maximum host, 2^8 - 2

Class D (Multicasting)
Class E (Reserved)

**Subnetting**
151.30.22.12 ip address
255.255.0.0 mask
151.30.0.0 network address
Create 4 diff network from network using borrowing 2 bits and using subnetting creating 4 subnets. If I want 5 networks need to take 3 bits. Can do multiple levels of subnet also
151.30.00|000000.0 = 151.30.0.0 = 255.255.192.0
151.30.01|000000.0 = 151.30.64.0 = 255.255.192.0
151.30.10|000000.0 = 151.30.128.0 = 255.255.192.0
151.30.11|000000.0 = 151.30.192.0 = 255.255.192.0

We have 3 smaller group and want to subnet 151.30.64.0 further
151.30.01|00|0000.0 borrow another 2 more bits
Mask will then be 255.255.240.0




**Question**

The network consists of three Local area networks: LAN 1, LAN 2, and LAN3. These three LANs are connected with three serial links: Link A, link B, and link C.

With an ID range - 192.168.4.0/24, please design an IP plan for the network using VLSM.

// sunnytable - class c

Step 5: Pick the next largest network

**Link A, B, C – 2 Hosts**

| Subnet | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |
|---|---|---|---|---|---|---|---|---|---|
| Host | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Subnet Mask | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

| Network ID | Subnet Mask | Host | Network |
|---|---|---|---|
| 192.168.4.0 | /26 | 64 | LAN 2 |
| 192.168.4.64 | /27 | 32 | LAN 1 |
| 192.168.4.96 | /28 | 16 | LAN 3 |
| 192.168.4.112 | /30 | 4 | Link A |
| 192.168.4.116 | /30 | 4 | Link B |
| 192.168.4.120 | /30 | 4 | Link C |
| 192.168.4.124 | /30 | 4 | Unused |
| 192.168.4.128 | /26 | 64 | Unused |
| 192.168.4.192 | /26 | 64 | Unused |

| Subnet | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768 | 65536 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Host | 65536 | 32768 | 16384 | 8192 | 4096 | 2048 | 1024 | 512 | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| SM | /16 | /17 | /18 | /19 | /20 | /21 | /22 | /23 | /24 | /25 | /26 | /27 | /28 | /29 | /30 | /31 | /32 |

| Network ID | Host Range (16,382) | Broadcast ID |
|---|---|---|
| 172.16.0.0 | 172.16.0.1 - 172.16.63.254 | 172.16.63.255 |
| 172.16.64.0 | 172.16.64.1 - 172.16.127.254 | 172.16.127.255 |
| 172.16.128.0 | 172.16.128.1 - 172.16.191.254 | 172.16.191.255 |
| 172.16.192.0 | 172.16.192.1 - 172.16.255.254 | 172.16.255.255 |

16384/256 =64 so network id increases in 64

| Subnet | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 4096 | 8192 | 16384 | 32768 | 65536 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Host | 65536 | 32768 | 16384 | 8192 | 4096 | 2048 | 1024 | 512 | 256 | 128 | 64 | 16 | 8 | 4 | 2 | 1 |
| SM | /16 | /17 | /18 | /19 | /20 | /21 | /22 | /23 | /24 | /25 | /26 | /28 | /29 | /30 | /31 | /32 |

| Network ID | Host Range | Broadcast ID |
|---|---|---|
| 172.16.0.0 | 172.16.0.1 - 172.16.0.62 | 172.16.0.63 |
| 172.16.0.64 | 172.16.0.65 - 172.16.0.126 | 172.16.0.127 |
| 172.16.0.128 | 172.16.0.129 - 172.16.0.190 | 172.16.0.191 |
| 172.16.0.192 | 172.16.0.193 - 172.16.0.254 | 172.16.0.255 |
| 172.16.1.0 | 172.16.1.1 - 172.16.1.62 | 172.16.1.63 |
| 172.16.1.64 | 172.16.1.65 - 172.16.1.126 | 172.16.1.127 |
| 172.16.1.128 | 172.16.1.129 - 172.16.1.190 | 172.16.1.191 |
| 172.16.1.192 | 172.16.1.193 - 172.16.1.254 | 172.16.1.255 |
| 172.16.2.0 | 172.16.2.1 - 172.16.2.62 | 172.16.2.63 |
| 172.16.2.64 | 172.16.2.65 - 172.16.2.126 | 172.16.2.127 |
| 172.16.2.128 | 172.16.2.129 - 172.16.2.190 | 172.16.2.191 |
| 172.16.2.192 | 172.16.2.193 - 172.16.2.254 | 172.16.2.255 |
| ... | ... | ... |
| 172.16.254.0 | 172.16.254.1 - 172.16.254.62 | 172.16.254.63 |
| 172.16.254.64 | 172.16.254.65 - 172.16.254.126 | 172.16.254.127 |
| 172.16.254.128 | 172.16.254.129 - 172.16.254.190 | 172.16.254.191 |
| 172.16.254.192 | 172.16.254.193 - 172.16.254.254 | 172.16.254.255 |
| 172.16.255.0 | 172.16.255.1 - 172.16.255.62 | 172.16.255.63 |
| 172.16.255.64 | 172.16.255.65 - 172.16.255.126 | 172.16.255.127 |
| 172.16.255.128 | 172.16.255.129 - 172.16.255.190 | 172.16.255.191 |
| 172.16.255.192 | 172.16.255.193 - 172.16.255.254 | 172.16.255.255 |

+64 so 172.16.0.192 range will end at 255 after 255 add 1 bit at the end so 172.16.1.0

**Classless inter domain routing (CIDR)**
CIDR Block - a.b.d.c/n
Size of network 2^(32-n) -2
First number: 32 - n and the rest of the bits is 0
Last number: 32 - n and the rest of the bits is 1

If n = 24, means 24 bits are the network which is also = to 255.255.255.0. But n can be anything. Can be 28 also which makes it 255.255.255.240(11110000).

**Network Allocation Translation**
Needs to be unique so allocation is controlled by organisations like ICANN, in Asia it is APNIC.
RFC1918 defines a class of private address for for users to use in their networks and will not have conflict as the ip cannot be reached by the internet:
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
// To access the public internet, there is a network address translation. When traffic goes out it will translate the ip address to a public one. It is performed by a device called edge device that sits at the edge of the corporate network. By using port address and 1 public address, when multiple devices try to access the internet, the table will remember the combination of public address as well as the port address and when the response comes back, it will translate the ip address from the public to private and send it to the corresponding ports.

**IPV6 - Not in scope**
IPV6, 128 bits, Classless
12AB:34EF:0000:0000
16 bits = 4 hexadecimal number (0-9, a-f)
separated by “:”
0000 = 0
0001 = 1
1111= f

**Routers and Routing Protocol**
Understand the ip address and make the routing decision. Before a packet can be sent to the destination, the route must be determined and there are two possibilities.

- // One, the packet has already reached its destination network. In this case, there is no need to do further routing and the router can use the data link layer function to deliver the packet
- // Two, the packet has not reached the destination network yet. So the router will decide through which interface the package should be forwarded to because the router might be connected to multiple networks with multiple IP addresses. So the table will consult the routing table.

