ISM

Unit-2

FC [Fiber Channel] :-

Fiber channel architecture forms the fundamental of construct of the FC-SAN infrastructure. Fiber channel is a high speed network technology that runs on the high-speed optical fiber cable and serial copper wire.

It was developed to meet the demand for increased speed of data transfer between the server and mass storage systems. It is introduced by American National Standard Institute (ANSI) in 1988.

High speed data transmission is an important feature of FC network technology. The initial implimentation offered a throughput of 200 MB/s and the latest implementation of 16 GFC offers the throughput of 3200 MB/s.

FC architecture is highly scalable and theoritically a single FC network can accomodate ~~the~~ approximately 15 million devices.

SAN and its Evolution :-

SAN stands for Storage Area Network

It is a dedicated, specialized and high speed network which provides block level data storage. It delivers the shared tool of storage devices to more than one server.

The main aim of SAN is to transfer the data between the server and storage service. It also allows transfering between the storage systems.

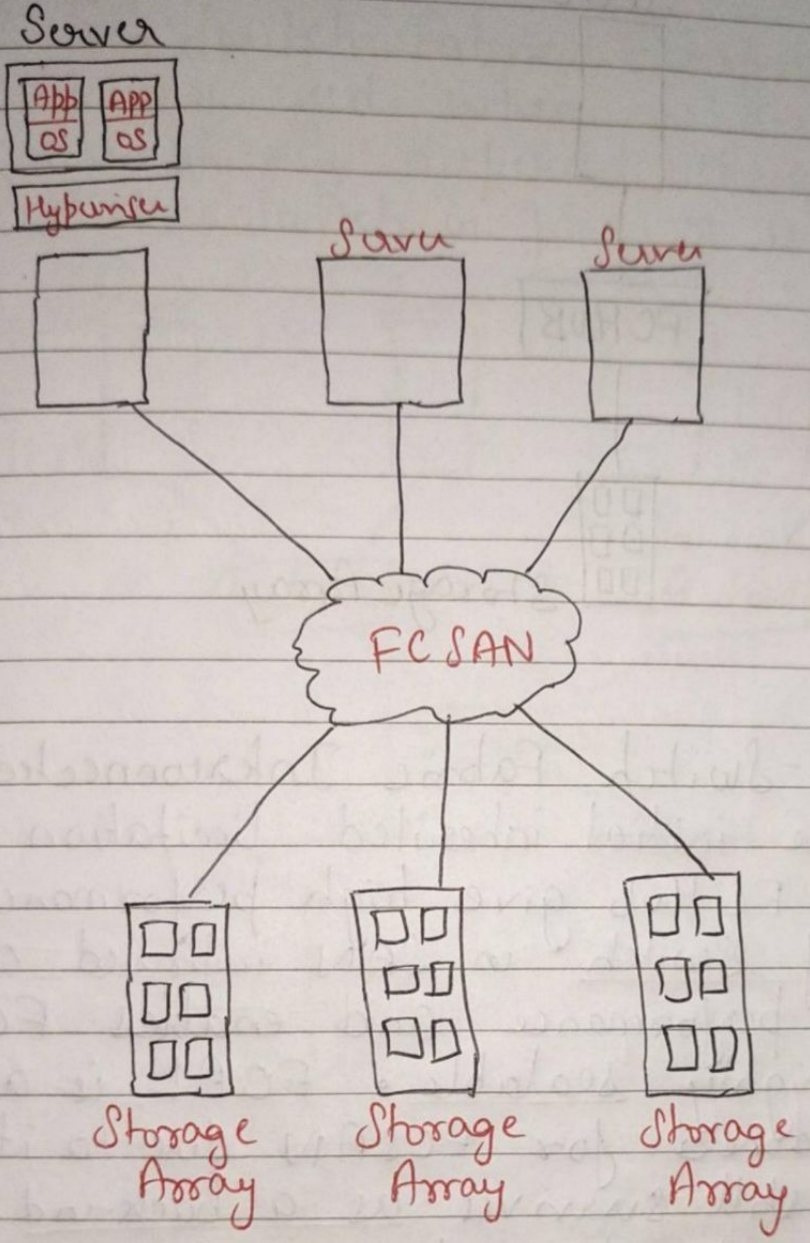
It is used for accessing storage devices such as tape libraries and disk devices from the server.

