KCS-401

Operating System

Dr. Upasana Pandey

Associate Professor

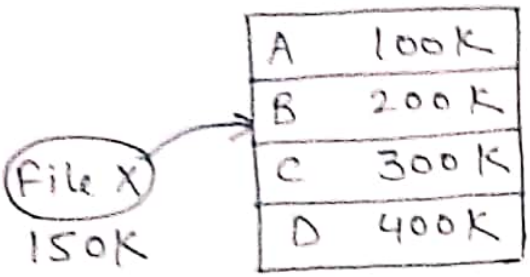
Department of Computer Sciences & Engineering

IMS Engineering College (College Code: 143)

File System

Free Space Management :

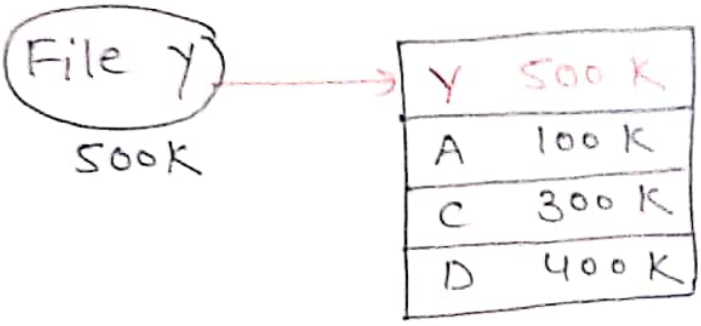
Free-space list is used to keep track of all free disk-blocks.



remove this entry after allocation.

Free-space list

File Y deleted from the disk then



Free-space list

- Free-space list can be implemented as bit-map or bit-vector.
- If Block allocated then represent by 0.
- If Block is free, represent by 1.

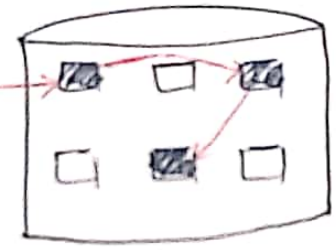
For example - Allocated blocks are :

2, 3, 4, 5, 6, 8

0	1	2	3	4	5	6	7	8	9
1	1	0	0	0	0	0	1	0	1

- Another approach is to link together all free disk blocks.

Free List have pointer of first free block.



File System Structure

- File structure
  - Logical storage unit
  - Collection of related information
- File system resides on secondary storge (disks).
- File system organized into Layers.
- File control block – storage structure consisting of information about a file.

Application Program
↓
Logical File System
↓
File organization module
↓
Basic File System
↓
I/O control
↓
Devices.

(i) Application Program : It is top Layer. The program which is developed by the user is called "Application program." It is a file or program.

This file is given as an input to the Logical file system.

(ii) Logical file system :

Logical file system will check whether file is present in directory structure. If the file is present in the directory structure then it finds the location of the corresponding file. It also find the logical block number

File name → Logical file system → checks its presence in directory structure → finds logical block number.

Logical block number will be given as input to the file organization module.

ii) File organization module :

Accepts input as logical block number, and map in order to find the physical block in which file is stored.

Physical block number is given to Basic file system as input.

(iv) Basic File system :

Basic file system issues a command to I/O control. with the help of Block number.

Received block number 123

↓

Read the block 123

↓

write the content in block 123 or print it.

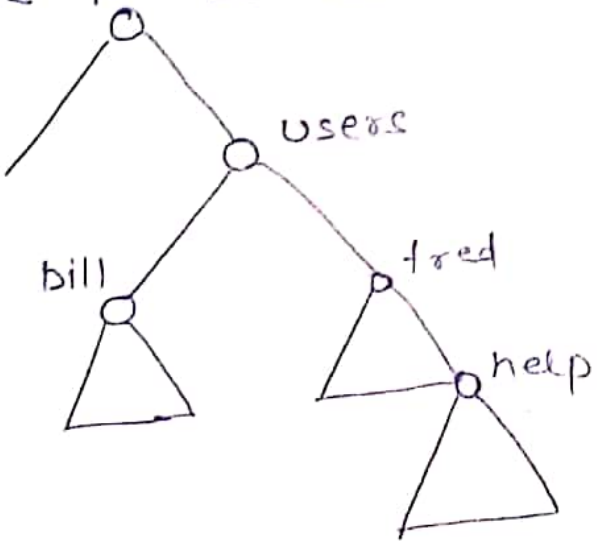
(V) I/O controls : (device drivers file)

Accept the command and operation will be done.