**Routing table**

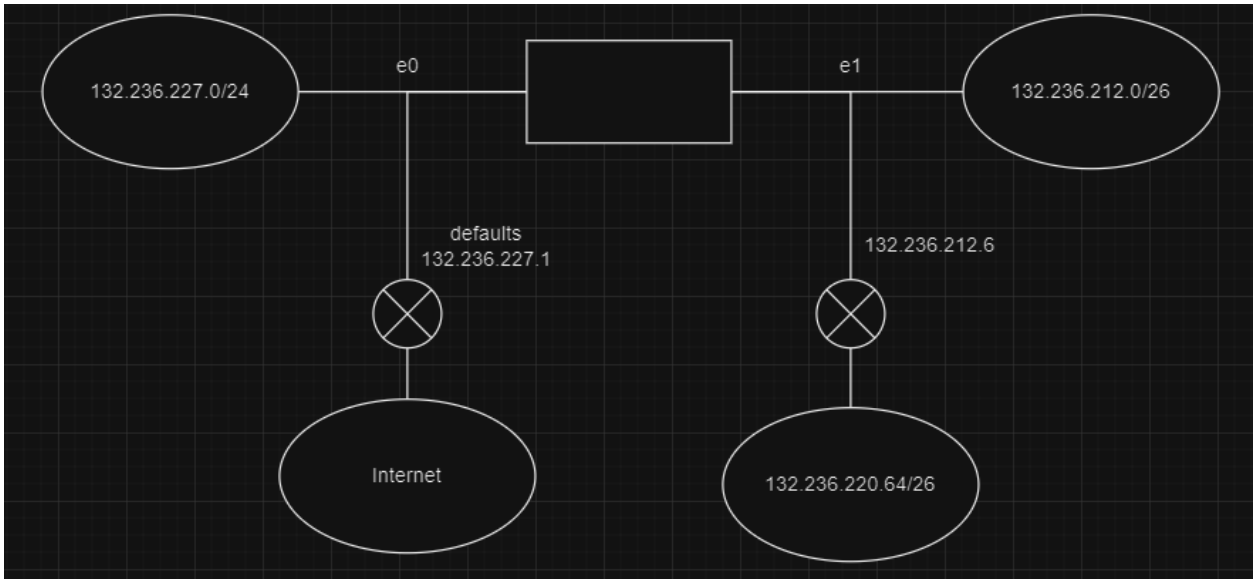
Every entry in the routing table will show the route information. It will contain the following fields:

| Destination (Destination Network) | Mask (Associated to the network) | Gateway (Next device or port the packet should go through) | Flags Interface (Represent Entry features) | If (Interface) |
|---|---|---|---|---|
| 130.130.68.0 | 255.255.255.0 | 130.130.68.4 | U (U means up, working) | hme0 |
| default | 0.0.0.0 | 130.130.68.254 | UG (G means gateway) | |

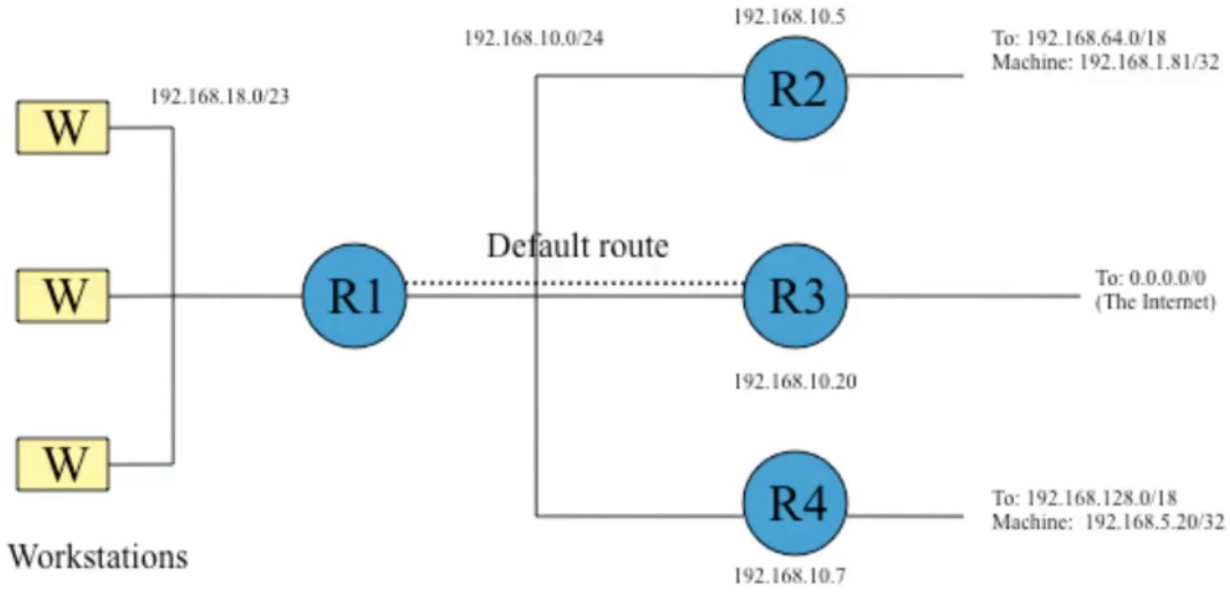
Router will receive the destination ip from the packet then apply the mask to retrieve the network address of that ip. If it matches the destination address, then the packet will be forwarded to that destination. Default is the last result. If no other entries will match then it will be chosen

Exercise
From table draw diagram

| Destination | Mask | Gateway | Flags | If |
|---|---|---|---|---|
| 132.236.227.0 | 255.255.255.0 | 0.0.0.0 | U | e0 |
| default | 0.0.0.0 | 132.236.227.1 | UG | e0 |
| 132.236.212.0 | 255.255.255.192 | 0.0.0.0 | U | e1 |
| 132.236.220.64 | 255.255.255.192 | 132.236.212.6 | UG | e1 |
| 127.0.0.1 | 255.255.255.255 | 255.0.0.0 | U | lo0 |



Exercise From Diagram Draw Table




Answer

| Destination | Mask | Gateway | Flags | If |
|---|---|---|---|---|
| 192.168.18.0 | 255.255.254.0 | 0.0.0.0 | U | eo |
| 192.168.10.0 | 255.255.255.0 | 0.0.0.0 | U | e1 |
| 192.168.64.0 | 255.255.192.0 | 192.168.10.5 | UG | e1 |
| 192.168.1.81 | 255.255.255.255 | 192.168.10.5 | U | e1 |
| default | 0.0.0.0 | 192.168.10.20 | UG | e1 |
| 192.168.128.0 | 255.255.192.0 | 192.168.10.7 | UG | e1 |
| 192.168.5.20 | 255.255.255.255 | 192.168.10.7 | U | e1 |
| 127.0.0.1 | 0.0.0.0 | 255.0.0.0 | U | 10 |

**RIP Protocol**
Router and host talk to each other to exchange route information. The simplest protocol is RIP (routing information protocol)
There are alot of routing protocols, like interdomain routing protocol
Routers will share information with each other periodically and when there is a change in the topology

**ICMP**
// Internet control message protocol
Used to support common utilities for network monitoring and testing.
Ping - When the host sends a request, the ICMP of the remote machine will give a response. Do not overly rely on it because routers can be configured to ignore ping request
Traceroute - uses error reporting of ICMP. Returns a list of routers in the past from the source to the remote machine

**Transport Layer**
// Generally in practice there are 2 main types of transport layer protocol and one of them is TCP which is known as a fully functional layer. It means connection needs to be established before transmission takes place. Connection is virtual and it is to synchronise between parties in communication.

Sender will send synchronisation message to receiver, receiver will send synchronisation message and acknowledge to sender and sender will send an acknowledgement to receiver.

TCP is fully functional which means it has many controls including congestion control flow control. It is responsible for assembling the segments based on sequence number. It is responsible for checking if there are errors occurring in the transmission and it is responsible for the requesting of the missing segments. In applications where performance is high priority, tcp will have the heavy protocol overhead

UDP has a casual protocol which means there is no need to have acknowledgement of the receipt of the message. If the message is lost it is lost. Usually used when high performance is needed but small traffic. Eg dns. SMNP  which is used to retrieve network status data also uses UDP

Port address has 16 bits to represent the port number. Port number that is lower than 1024 is considered as a privilege number so they are used for many services. Things like FTP, SSH, Web, SMNP, SMTP will use a dedicated port number lower than 1024. Need root privilege to open these ports

**Address resolution protocol**
Way to map IP address to physical address.
For any machine, at the final delivery of the package they will need to know the physical address of the destination so that a frame containing the physical address can be constructed. An arp request will be sent out to ask who has the ip address and the one with the ip address will send the physical address. At the same time the machine will keep the address in the cache.

**Reverse address resolution protocol RARP**
Old mechanism to assign IP addresses based on the physical address.
Replaced by DHCP

**DHCP - Dynamic Host Control Protocol**
Used to assign network parameters to the host when the host starts up. Can retrieve a lot of configuration details including IP, DNS, Default gateway from DHCP server.
Without a DHCP server, every device, host, system needs to have their network parameters configured manually.
DHCP is a service that operates when the device accesses a network for the first time. It will provide devices with an IP address, address mask, gateway address of router, dns addresses and other features.
When the device starts up, it will broadcast a DHCP discover message because it does not know where the server is. The DHCP server will then respond with a DHCP offer message. Host will then request IP address with DHCP request message from DHCP server and DHCP server will send address with DHCP ack message.
Internet System Consortium (ISC) maintains a range of open source implementations of DHCP. In linux, DHCP 3 is used. Client side DHCP server comes with the device so there are no requirements.
Server daemon in linux is dhcpd and the associated configuration file is called dhcpd.conf. It is located in the /etc directory.