Common SAN deployments are Fiber Channel SAN (FCSAN) and IPSAN. Fiber Channel SAN uses Fiber Channel protocol for the transport, commands and ~~info~~ status information. IPSAN use IP based protocol for communication.

SAN also enables organization to connect geographically dispersed server storage.

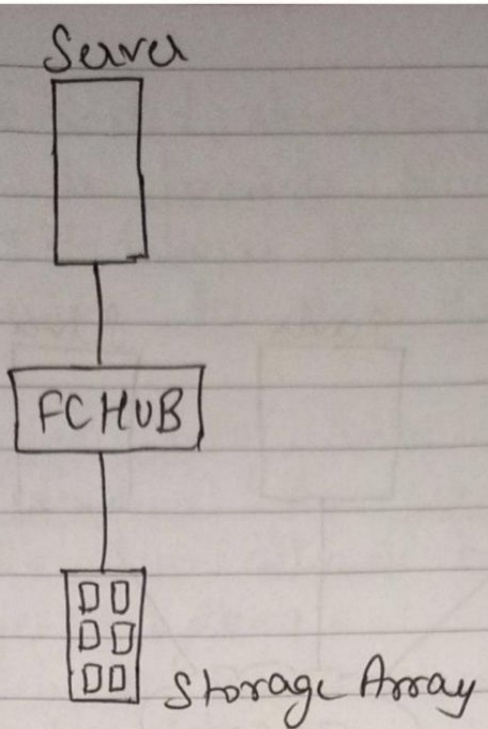
SAN Implementation :-

Given below is the diagram to demonstrate the implementation of SAN :-

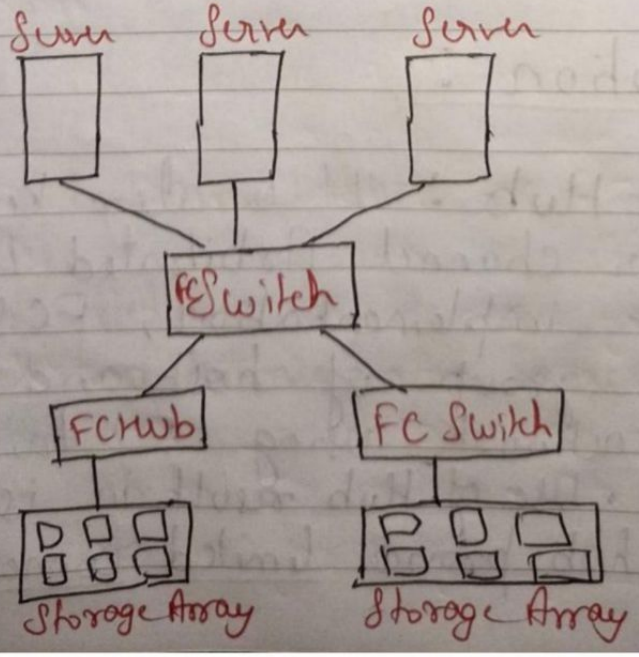


Evolution :-

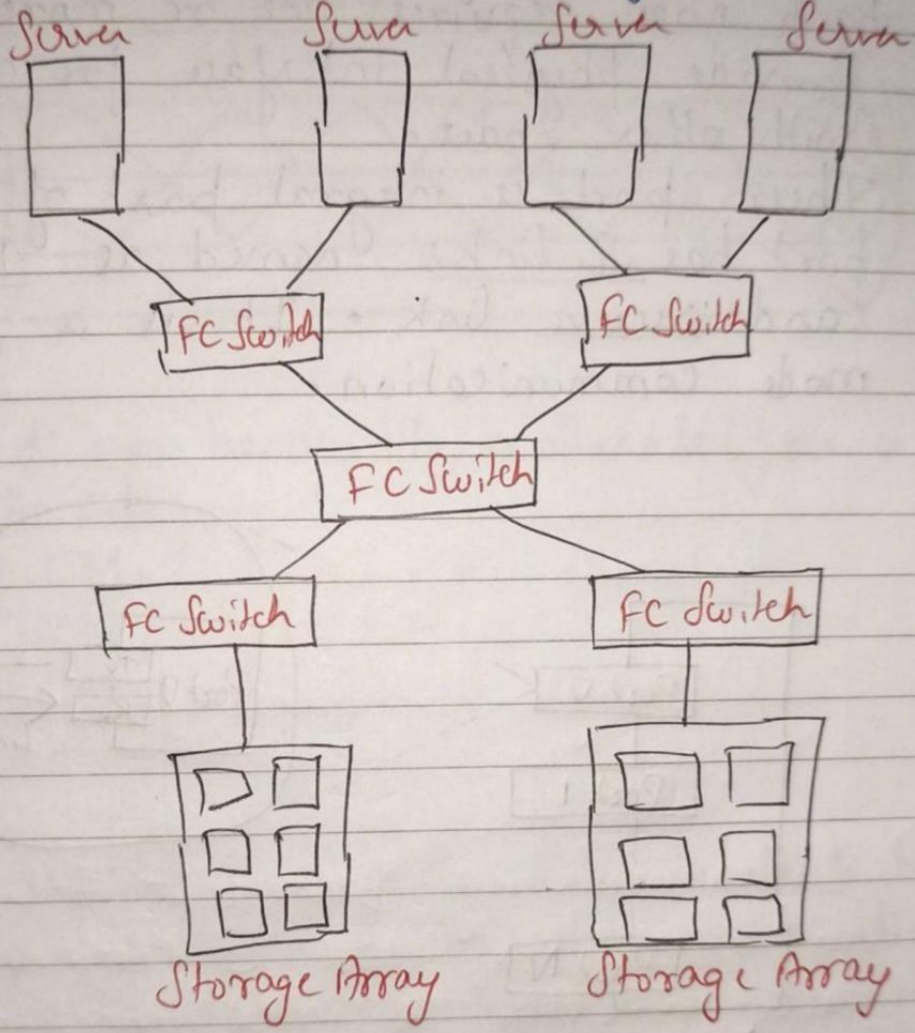
1) FC-Hub :- It is also known as FC-AL (Fiber channel Arbitrated Loop). In the earliest implementation, FCSAN was a simple group of host and storage devices to a network using FC hub as a connectivity device. Use of Hub result in isolated FC-AL because hub provide limited connectivity & bandwidth.