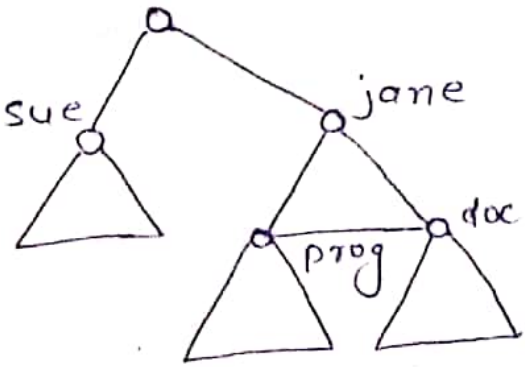
(VI) Device : Perform I/O operations.

File System Mounting :

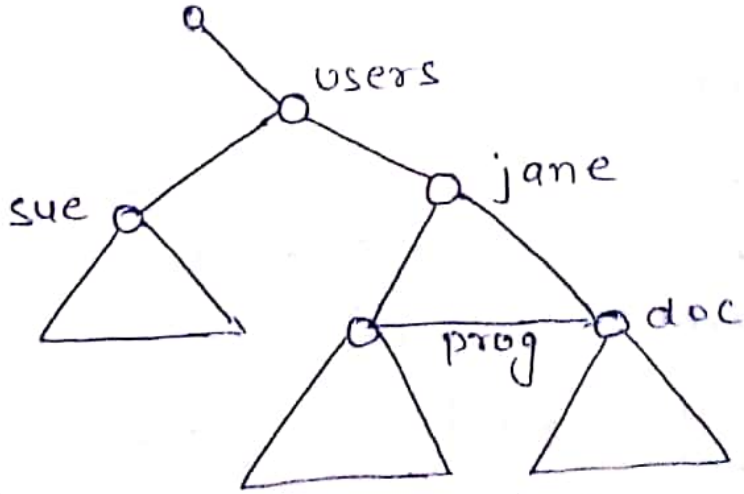
- A file system must be mounted before it can be accessed.
- A unmounted file system is mounted at a mount point :- the location within the file structure where the file system is to be attached.



(a) Existing system



(b) Unmounted volume.



Mount point.

File Sharing :

- Sharing of files on multi-user systems is desirable.
- Sharing may be done through a protection scheme.
- On distributed systems, files may be shared across a network.
- Network file System (NFS) is a common distributed file-sharing method.

Multiple Users :

- User IDs identify users, allowing permissions and protections to be per-user.
- Group IDs allow users to be in groups, permitting group access, right.

Remote File Systems :

- Uses networking a allow file system access between systems.
  - Manually via programs like FTP.
  - Automatically, seamlessly using distributed file systems.
  - Semi automatically via the world wide web.

- Client-Server model allows clients to mount remote file systems from servers :
  - Server can serve multiple clients.
  - Client and user-on-client identification is insecure or complicated.
  - NFS is standard UNIX client server file sharing protocol.
  - CIFS is standard Windows protocol.
  - Standard operating system file calls are translated into remote calls.
- Distributed Information Systems (distributed naming services) such as LDAP, DNS, NIS, Active Directory implement unified access to information needed for remote computing.

Failure Modes :

- Remote file systems add new failure modes, due to network failure, server failure.
- Recovery from failure can involve state information about status of each remote request.
- Stateless protocols such as NFS include all information in each request,

allowing easy recovery but less security.

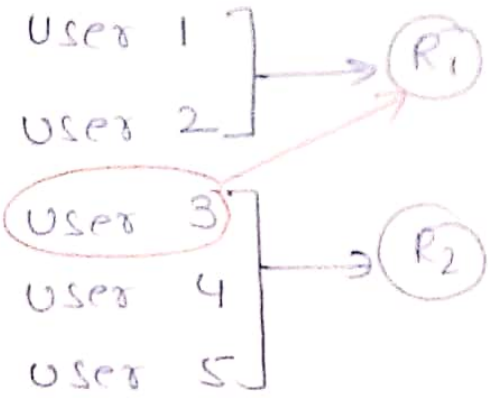
Consistency Semantics :
specify how multiple users are to access a shared file simultaneously.

- Process synchronization algorithms
  > Tend to be less complex due to disk I/O and network latency (for remote file systems)
- Andrew File System (AFS) implemented complex remote file sharing semantics.
- Unix file system (UFS) implements :
  > write to an open file visible immediately to other users of the same open file.
  > Sharing file pointer to allow multiple users to read and write concurrently.
- AFS has session semantics
  > writes only visible to sessions starting after the file is closed.

- Protection and security :
  are implemented to prevent interference with the use of files, both logical and physical.