# Lecture 6

**Network Management -**
To keep network healthy

FCAPS

- **Fault management**
    - Identify and fix fault
    - Predict and acquire information on the likelihood of hardware failure
    - Hardware this days are intelligent enough to send notifications about abnormal conditions that might indicate fault
    - Error notifications need to be managed because some are critical and some are not. If not configured properly, there will be hundreds or thousands of notification
    - Use logic to configure error reporting. Maybe if door open and close too many times within a small time frame, it might mean sensor faulty
    - Document all faults and the fixes. If fault reoccur to many times that means administrator needs to do long term planning
- **Configuration management**
    - Documentation for configuration details is needed otherwise will lose track of configuration details
- **Accounting management**
    - Monitor usage of network resources
    - Do not want user to misuse and monopolize network resources
    - Some users might have limit and quota
- **Performance management**
    - Monitoring users application and devices and make sure the performance level are inline of service level agreement
    - Not every user will have the same access permission to the resources within the network
    - Eg It is the same as service provided by isp. More you pay, faster the connection
    - Traffic needs to be identified to see which bundles the user bought and this is usually identified based on ip addresses or port number or protocols
    - Once identified, different amount of resources will be given with accordance to their agreement
- **Security management**
    - Frequent inspection of packets, monitoring, configuration, retrieving data from devices about network status

    - Potential security hole and hackers can misconfigured network, penetrate system and steal information
    - Ensure that management is done in a secure way and assured that management traffic is coming from authorised administrators
    - Data confidentiality, data integrity, data availability, data privacy, etc. are also part of security management

**Principles**

- Make one change at a time
    - Check the impact of the change one by one
    - Network connecting multiple devices may have different impact on different systems and devices
    - By making multiple changes, it will make it very complicated when it does not work with systems or if it does not work together or if it offsets other changes.
- Document the situation as it was before involvement and document the changes made
    - In order to bring back to previous state in case there is an unexpected impact to the network
    - The best course of action is to roll back to previous state and document it
- Start one end of a network and work through the system's critical component
    - Work from the edge of the network to the core of the network.
    - From the edge of the network it is isolated and can be monitored easily. Once it reaches the core part of the network, it will be aggregated. Thus user might lose track of the individual traffic
- Communicate regularly
- Work as a team
- Use the layers of the network to negotiate the problem. Start at the "top" or "bottom"
    - Look at the perspective of the osi layers from the application layer to physical later or vice versa to make sure every layer works perfectly

**Network Troubleshooting**

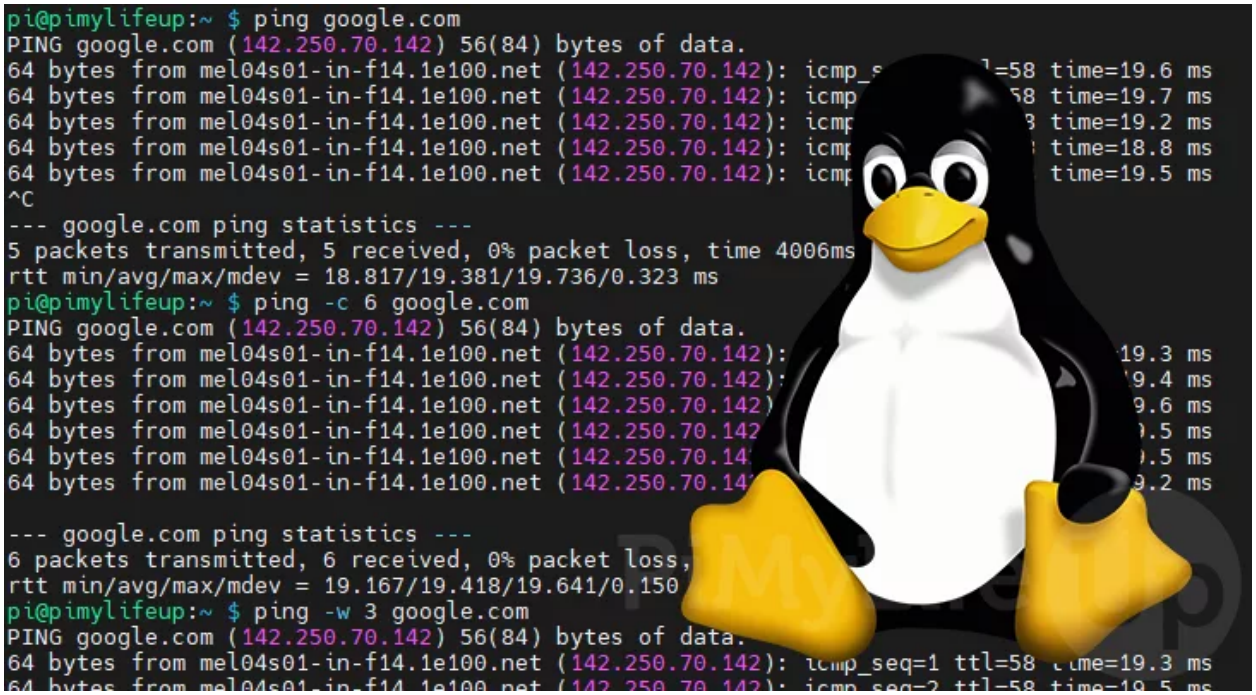
Once have a fix in mind, think about the effect of the change and what is likely to happen, is the effect acceptable

**Ping**

Sends ICMP ECHO_REQUEST to target host and waits for response

Routing table, physical network, and gateways are all involved

Output for ping shows host's ip address and icmp sequence number and round trip travel time




If packet has been dropped, using traceroute will help to find out which section has a problem

**Traceroute**

Uses time to live TTL in ip packets to discover every router on the path from source to destination. Uses TTL number to identify every router on the path.

By running traceroute, the full route to the target host can be discovered and then by pinning intermediate gateways one by one, user can find which gateway is causing the problem

**Inverse Traceroute**

Discover from the external perspective on how to get to host.

**netstat**

Collects a wealth of information about the computer's network status.

- Interface statistics

- Routing information
- Connection tables

**Uses**

- Inspect interface configuration information (netstat -ie)
    - RX and TX - “R = receive, T= transfer. Counter to show the number of packets received and sent on this interface since the start of the machine. Errors and dropped packets can be seen as well”
    - Collision - “Shouldn't be seen even when the network is under heavy load. It is a problem of the past. CSMA CD, carrier sense multiple access with collision detection is used to sense transmission media before they send. Every network card has this inbuilt sensor. With the switch, each machine has its own broadcast channel. If there is collision on network means switch is faulty”)
- Monitor status of network connections (netstat -a)
    - Displays status of active TCP and UDP ports
    - netstat -at (view TCP), -au (view UDP), -p (displays process ID and program each socket belongs to) -atp (), -tnl/-unl (listening tcp and udp with ip address)
    - Shutdown ports that are not listening necessarily
    - Established means it is an active connection and working properly
    - Close wait means its closing
    - Syn send - sent synchronisation message but no acknowledgement has been received
    - Syn wait - is when the host receives a synchronisation message and when the host sends its synchronisation message, the receiver does not acknowledge it. This means host is under a dos (denial of service) attack
- Identify listening network services (-lp (view listening tcp), -lu (view listening udp))
- Examine the routing table (netstat -r)
    - U means up, G means gateway, H is host route, D is route resulting from ICMP redirect (when router a sends packet to b, but should be routed to c instead. B will then inform A that the packet should go to C and A will update its routing table with a D flag to show that it is learnt from ICMP redirect message. It might not be accurate and it needs to be removed after a certain amount of time)
- View the operational statistics for various network protocol (netstat -s)
    - Pay attention to the number of packets that are dropped or discarded
    - See if there is a sudden spike in packets received as well. Might be attackers sending a lot of rubbish packets

    - If a lot lesser traffic, maybe packets have been blocked by firewall or network performance is dropped.

