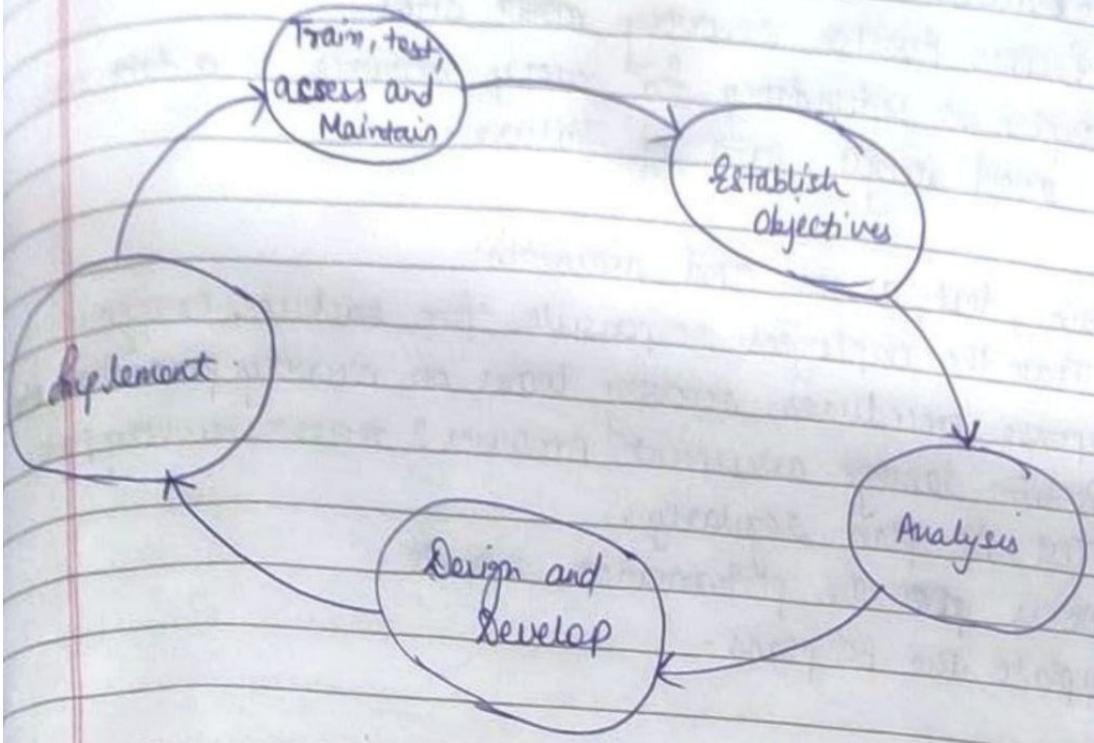
Business Continuity Planning life cycle:



① Establish objectives: ⓐ Determine Business Continuity Requirements.
ⓑ. Estimate the scope and budget to achieve requirements.
ⓒ. Select BC team.
ⓓ. Create ~~the policies~~ BC policies.

② Analysis: ⓐ. Collect information on data profiles, business processes, etc.
ⓑ. Conduct a Business Impact Analysis (BIA)
ⓒ Identify critical business processes & assign recovery priorities.
ⓓ. Perform risk analysis.
ⓔ. Perform cost benefit analysis
ⓕ. Evaluate options.

③ Design and develop: ⓐ. Define team structure and assign individual roles and responsibilities.
ⓑ. Design data protection strategies & develop infrastructure.
ⓒ. Develop contigency solutions, emergency response procedures
ⓓ. Detail recovery & restart procedures.

④. Implement: ⓐ Implement risk management and mitigation procedures.
ⓑ Prepare disaster recovery sites.
ⓒ Implement redundancy for every resource in a data center to avoid single points of failure.

⑤. Train, test, assess and maintain:
ⓐ. Train the employees responsible for backup, emergency response procedures, recovery team on recovery procedures, etc.
ⓑ. Perform damage assessment processes & review recovery plans.
ⓒ. Test BC plan regularly.
ⓓ. Assess the performance reports.
ⓔ. Update the BC plans.