- Threats may be of two types :
  (i) Internal
  (ii) External

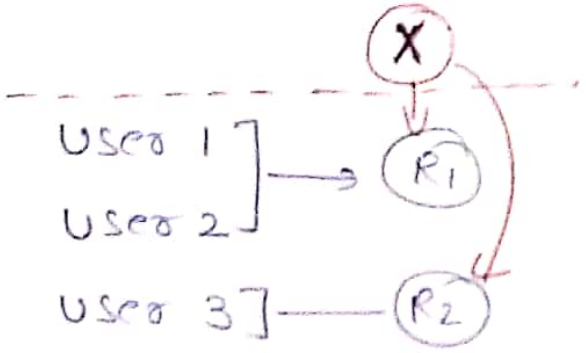
- There are five users and two files as resources.



User 3 tries to access resource R1. This is called as Internal threats.

- All Internal threats are handled by Protection.

- External Threats :



X is the external user and wants to access R_1 and R_2. This is known as External threats.

- External threats are handled by Security.

- Protection is providing mechanism for controlling the access to program, process, user to a resource, while Security is used to impart certain mechanism to prevent malicious user to enter into the system. for eg. Firewall, Encryption technique etc.

- Goals of Protection :

(i) Safe sharing of a common logical address space or common physical address space.

- Common logical address space means directory of files. It should be shared safely.

(FS.4)

- common physical address means memory.

(ii) Fair and Reliable Resource usage

Processes use the resources according to the policies.

- Protection Domain :

protection mechanism can be employed:

(i) User : A set of objects can be used on the identity of the user.

(ii) Process : Process id used as the identifier

(iii) Procedure : Set of objects can be accessed corresponds to the local variables defined within the procedure. So, Local variables are used to define the domain of the resource in this procedure.

- Access Matrix :

- It is used for the implementation of the protection model.
- In this matrix, Rows are used to represent domain. These can be different domains like user, process, and procedure.
- Columns are representing the objects. These objects are actually the resources.

Domain \ objects	File 1	File 2	File 3	Printer
D1	Read		Read	
D2				Print
D3			Execute	
D4		write		

Access Matrix

- Each Entry in the matrix consists of a set of access rights.
- The entry access (i, j) defines the set of operations that a process executing in Domain Di can invoke an object Oj. (FS-6)

- It must be ensured that a process executing in domain Di can access only those objects specified in row i.

Security

- Generally deals with external environment.
- Some of the misuse incidents are :
  (i) Theft of information.
  (ii) Unauthorized modification of data.
  (iii) Unauthorized destruction of data.

Security Levels :

(i) Physical : Site containing computer system must be physically secured. For example : Like bank; Security guards prevent to let any malicious user enter into the Bank premises.

(ii) Human : Authorization / Authentication mechanism should be employed. Therefore a normal user can be distinguished from intruder.

(iii) Network : Encryption techniques are used to avoid any malicious activity (Denial of service attack) on computer network while transmitting of messages.

(iv) Operating System : System must be protected itself by accidental security breaches. Security tools must be installed to protect system by itself.

— Authentication :

It is one of the major issues associated with the operating system.

(i) Password Based :

Simple password authentication offers an easy way of authenticating users. In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password, for each user.

Disadvantage :

An attacker can modify the document containing name and password for authentication.

Solution : hashing techniques

(ii) Artifact - Based :

This mechenism includes machine readable stips or magnetic strips.

- Smart cards.
- Debit cards.
- Credit cards.

] contains machine readable magnetic strips.

(iii) Biometrics Based :

- It is most secured technique.
- It uses two different characteristics of human.

(i) Physiological
fingerprints, retina and face.

(ii) Behavioural
Signature, voice.

Disadvantages :
- It is costly. It intrudes the privacy of users.

Threats.

(1) Program Threats :

When any program, created by a user is used by another use then misuse of the program may occur.

For example :

- Trojan Horses
- Stack / buffer overflow.

(2) System Threats :

In this O.S. files or resources are misused.

(a) WORMS : Replicated (duplicate) themselves.

- contains malicious code that cause major damage to O.S files.
- do not cause direct ~~messge~~ damage, instead consumes lot of system resources thus denying service to the user.

(b) VIRUSES : Small programs written to alter the way a computer operates.

- executes without user permission.
- can replicate itself.
- stages
  - (i) Dormancy : sitting ideally.
  - (ii) Propogation : gets attach to the host files.
  - (iii) Triggering : count no. of clicks & activated. to cause damage.
  - (iv) Damage : crashed.