Inspection of live interface activity

- View live activity to identify network problems
- sar -n DEV 2 30 = show network statistics every 2 seconds for 30 times. DEV to show device level information which contains statistic on network interface

**tcpdump**

Packet sniffer that listens to network traffic and records packets that meet criteria of choice.
Need to justify reason on why tcpdump is used as it can violate people's privacy
Sniffers must run as root
It can produce an overwhelming amount of information
Wireshark is a packet sniffing tool
Eg.
sudo tcpdump host bull
sudo tcpdump src net 192.168.1.0/24 and dst port 80

**SNMP - Simple Network Management protocol**

// V1- Protocol for managing network devices. Network devices like router and switch have very little processing power as their main job is to do the routing and switching. So the protocol has a very light overhead so that devices without powerful processing capacity would also be able to support it
Uses agent/station model

- Agent is software capable of answering valid queries from an SNMP station
- Station such as network management system, is software capable of forming queries based on information defined in the MIB
- Can have many servers to one or few clients unlike traditional one server and many clients.
- Manager will run client software so that they can request information from server software which runs on devices
- SMNP is an application layer function that is based on UDP which also has a light protocol overhead so that means it can be used in any devices regardless of their hardware configuration or platform. All the lower layer details will be transparent to SNMP.
    - Performs 3 basic ideas

        - Manager checks agent by requesting information that reflects the behavior of the agent (eg. how many packets have they send, received, dropped
        - Manager can force an agent to perform a task by resetting values in the agent database. (eg. routers have a counter for reboot and if the counter has value zero it will reboot. Therefore a manager can set the agent value as zero to reboot it)
        - An agent can contribute to the management process by warning managers of unusual situations. A trap can be set to monitor buffer utilisation. When it hits the threshold, the manager will be notified. Devices are also able to monitor delays. When it crosses a threshold, it will report to the manager that the device is experiencing a longer delay

**SNMP V1**

- Get-Request
    - Manager will send a get request and agent will reply with a get response
- Get-Next-Request
    - Used in order to retrieve the value of the next item. Used because the manager may not know what information the agent has. To get all the information about the active connection the agent has, manager will keep requesting get next until it reaches the end of the table
- Set
    - To set the parameter
- Get-Response
    - Sends a response to a manager requests
- Trap
    - Informs manager of an event

SNMP needs Structure of Management Information (SMI)(Defines all data structure and data relationship like in a request, date structure needs to be defined eg is this an integer type of data which answers are provided by SMI) and Management Information Base (MIB)( What data is available and what is the type of data) in order to work.

MIB can be defined as a datastore. Each management station or agent maintains a local store of information which is known as MIB. Data stored is live data that changes.

**Management information Categories of Data**

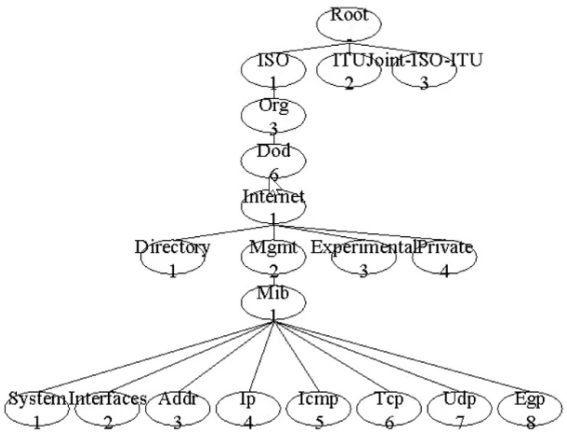
// Stores 4 categories of data

- State information
    - Information about the current state of physical and logical resources along with operational data - provides an instantaneous snapshot in a table (eg. how long system has been running, when was the last time it rebooted, current performance of system)
- Physical configuration information
    - How devices are physically configured (device type,, physical configuration serial number and MAC addresses) Cannot be set
- Logical configuration information
    - How devices are configured such as IP address information, protocols implemented - managed using CLI (command line interface)
- Historical Information
    - Snapshots of performance-related states information (such as packet-counts for each 15 minutes interval over past 24 hours)(usually proprietary format)

MIB Namespace

Can be represented as a tree structure. All nodes of the tree are assigned numeric values.

- iso .org.dod.internet.mgmt.mib.ip.ipInReceives has value 1.3.6.1.2.1.4.3




Limitations of SNMP

- No consideration of security cause anyone can use get and set without authentication
- Officially only standardised for use on IP networks
- Inefficient at large table retrievals (need to keep using get next)

SNMP v2
Same features as SNMP but with enhanced
- Authentication
- Message integrity
- Privacy
- Authorisation and access control

**nmap Network port scanner**
Checks a set of target host to see which TCP and UDP ports have servers listening on them
Find out what a system looks like to someone on the outside who is trying to break in

**DNS**
Used to make people's lives easy and provide a heap of extra information to users.
// DNS is a database that provides name and address mapping from a name to an address or vice versa. DNS can also resolve address and name mapping.

DNS is a distributed database given the size and scale of the internet and has a high performance requirement as it needs to resolve any name quickly. Protocol overhead needs to be light so DNS is based on UDP.
It is responsible for giving structure to the network and since it is hierarchically organised, a part of the domain can be delegated into a subdomain and can be managed separately.

Address mappings used /etc/host back in the day and still can be used till this day. Does not scale well and sites will start exchanging this file in order to learn more but is not scalable, complex and inefficient and DNS was created to solve this problem

DNS was created to solve 2 problems:
- Organization of the internet
    - As ARPANET grew, researches realise that names for host were running out so they needed to impose hierarchy structure
- Synchronisation of host databases
    - As ARPANET grew, it became difficult to keep track of nodes as data quickly became dated

DNS Architecture
DNS defines a tree of domains and each domain represents a chunk or grouping of the network which is managed by a single administrative entity. DNS defines what are known as Top Level Domains (TLDs)

**gTLD - generic top level domains:**

1. Commercial Entities - com
2. Network Providers - net
3. Education Entities - edu
4. Non Profit Organizations - org
5. Government - gov
6. International - int
7. Military network - mil
8. Old Style Arpanet - arpa

**ccTLD - country code top level domains**

1. Australia - au
2. Finland - fi
3. Hong Kong -hk
4. Switzerland - ch
5. Hungary - mu
6. Sweden - se
7. Germany - de
8. Mexico - mx
9. Japan - jp

**Subdomain -**

Domains can create multiple sub domains without the need of approval from anything and anyone

Eg UOW owns uow.edu.au domain which means if they would like to create test.uow.edu.au, they can and they do not need to inform anyone

There is no implicit tie between network number and domain names but it makes administrative sense to keep some relationship between networks and names.

Eg. uow.edu.au has a network address 130.130. The TLD will configure their dns to let it know that subdomains that has the domain name of uow.edu.au authoritative is the university's dns.

If there is a website cs.uow.edu.au, the authoritative server that will resolve this name will be uow.edu.au. If there is a website abc.cs.uow.edu.au, the authoritative server that will resolve this name will be cs.uow.edu.au

**Types of DNS**

- // Authoritative and Non Authoritative DNS
    - Authoritative
        - Authorised to answer queries for a domain. It is guaranteed to be up to date and considered the official representative of a zone/domain
    - Non Authoritative
        - Answers a query typically from a cache and does not know if the data is still valid.
        - Typically include things such as caches and forwarders
- In authoritative grouping, there are 2 kinds of servers. It is a standby server, when the primary server fails, the secondary server will be in service.
    - Masters (Primary)
    - Slaves (Secondary)
- Slave gets a copy of its records from the master using the SOA (Start of Authority) record for the zone
- The data is maintained between the master and slave using zone transfers (over TCP). We can control zone transfers using software eg. ndc