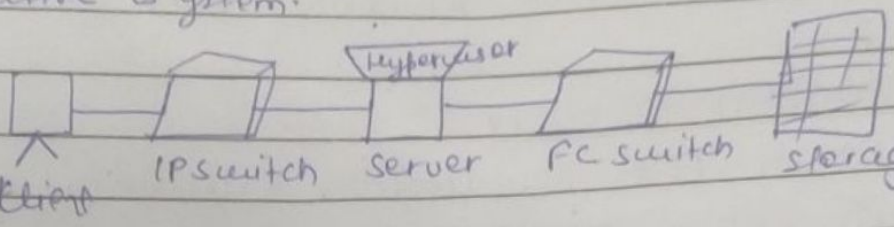
* Backup Purposes:
ⓐ. Backup is an additional copy of production data, created and retained for the sole purpose of recovering lost or corrupted data.
Backup Purpose:
→ Disaster Recovery
→ Operational Recovery
→ Archival.

Unit-3

* Failure Analysis :-

→ involves the analysing failure of physical and virtual components and implementing mechanisms to overcome the failure

→ Single Point of failure → failure of the component that can terminate the availaibality of the entire system.



For e.g, failure of hypervisor causes disruption of entire system.

* Resolving Single Points of Failure :-

→ System are designed with redundancy such that the system fails only if all the components in the redundancy grp fails.

→ This ensure that a failure of single component does not affect data availability.

→ Data centres follow guidelines to implement fault tolerance for interrupted information availability.

→ Analysis is performed to eliminate every single point of failure.

e.g. ① Configuration of redundant switches for switch failure

② Configuration of multiple storage arrays ports for a port failure.

* Back-up Purpose :-

(i) Disaster Recovery :-

→ The backup copies are stored at an alternate site, when the primary site is ~~disrupted~~ disrupted due to a disaster.

→ Later, the info. can be recalled for restoring at the Disaster Recovery site (DRS).

(ii) Operational Recovery :-

→ Data in the production environment changes with every business transaction & operation.

→ Backups are used to restore data, if data loss or corruption occurs during routine processing.

e.g., ~~it is common~~ deletion of email can be restored using backup-data

(iii) Archival :-

→ Content addressed storage (CAS) has emerged as the primary sol^n for archives, traditional backups are still in use for small and traditional enterprises.

* Backup consideration :-

→ Primary considerations → RPO, RTO

→ RPO :- determines backup frequency.

- Refers to the point-in-time at which the data must be recovered and the point-in-time ~~at~~ from which to restart business operation
- Specifies time interval bet^n two backups

For e.g., if RPO = 1 day, the day should be backuped once every day.

→ RTO :- determines the "backup media type" and determines data recovery time.

→ Location, size & no. of files should also be considered because they might affect the backup process.
→ Backing up large files takes less time as compared to equal amount of data divided into small files.
→ Data compression & Data duplication should also be considered

* Backup-Methods :-
→ Two methods → Hot backup (online backup)
→ cold backup (offline ")
→ Hot backup :- the application is up & running & the users can access data during the backup process.
→ cold backup :- it requires application to be shut down during the backup process
→ Hot backup is challenging because the data is actively used & changed.
→ If a file is open it is not normally backed-up during the backup process. In such situation an Open File Agent (OFA) to backup the file.
→ Consistent backups of databases can also be done by using a cold backup but a disadvantage associated with this is that the databases remains inactive.
→ Certain attributes & permissions attach to a file such as permission, owner also needs to be backed-up.

* Backup - Architecture :-

→ Uses client-server architecture with a backup server & multiple backup clients.