**Recursive vs Non Recursive Queries**

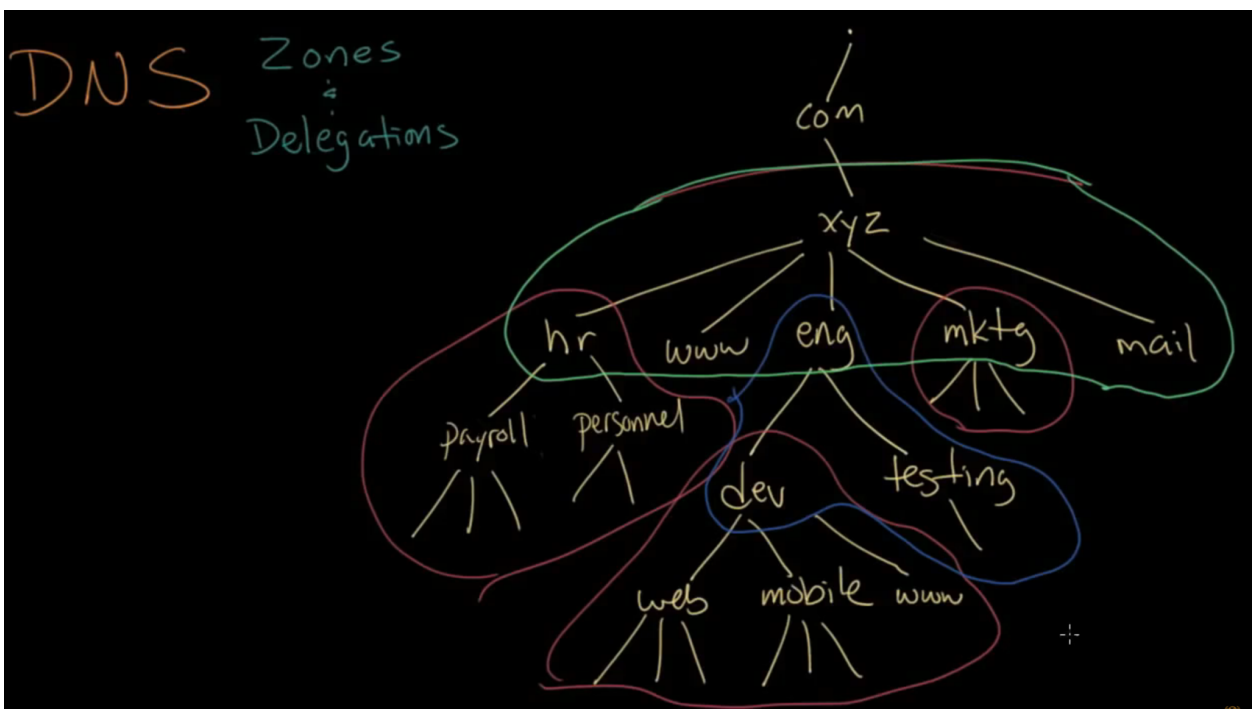
There are two ways in which DNS servers can answer queries

- Non-Recursive
    - DNS will only answer queries that it has the answer for. This may be cached or authoritative. If it does no have the answer, it returns the address of the server that is likely to know the answer
    - If he doesn't have an answer he will give the host another address to ask for the answer.
    - Eg. if the user searches uow.edu.au, and dns does not have the record, it will return the TLD address. In this case the host will ask edu.sg and then edu.sg will say oh i do not have the record and then they will be redirected to the .sg dns authoritative. If .sg DNS does not have the record, it will redirect host to .au DNS followed by the edu.au DNS and lastly the uow.edu.au authoritative
- Recursive
    - DNS returns only names or errors. It follows the referrals to yield the answer. The way this is done is by forwarding the query to a root server that is known.
    - If he does not know the answer, he will ask the and find the answer for the host

- Eg. When a user searches for google.com, the host machine will check its cache as well as the /etc/hosts file. If it cannot find the ip address for google.com, it will ask the local dns for the ip address. If local dns does not know the ip address as well. It will ask the root dns server. The root dns server will then respond with the ip address of the com domain server. The local dns server will then ask the com domain server for the ip address. If it does not know, it will reply with the ip address of google.com domain server. Since www.google.com belongs to the google.com domain server, it will respond with the ip address. The local dns will cache the ip address of www.google.com and send the ip address to the host machine.

**Zone**

- A zone is a domain minus its subdomains
- Each zone has one master name server that keeps the official copy of the zone's data on disk.
- A zone can have several slave name servers that get their data from the master server through a zone transfer operation.
- Typically have two zones;
    - Forward zone name to address mapping
    - Reverse zone address to name mapping



// In zone file there is DNS records which consists of

- **SOA: Start of Authority**
    - Indicates the beginning of a Zone
    - Zone be considered a grouping in the DNS name
    - Have two zone
        - Forward zone for name to address mapping
        - Changed in named.conf
        - ```
          zone "csci322.test"{
             type master;
             file "/etc/bind/db.csci322.test";
          };
          ```
        - Reverse zone for address to name mapping
        - Changed in named.conf
        - ```
          zone "2.0.10.in-addr.arpa" {
          type master;
          notify no;
          file "/etc/bind/db.10";
          };
          ```
    - SOA record typically contains the following
        - The name of the Zone
        - The administrator for the Zone
        - Timeout information e.g.
            - Serial is typically used to indicate last change
            - Refresh specifies how often slave servers check with the master to see if the serial has changed
            - Retry specifies how long after a failure a slave checks the master.
            - Expire
            - Negative Cache TTL is named that cannot be resolved and for this period of time, any other request that has the same name resolution will be rejected for as long as the name resolution stays in the negative cache
        - SOA information is used by slaves to identify when it is necessary to do a Zone Transfer
        - A Zone Transfer allows master and slaves DNS servers to remain in sync
- **NS: Identifies Zones Servers**
    - Identifies which servers are authoritative for a zone

    - How master and secondary DNS servers are defined
    - dig uow.edu.au NS
    - Each domain should have a primary server and at least one secondary
    - Primary and secondary name servers talk among themselves to ensure the consistency of the database
- **A: Name to Address Mapping**
    - Typically look like this “abc in A 130.130.64.68”
- **PTR: Address to Name Mapping**
    - Reverse of A record
    - Typically look like this “68 in PTR  abc”
- **MX: Mail Exchange (used for mail routing)**
    - Help routing of email
    - uow.edu.au 3600 IN MX 100 smtp-gateway.uow.edu.au
    - 100 is the priority. The lowest priority is the primary server
- **CNAME: Synonyms for hosts i.e. Nicknames**
    - Creating a nickname will redirect user from the nickname to the page the cname is pointing to
- **Glue: A Record for a Nameserver**

**Adding new machine to dns bind server**

1. Assign an unused name and address to new machine
2. Log into master name server use dig to find
3. Find name server configuration file (Usually /etc/named.conf)
```
zone “example.com”{
        type master;
        file “filename”;
};
zone “188.77.208.in-addr.arpa” {
        type master;
        file “filename”;
};
```
4. Identify the record of similar machine in the same subnet, eg.
```
template IN A 208.77.188.100
            IN MX 10 mail-hub
```
5. Duplicate this record and change accordingly
6. Change the serial number in the SOA record at the beginning of the file
7. Edit the reverse zone file
```
100     IN PTR template.example.com
```
8. Change the serial number in the SOA record at the beginning of the file

9. Reload the domain
   sudo rndc reload forward-zone-filename
   sudo rndc reload reverse-zone-filename

Host on the Network
Hosts will require many IP addresses if they have multiple interfaces. Each interface to one IP address

Importance of DNS
If DNS fails, most of the service will be down

**The Resolver**
It is edited on the host machine. The file is called /etc/resolv.conf.
File looks like this:

```
domain it.uow.edu.au
nameserver 130.130.68.1
nameserver 130.130.64.1
nameserver 129.78.64.1
options retry:2 retrans:5
search uow.edu.au cs.uow.edu.au
```

domain is the primary DNS domain for the current host
nameserver is the directives to specify the name server to use to resolve queries and is sent from the top to bottom order
For each server can specify a series of options. In the case above is to wait 5 seconds for reply and retry each nameserver 2 times before moving to the next and trying
If nameserver doesn't work, search the bottom 2 domain as well

# Lecture 7

Security
UNIX is optimised for convenience and security was not a high priority during development.
It is an open source software and everyone is able to read the implementation and codes.
Programmers can develop different programs that can run on unix and linux and also the administration jobs are implemented outside of the kernel.
Whilst hackers are able to read the code to find vulnerabilities of the system, developers can do the same as well and fix it.
For Microsoft, you will never know if there is any vulnerability until a successful attack happens. Microsoft will then patch the system.

**How is it compromised**

- **Social engineering**
    - Unsuspecting users have good intentions to help others but easily convinced to give away sensitive information
- **Software vulnerabilities**
    - Software bugs that are exploited by hackers and the solution is to ensure that when there is a new software patch or update, it should be installed.
- **Configuration errors**
    - Made by administrators because they want to get their jobs done easily by bypassing some security controls.

Security Tips

- Keep system updated
- Disable unnecessary services
- Consider setting up secure host to act as central logging machine
- Regular system backups are essential part of any site security plan
- UNIX is relatively immune from virus but because it is difficult does not mean impossible

**Trojan Horse**

Program that contains hidden functionality and when an unsuspecting user executes the code, it does something to compromise the security. An example is the turkey software, where it will draw a turkey on the screen but it will delete files of the system in the background.

**Rabbit program**

- Code that reproduces itself at a high rate and consumes resources intended for other purposes.
- This basically a DOS attack by consuming a lot of resources

**Rootkit**

- Hides certain information (eg, certain files don't show up when user uses ls, certain network information does not show up when user use netstat)
- Hackers use this to remain undetected if they are running process on the system

**Security policy**

System admins need to develop or assist in the development of IT policy within their organisation
If organisation does not have a policy base, they need to change their perspective
Any organisation should have policy documents to cover each operational area

- IT security policy
    - High level should include the vision and mission of the organisation, security philosophy, structure of security, responsibility of security
    - Middle level is defined as issue specific security policy. (eg. policy for internet use or for lab use
    - Lowest level is system specific security policy (eg. system parameters like authorised user for the system)
- Acceptable use policy
- Privacy policy

**Writing policy**

Establish why policy is needed
Questions to ask when writing policies

- What do we need to protect? (Assets can be tangible or intangible? Hardware? Data? Reputation?)
- What might result from failure to protect it? (Risks - Lost of business, trust)
- How might it be attacked and by whom(What channels/mechanism may we be compromised? Network, physical security?)
- What is the cost of protecting it? (Can we afford to not protect it)
- This will allow company to conduct proper risk analysis and develop an appropriate security policy

Mindful that security depends on having a solid computer and network infrastructure
Policy depends on the right questions being asked

**Accessing and prioritising risk**
Identify all the resources in the system. This includes hardware services and data.
Identifying threats to the resources that if realised would cause an interruption to the normal function of the system.
Calculating the risk probability.
The threats do not have to be malicious.
Non malicious threats:

- Software bugs
- Fire
- Power Failure

Cost benefit analysis involves

- Probability it will happen
- Financial impact or costs associated to the risk
- How much money will be lost if the risk is realised multiplied by the probability that it will be.

Bad and good policy
“ all passwords shall be a minimum of 9 characters in length and must include a letter, a digit and a punctuation character.”
It is bad as it contains specifics and will not scale with technology/organisational procedures
“ As far as is possible, machines shall be configured so as to enforce the use of passwords which are difficult to attack via brute force search methods.”

**Policy vs Procedure**
Policy shouldnt be changed often, but procedures can be changed more often and can be attached to the technology.
Procedure are usually more specific and longer as compared to policies.
Policy usually do not change overtime

Management needs to support the security program in order for it to work.

**Policy models**

- Passive
    - Easiest approach to take
    - What i do not know can't hurt me, what they do not know can't hurt me and what i/they do not understand cannot hurt me
- Reactive
    - Better than passive security but it is usually too late.

        - Shutting the stable door after the horse has bolted
            - “We wont have that problem again
            - He/she will not do it again
- Proactive
    - Solve problem before it is exploited
    - Hardest to implement
        - Requires most work, knowledge and understanding from SA
    - Examples of this model include
        - Laissez Faire
            - What is not forbidden is permitted
        - // Draconian (not yours dont touch)
            - What is not permitted is forbidden

**Logging**

Does not increase the security of the system but enforce security
Helps to detect when compromise has occurred
If logged attempts to break in, defences in area that is under attacked can be strengthened
Should be done to at least 2 destinations. Local machine and relatively secure log host.
If a person gets root on a machine, they can delete the log files but not on the log host
Alternatively, they may attack the log host first in which case the local machine logs may be the only record of the event if the attack fails.
With all servers logging to a central syslog. It becomes easier to correlate events across the company

**syslog**

On unix, logging is typically performed by syslog. It allows facilities to be defined.
Logs can be stored on a local host or forwarded to a remote host
SA can define which facilities would be able to log and the severity level of the event that needs to be logged.
Attackers will fabricate alot of log data so that when there is not enough space for logging, their attacks will not be logged
2 descriptive labels associated with the message to make it easier to handle
One is to describe the function (facility) of the application that generated it
Second is the degree of severity of the message
syslog defines facilities which identify programs that can log
This includes:

- auth,
- kern,
- mail,

- cron,
- lpr and others

Syslog severity levels

| Severity Level | Keyword | Description |
|---|---|---|
| 0 | emergencies | System unusable |
| 1 | alerts | Immediate action required |
| 2 | critical | Critical condition |
| 3 | errors | Error conditions |
| 4 | warnings | Warning conditions |
| 5 | notifications | Normal but significant conditions |
| 6 | informational | Informational messages |
| 7 | debugging | Debugging messages |

Sample of syslog.conf

- *.debug /var/log/messages (captures messages from debug severity and above in the /var/log/messages file.)
- .info;mail.none;authpriv.none;cron.none /var/log/messages (captures all messages of severity “info” and above are logged but none from mail, authentication, facilities/subsystem or cron)

**What to log**

List of things to always log:

- Su attempts
- Network connections
- Failed logins
- Rejected file system mount operations
- Transaction on services

Use cron job scheduler to analyse logs and check for anomalies. Usually scheduled at non peak hours when system load is light

Never trust logs as hackers know how important log files are and they can flood it to cover illicit activities or modify log information

Overall security level is determined by the weakest link which is humans.
Users can never be predicted. They hate security in general because it is controlling. Security means everything they do is monitored, audited and corrected. Often needing to do extra stuff for security and not for the job

- Users storing sensitive information on machine for convenience
- Users letting their boy/girl friend use their account
- Users bring sensitive information home

SA focuses too much on external threats as well but there are malicious users internally as well

**Physical security**

No system is secure against an intruder who has physical access to a machine
An intruder can:

- Boot from an alternate media
- Remove/Copy disks or tapes
- Install additional hardwares

Machine rooms need to be secure and the data they house needs to be protected.
Difficult in an environment where there are contractors.
Servers needs to be housed in secure environments

**Backups**

Backup strategy are important adjunct to system security since if a compromise is detected, trusted data will have to reload from backups
Once a machine is root compromised, the data cannot be trusted anymore.
However sometimes hackers go for backup data when they attack organisations, so have a copy off site

**Data integrity check**

System components not required to be modified would be read only and not modifiable even by root and is difficult to achieve.
Integrity checking of important files is the best way to detect intrusion
Tripwire stores checksum in secure way to track changes if user modifies the file

**Encryption**

Basic tool of system security and should be used a lot more than it is
Transforming text into something that cannot be understood
Not used as much because of high cost in CPU and difficulties of administration (PKI - public key infrastructure)
Particularly sensitive information should be encrypted especially for network transmission

SA errors also play a part

- Simple typing errors

- Bugs in code
- Careless system configurations
- Bad system default settings

Eg files left laying around containing encrypted password
These sort of problems are much more common than attacks against encryption keys
More likely caused by human aspects

What should administrator do

- Ensure physical security
- Stay on latest patch release
- Remove unnecessary service
- Check permission on important files/directories
- Set up logging properly
- And monitor important logs
- Know and control trust relationship

Cert and auscert helps to keep SA up to date about security knowledge

Network security

- Set of measures to mitigate risks to the network and devices using the network
- Network security allows to build layers of protection
- Erect multiple hurdles or “safety nets” to make life difficult for an attacker or to catch unexpected behaviour at an early stage

Rationale

- Are all devices on network as secure as they should be
- SA will not have control over every device using the network (Personal devices of staff)
- Will not have enough resources to make every device secure
- Some device cannot be made sufficiently secure