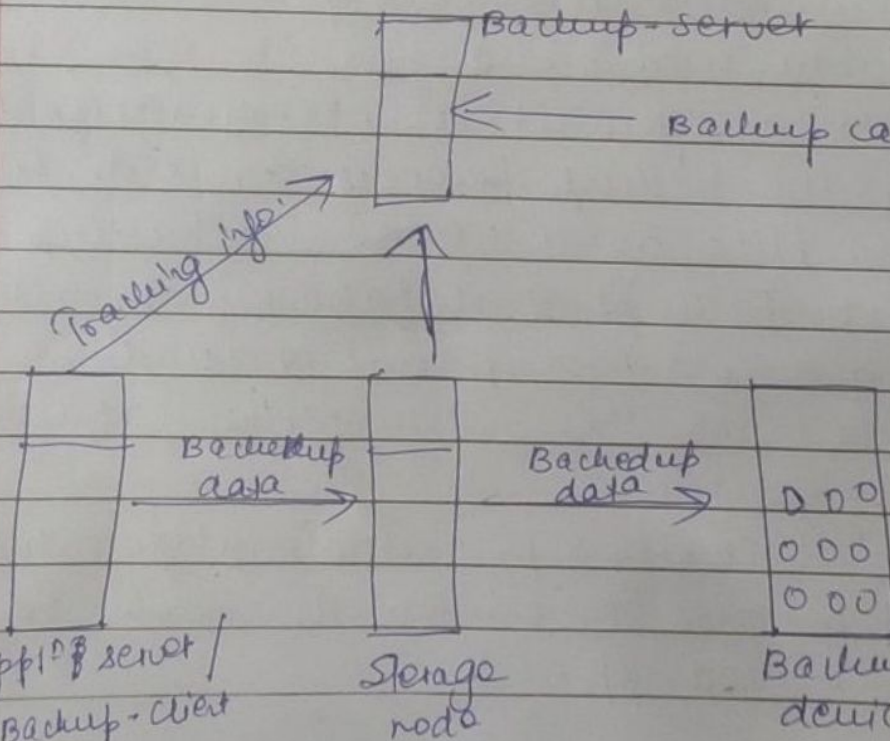
→ Backup server → manages backup operations which contains info. about the backup.

→ Backup configuration contains info about when to run backup.

→ Backup client → gathers the data to be backed up & sends it to storage node.
It also sends the tracking info. to the backup server.

→ Storage node → write the data to the backup device.
Backup-devices is attached directly attached to the storage node.

→ Backup S/w provides reports that include info. about the amount of data backed-up, no. of complete / incomplete backup and the errors that might have occured.

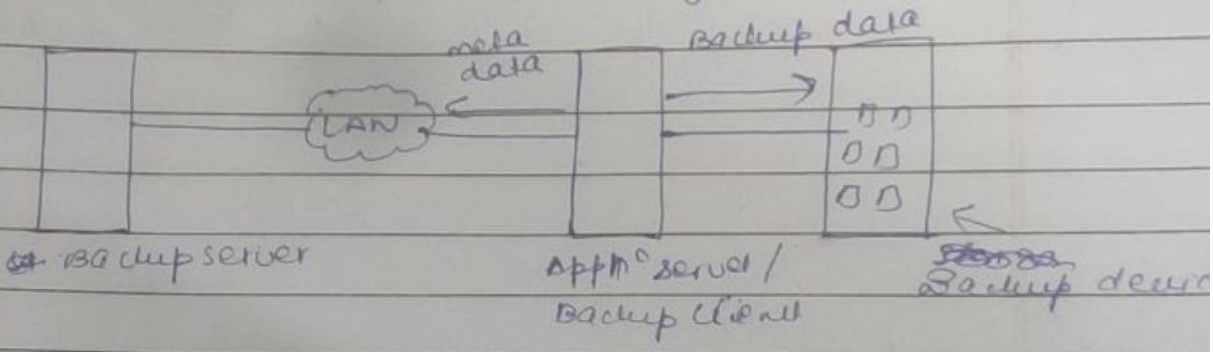


* Backup Topologies :-

(I) DAS → Direct Attached Backup
(II) LAN Based Backup
(III) SAN " "
(IV) Hired topology [LAN + SAN]

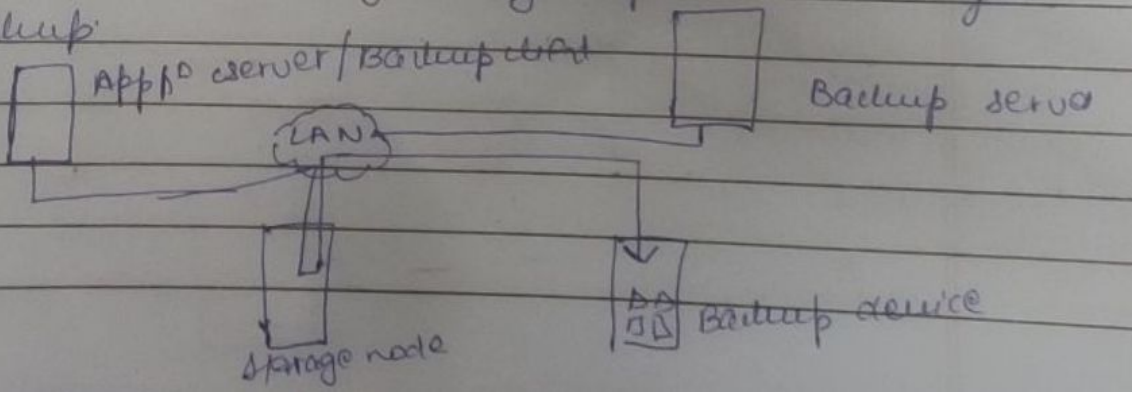
(1) DAS :-

→ Storage node is configured on backup client, backup device is attached directly to the client.
→ This configuration ~~[illegible]~~ frees the LAN from backup traffic, only the meta data is sent to the backup-server through the LAN.
→ Cost ↑ as the environment grows.



(2) LAN :-

→ Clients, backup server, storage nodes & Backup devices are connected to LAN.
→ The data to be backed-up is transferred from backup-client to the backup device over LAN which affects the n/w performance.
→ Can be minimized by using separate n/w for backup.



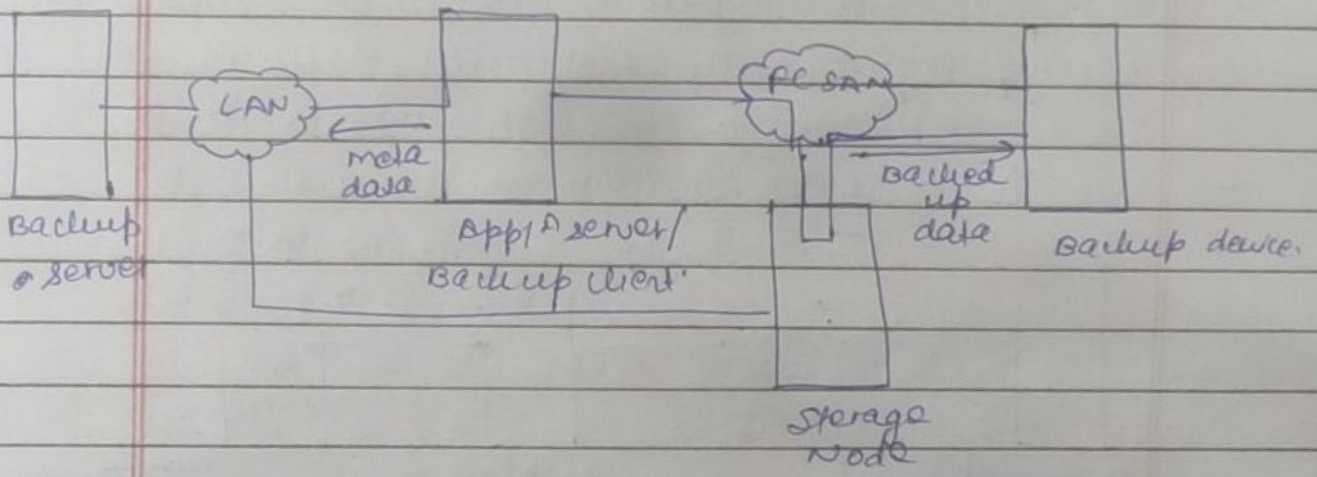
(3) SAN :- [also called LAN free backup]

→ appropriate when backup device needs to be shared among clients.

→ The backup device & clients are attached to SAN

→ The backup data traffic is restricted to SAN and only the backup meta data is transported over the LAN.

→ The LAN performance is not degraded in this configuration.