Threats

- Eavesdropping
    - Listens or watches traffic on network to capture confidential data
    - Need to make the data encrypted
- Spoofing (impersonation)
    - Impersonates user or device by faking an protocol attribute that is used in authentication process
    - Faking the source address on UDP packets

        - Man in the middle is a famous attack in this category by intercepting messages and modifying the message. By being in the middle and disrupting the communication process by giving both users wrong messages
    - Modification of network communications
        - Hijack communication between two devices and modify messages to influence the behaviour of one or both parties
    - Denial of service
        - Attackers finds a way to cause network service to stop functioning as expected and is a threat to accessibility
        - Achieved by flooding network with messages like TCP SYN messages with fake IP addresses
        - DDOS is this but with the use of bots

Often used in combination

Network security measures
Implemented
- At the end host
- Networking devices

By restricting who and what can access network physically and otherwise and be careful on how data is transmitted on the network
Restrict access to services to only people that require them by using authentications
Eg
- Passwords
- Public key authentication
- One shot password
- Kerberos

Physical security is important as well because it is often large and covers a large area. Attacks can be made if attackers have physical access to the infrastructure. Devices should be physically secured and authenticated secure.
Data integrity
Many protocols have been designed without much thought to security eg IP
Secure ip like ip sec, secure dns like dns sec and secure shell like ssh is used
IPSec has two mode
- Transport mode
- Tunnel mode
    - Create an additional IP header and will have the two ends of the tunnel at its IP address.

        - The two IP at the ends of the tunnel will be the source and destination of the new header so no one can see what is happening in the tunnel

Secure DNS

- Used to secure zone transfer between master and slave
- Need to protect when the data is copied from master to slave, we want the data to be correct otherwise if hackers attack zonetransfer and make fake copy of the zone files on slaves, it will be redirected to the fake server

Does not need to secure dns resolution because the information is supposed to be public

Packet filtering

Most effective control and they are basic and easy to configure, maintain operate and powerful

Access control lists

Networking devices that understand the transport protocols and sometimes higher can decide which individual protocol data unit it will allow into or out of the network

This can be used to permit or deny access to services based on rules

Intrusion Detection System

Detect any potential intrusion and prevent it from happening

Can be implemented in two different ways

- Network based intrusion system
    - Monitor the network to detect the intrusion
        - By using signatures, most attacks will have a unique signature. So have a few signatures and then compare with the network traffic and if it is a match then it is an intrusion
        - Anomaly based attack type. What SA knows is the baseline traffic and anything that is significantly deviated from this place traffic pattern will be suspicious and regarded as an intrusion
- Host based intrusion
    - Attackers will try to modify the file and this type of intrusion detection will monitor the key configuration file to see if anyone tried to modify, read or write it

Prevention

If traffic coming from an IP is intrusive, SA can dynamically change IP filters or change firewalls to block the traffic from this site.

Secondly if the intrusion is happening, SA can create a honeypot to make attackers hack that site instead. Honeypot is a part of a system that is not important but staged to look

important by the SA. Once they attack the honeypot, they will leave. If they stay then SA can collect more evidence.
Worst case scenario is to shutdown the network to stop the intrusion completely.
Incident response plan
It defines clearly when this incident is detected, who was reported, who will be reported, what actions need to be taken, what actions need to be taken to mitigate the impact or stop the incident.
Incidents are small
Disaster recovery plan is covered for more disastrous event which would need approval from higher level and would involve external agencies if it is a large scale attack
Business continuity plan is another level where current site is no longer usable and company will shift to different site to continue

- Cold site
    - Have infrastructure only, no data
- Hot site
    - Have infrastructure, hardware, software and data to continue.
    - More expensive to maintain

# Tables and Cheat Sheets

### UNIX Command Cheat Sheet

| Command | Description |
|---|---|
| ls | List your files |
| more filename | Show the first part of a file |
| emacs filename | Create and edit a file |
| vi filename | Create and edit a file |
| mv fn1 /destination/path/ | Move a file |
| cp fn1 fn2 | Copy a file |
| rm filename | Remove a file |
| diff fn1 fn2 | Compare files, and show where they |
| wc filename | How many lines, words, and characters |
| chmod | Change the permission of a file |
| gzip filename | Compress a file gzip |
| gunzip filename | Uncompress a file gunzip |
| gzcat filename | Look at a gzipped file without having to gunzip it |
| cat filename | Look at the content of the file |
| lpr filename | Print |
| mkdir dirname | Make a new directory |
| cd dirname | Change the directory |
| pwd | Where you are |
| grep “pattern” filename | Look for the string in the files. |
| w | Who’s logged in and what they are doing |
| who | Who’s logged in and there they are coming from |

| | |
|---|---|
| finger | Display information on system users |
| last | Give a list of everyone’s logins |
| id | Display the user id and group id |
| uname -a | Display all information about the system |
| date | Current date and time |
| cal | Display the calendar of the current month |
| exit | Exit the current shell |
| whoami | Return your username |
| passwd | Change your password |
| ps | Display current processes |
| kill PID | Kill the process with the id you have |
| quota -v | Show what your disk quota is |
| echo | Print text to the terminal screen |
| mail | Send file by email |
| ssh | Open a secure connection |
| ftp | Upload or download file |
| !! | Repeat the previous command |

| | |
|---|---|
| cut | Prints selected portions of its input lines |
| sort<br>sort –r | Sorts lines in a file (ASCII)<br>Reverse sorts lines in a file (ASCII) |
| wc<br>wc -l<br>wc -w<br>wc –c | Counts the number of lines, words, and characters in a file |
| pr<br>pr –d | Formats a file for printing<br>Formats a file double spaced |
| tr | Replaces characters in the text of a file |
| grep | Displays lines in a file that match a regular expression |
| nl | Numbers lines in a file |

# Sort

| Option | Meaning |
|---|---|
| -b | Ignore leading whitespace |
| -f | Case insensitive sorting |
| -k | Specify the columns that form the sort key |
| -n | Compare fields as integer numbers |
| -r | Reverse sort order |
| -t | Set field separator (the default is whitespace) |
| -u | Output unique records only |

| String | Numeric | True if |
|---|---|---|
| x = y | x -eq y | x is equal to y |
| x != y | x -ne y | x is not equal to y |
| x < y | x -lt y | x is less than y |
| x <= y | x -le y | x is less than or equal to y |
| x > y | x -gt y | x is greater than y |
| x >= y | x -ge y | x is greater than or equal to y |
| -n x | - | x is not null |
| -z x | - | x is null |

- nt and -ot important

| Operator | True if |
|---|---|
| -d file | file exists and is a directory |
| -e file | file exists |
| -f file | file exists and is a regular file |
| -r file | You have read permission on the file |
| -s file | file exists and is not empty |
| -w file | You have write permission on the file |
| file1 -nt file2 | file1 is newer than file2 |
| file1 -ot file2 | file1 is older than file2 |

**Shell Metacharacters**

| Metacharacter | Description |
|---|---|
| $ | Shell variable |
| & | Background command execution |
| ; | Command termination |
| < << > >> | I/O redirection “>>” is to append and add to the bottom of the file |
| \| | Command piping |
| *<br>?<br>[] | Shell wildcards<br>0 or any character<br>0 or 1 of that character<br>Either of the items inside the set |
| ‘ “ \ | Metacharacter quotes |
| ` | Command substitution (Eg. echo Today is `date`) |
| () {} | Command grouping |

**Manual Section Number**

| Section | Description |
|---|---|
| 1<br>1M<br>X1M | Commands that any user may execute<br>Command that only root user may execute<br>X Windows commands that only the root user may execute |
| 2 | System calls |
| 3<br>3M<br>3F | Library routines and functions<br>Mathematical functions<br>Fortran functions |
| 4 | File formats |
| 5 | Miscellaneous |
| 6 | Games |
| 7 | Device drivers and interfaces |

**useradd and usermod Options**

usermod does not have “-m”, “-k”, “-o” options

| Option | Description |
|---|---|
| -c “description” | Adds a description for the user to the GECOS field |
| -d homedir | Specifies the user’s home directory |
| -e expirydate | Specifies the date to disable the account |
| -f days | Specifies the number of days that an inactive account will be disabled |
| -g group | Specifies the primary group for the user |
| -G group1, group2, etc. | Specifies all other group memberships for the user |
| -i | When used with the -u option, it allows a UID that is being aged to be used |
| -k directory | Specifies the skeleton directory used when copying files to a new home directory |
| -m | Specifies that a home directory should be created for the user account |
| -o | When used with the -u option, it allows a UID to be duplicated on the system |
| -s shell | Specifies the absolute pathname to the shell used for the user account |
| -u UID | Specifies the UID of the user account |

**Check file system type**

*df* Command – Find Filesystem Type.