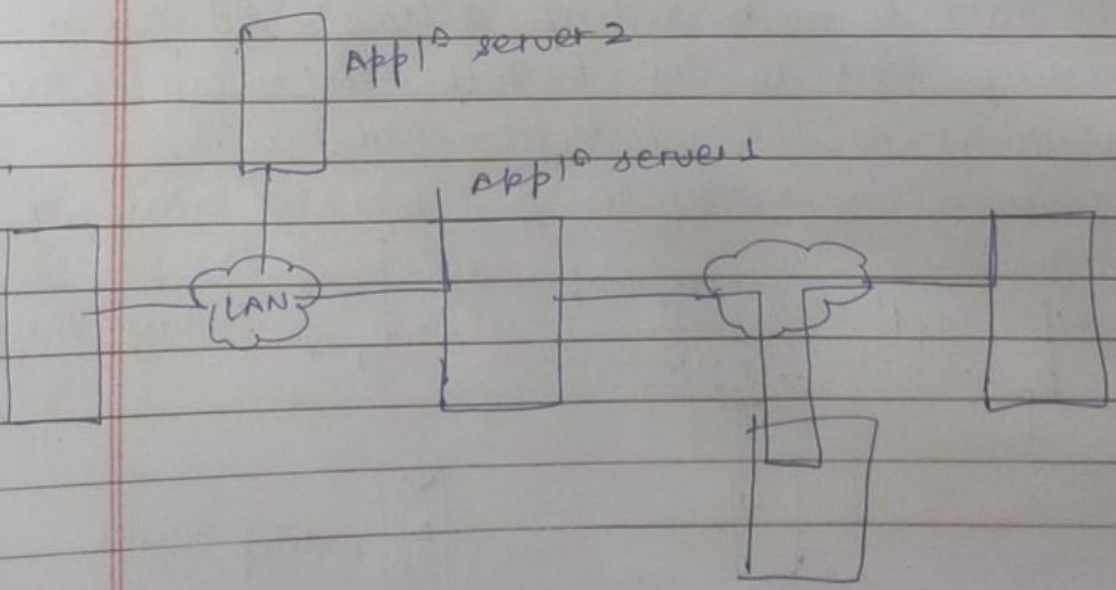


(4) Hired Topologies :-

→ LAN based + SAN based topologies.

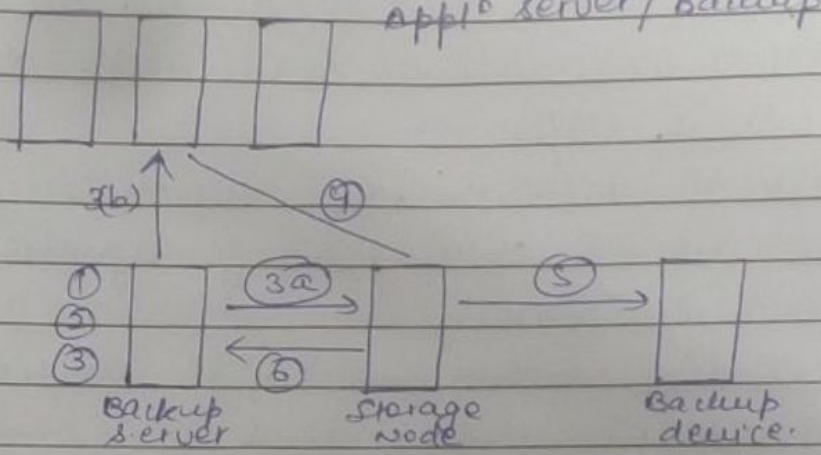
→ cost reduction

→ inferior performance.



* Backup and Restore operation :-

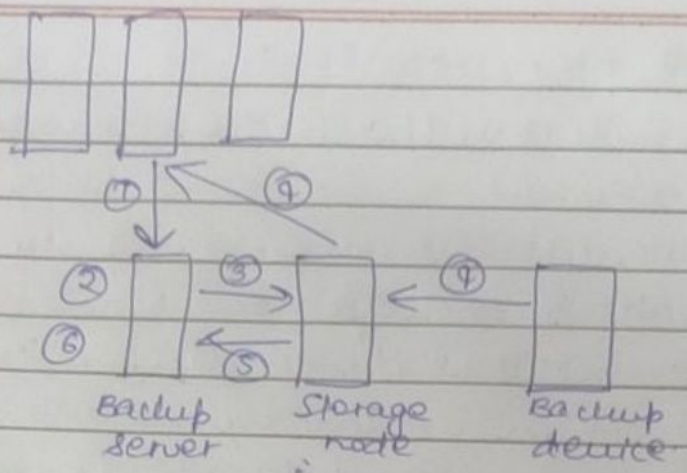
(1) Backup server initiates the backup process
(2) " " retrieves " " related info.
(3)(a) " " instructs the storage node to load the backup media in backup device.
(3)(b) Backup server instructs the backup client to send the data to be backed up to storage node
(4) Backup clients send the data to storage node and updates the info.
(5) Storage node sends the data to backup device
(6) " " " " meta data " " server.
(7) Backup server updates the info.



* Restore operation :-

(1) Backup client request the backup server for data restore
(2) Backup server identifies the data to be restored.
(3) " " instructs " storage node to load the backup media in backup device.
(4) Data is then read & sent to the backup client.
(5) the storage node send the ~~storage~~ restore meta data to the backup server.
(6) Backup server updates the info.

Appl^n server / Backup Client



* Backup Targets :-

→ Tape & disks are two most commonly used backed-up targets.

* Back-up to Tape :-

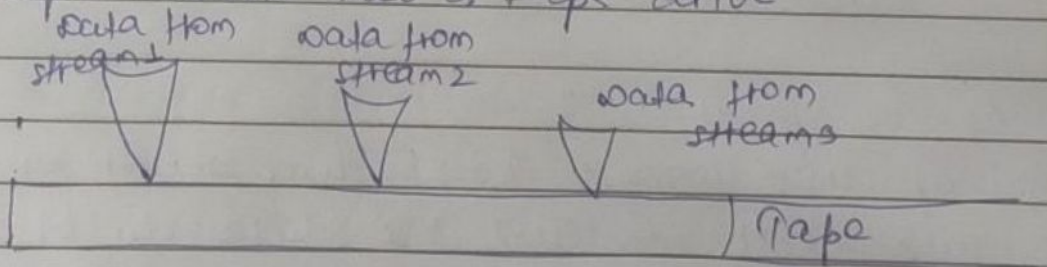
→ low cost solutions used extensively.

→ Tape drives are used to read/write data from/to a tape.

→ The data is written or read sequentially.

→ The tape cassette is composed of magnetic tape in plastic enclosure.

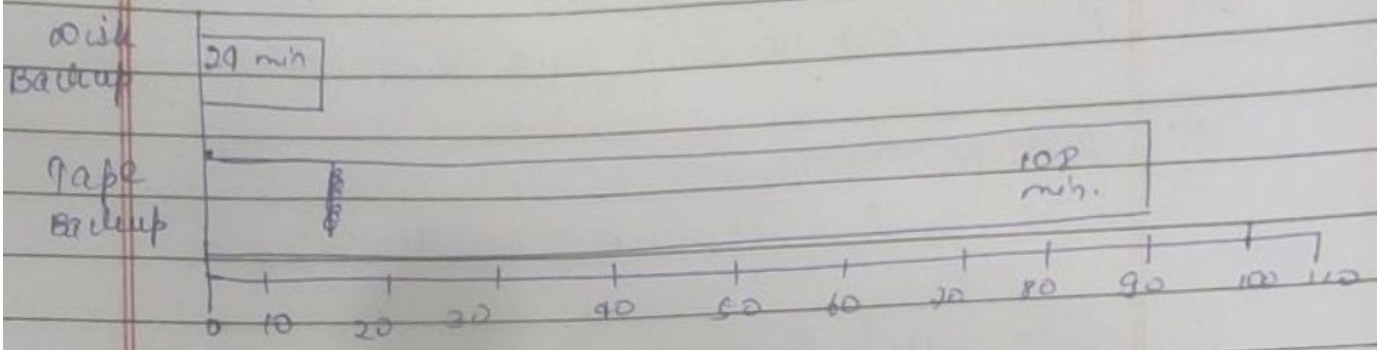
→ Tape mounting is the process of inserting a tape cassette into a tape drive