*fsck* – Print Linux Filesystem Type.

*lsblk* – Shows Linux Filesystem Type.

*mount* – Show Filesystem Type in Linux.

*blkid* – Find Filesystem Type.

*file* – Identifies Filesystem Type.

*fstab* – Shows Linux Filesystem Type.

important  - lsblk (command), fstab (file), mount (command)

**Format disk**

```
FORMAT MENU:
        disk          - select a disk
        type          - select (define) a disk type
        partition     - select (define) a partition table
        current       - describe the current disk
        format        - format and analyze the disk
        repair        - repair a defective sector
        show          - translate a disk address
        label         - write label to the disk
        analyze       - surface analysis
        defect        - defect list management
        backup        - search for backup labels
        verify        - read and display labels
        save          - save new disk/partition definitions
        volname       - set 8-character volume name
        !<cmd>        - execute <cmd>, then return
        quit
```

Practical 1 -

- shutdown -h now
- ping -c 4 8.8.8.8

Practical 2 -

- cd /tmp
- pico filename1.sh
- #!/bin/bash
- sudo useradd
- tail /etc/passwd
- sudo usermod -g, -G
- crontab -u user -e (edit)
- crontab -u user -l (list)

Practical 3 -

- date
- more /etc/timezone
- timedatectl list-timezones | grep Australia
- sudo timedatectl set-timezone Australia/Sydney
- timedatectl status
- sudo service cron restart
- arp (to find ip address)
- sudo arp -d ipaddress (remove ip)
- sudo tcpdump -c 4 “icmp or arp” (track 4 packets from icmp or arp)
- sudo wireshark & (& to push to background)

Practical 4 -

- cd /etc/bind
- sudo pico /etc/bind/named.conf.options (setup cache/forwarder nameserver)
- sudo service bind9 restart
- dig

- route -n (find router gateway)
- sudo pico /etc/netplan/50-cloud-init.yaml (static ip)
- sudo netplan apply
- sudo pico /etc/netplan/named.conf.local
- sudo cp /etc/bind/db/local /etc/bind/db.mycompany.com
- sudo pico db.mycompany.com (forward zone)
- sudo cp /etc/bind/db/local /etc/bind/db.10 (reverse zone)
- dig -x (ip to lookup) @(dns to query)
- dig -t MX uow.edu.au (finds the name of the uow mail host)

Practical 5 -

- lsblk -o NAME,SIZE,FSTYPE,TYPE,MOUNTPOINT (Identify disks)
- sudo mdadm --create --verbose /dev/md0 --level=5 --raid-device=3 /dev/sdb /dev/sdc /dev/sdd (create raid 5 with 3 disk called md0)
- cat /proc/mdstat (view raid status)
- sudo mkfs.ext4 /dev/md0
- sudo mount /dev/md0 /mnt/md0
- df -h (disk free that is human readable)
- sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf
- sudo update-initramfs -u (arrange array to reassemble automatically at boot)
- echo '/dev/md0 /mnt/md0 ext4 defaults,nofail,discard 0 0' | sudo tee -a /etc/fstab
- sudo pico /etc/exports
- /mnt/md0 *(rw,sync,no_root_squash)
- sudo systemctl start nfs-kernel-server.service
- showmount -e server.test.com
- sudo mkdir -p /share/md0
- sudo mount -t nfs server.test.com:/mnt/md0 /share/md0
- server.test.com:/mnt/md0 /share/md0 nfs defaults,user,exec 0 0 (edit in fstab)

Practical 6:

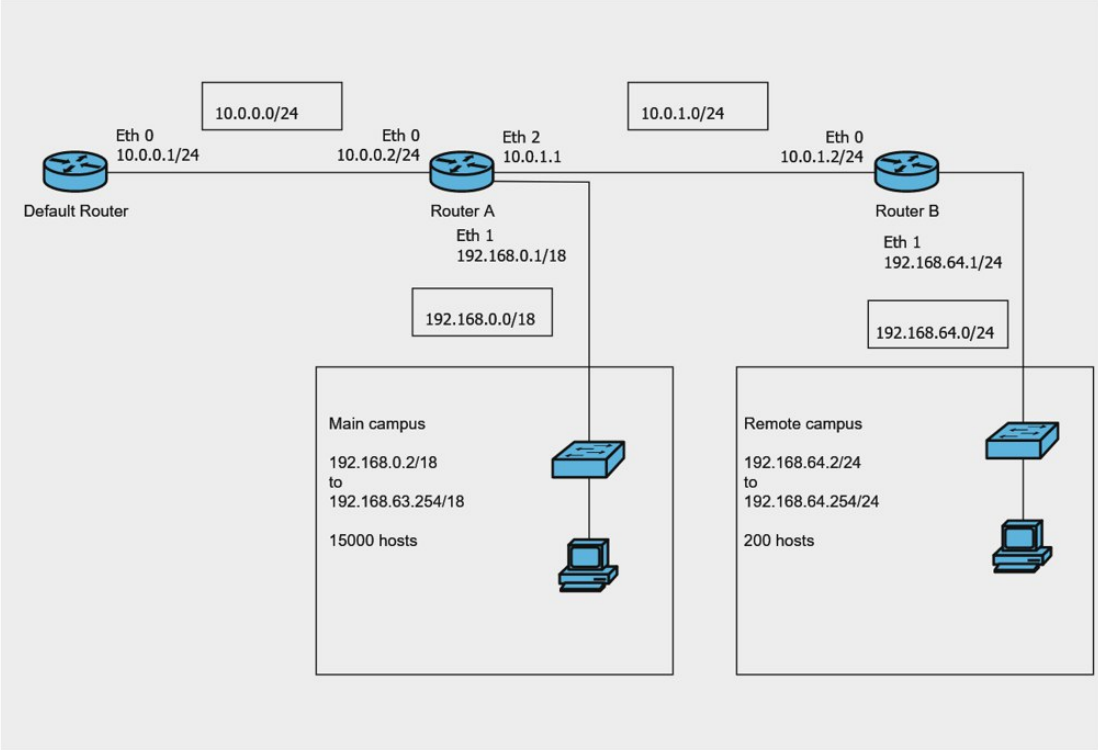
- sudo zpool create myZpool mirror /dev/sda /dev/sdb
- zpool status
- df -h
- zpool get health myZpool
- zpool get size,free,allocated myZpool
- sudo zfs create myZpool/test1
- zfs list
- sudo chmod 777 myZpool/test1
- zfs get -r compression myZpool
- sudo zfs set compression=lz4 myZpool/test1
- zfs get compressratio myZpool/test1
- sudo zfs snapshot -r myZpool/test1@snapshot1 (cd /myZpool/test1)
- zfs list -t snapshot
- cp .zfs/snapshot/snapshot1/file1.txt file1.txt
- sudo zfs rollback myZpool/test1@snapshot1

Practical 7

- echo 1 > /proc/sys/net/ipv4/ip_forward (allow packet forwarding)
- iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE (Postrouting chain in the nat table indicates that the interface enp0s3 should be used for outgoing packets and Masquerade indicates that the interface will mask the internal IP address with the external ip address of the router)
- sudo pico /etc/sysctl1.conf (edit: net.ipv4.ip_forward = 1)
- sudo apt install iptables-persistent
- sudo netfilter-persistent save

//

## Network diagram




## Router A routing table

| Destination | Mask | Gateway | Flags | Interface |
|---|---|---|---|---|
| 10.0.0.0 | 255.255.255.0 | 0.0.0.0 | U | Eth0 |
| 192.168.0.0 | 255.255.192.0 | 0.0.0.0 | U | Eth1 |
| 10.0.1.0 | 255.255.255.0 | 0.0.0.0 | U | Eth2 |
| 192.168.64.0 | 255.255.255.0 | 10.0.1.2 | UG | Eth2 |
| Default | 0.0.0.0 | 10.0.0.1 | UG | Eth0 |