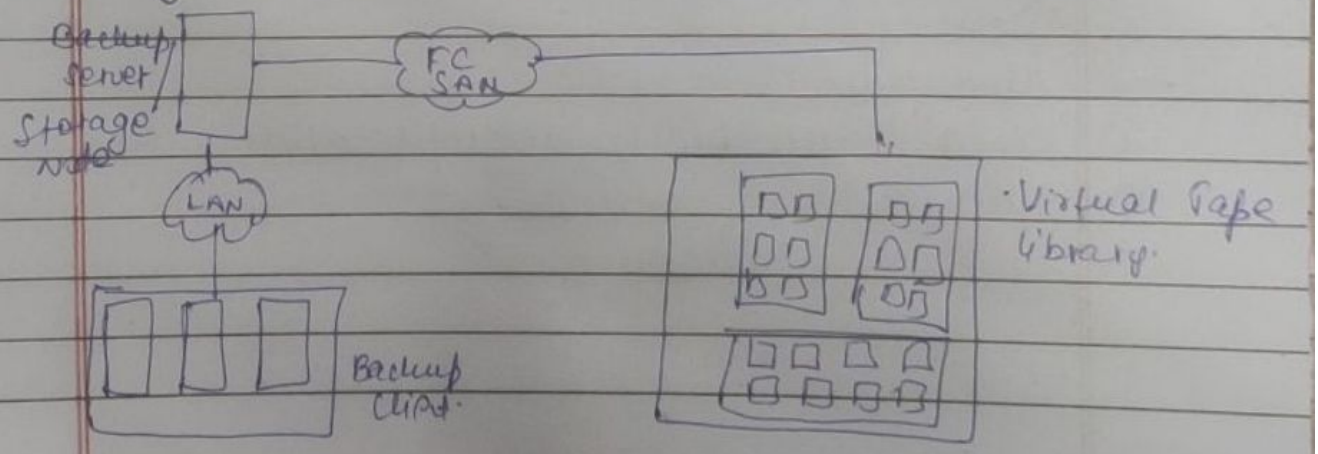
* Disadvantage :-

① slow backup & recovery operation due to sequential data access.

* Backup-to disk :-
→ Disks replaced tape because they are low cost.
→ Better performance
→ ease of implementation
→ ↑ quality of service.
→ RAID protection capabilities
→ Data is stored temporarily on disks before transferring them to tapes.



* Backup-to-Virtual Tape :-
→ same as Physical tape except for virtualization of majority of components
⊙ Virtual Tape Library :-
→ uses disk as backup media.
→ better reliability
→ Faster backup & recovery.
→ No maintaince.
→ Easy installation



* Data Deduplication for Backup :-
→ process of identifying & removing redundant data.
→ When a duplicate data is detected during backup & data is discarded and pointer is created to refer the copy of data that is already backed-up.
→ Helps to ↓ storage requirement for backup.
→ Removes n/w burden.
→ Retain data on disk for a longer time.

* Two methods :-
① File level ② Sub-file level.

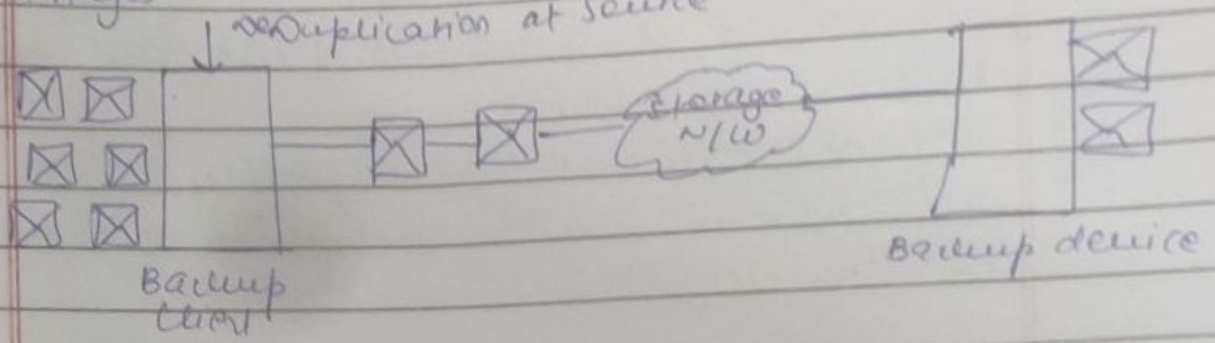
① File level :-
→ also called single instance storage
→ removes copies of identical files.
→ Simple & fast
→ does not address the problem of duplicate content inside the files.

② Sub-file level :-
→ breaks the file into smaller chunks then uses specialized algorithms to detect duplicate data.
→ Two forms :-
① Fixed length block deduplication
② Variable " " "

* Data Deduplication Implementation :-

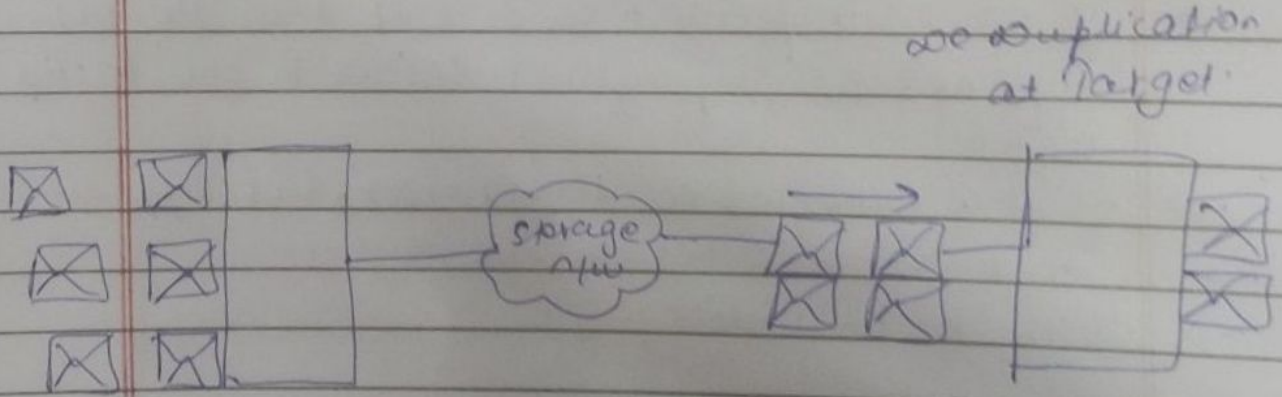
(I) Source Based :-

→ eliminates duplicate data at the source before transmitting it to the backup device.
→ ↓ amount of back-up data sent over the n/w.
→ requires less n/w bandwidth.
→ Reduction in capacity required to store backup images.



(II) Target Based :-

→ alternative to source based.
→ occurs at the backup device.
→ the data is deduplicated at the backup device either immediately or at a scheduled time.
→ Increased Bandwidth requirements.
→ doesn't requires any changes in the existing backup S/W.



(iii) Inline deduplication :-

→ performs deduplication on the backed up data before it is stored on backed up device

→ ↓ storage capacity needed for backup.

→ best suited for environment with large backup window.

(iv) Post Process deduplication :

→ enables the backed-up data to be stored on the backed-up device at first and then deduplicated later.

→ requires more storage capacity.

→ suitable for environment with lighter backup window.

* Backup in Virtualized environment :-

→ it is important to backup virtual machine data to prevent its loss due to human or technical error.

→ Two approaches :-

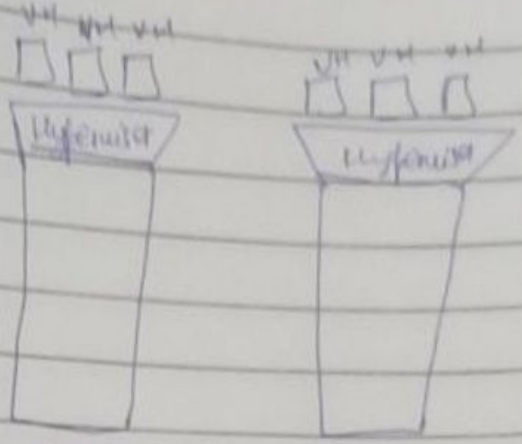
(1) Traditional Backup approach :-

→ Backup-agent is installed either on VMs or on the Hypervisor.

→ If the backup agent on a VM then the VM appears as a physical server to the backup agent.

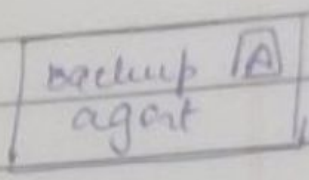
→ If it is installed on Hypervisor, VM appears as a set of files to the agent.

→ High CPU utilization.



Backup agent run on each VM

on hypervisor



(11) Image Based Backup Approach :-

→ operates at Hypervisor level.

→ the backup is saved as single file called as image.

→ this image is mounted on separate proxy server which act as a backup client.

→ the backup S/W then back-up thes image files normally.

→ enables quick restoration of VM.