2) FC-Switch Fabric Interconnected SAN :-
The ~~initial~~ inherited limitation associated with FC Hub give high performance FC-Switch. Use of Switch in SAN improved connectivity and performance and enables FCSAN to be highly scalable. FCAL is almost abandoned for FCSAN due to it limitation but still survive as a back-end Connectivity option to disk drive.



3) FC-Switch Fabric Enterprise SAN :-
It is used when we need to connect geographically dispersed storage. In this we use switch in place of HUB.

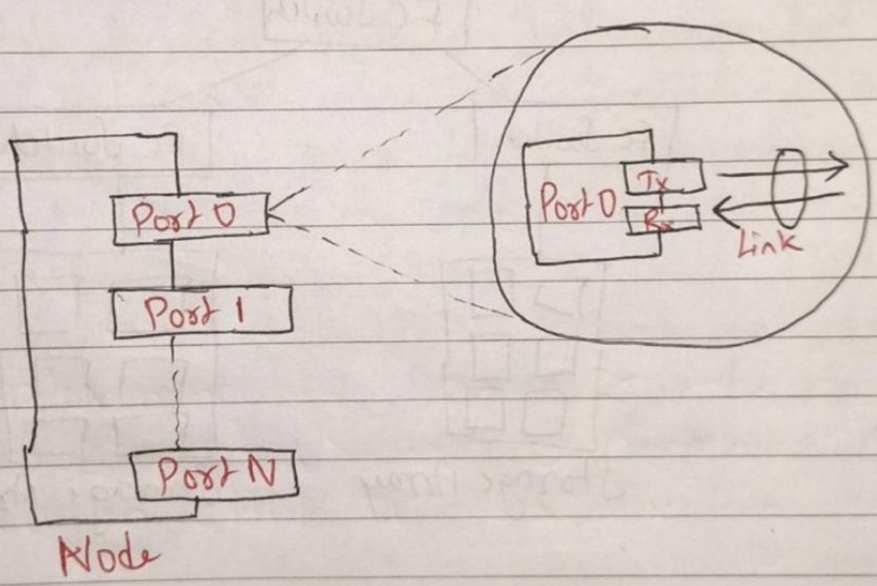


Component of FC-SAN :-

1) Node port
2) Cables and Connectors
3) Interconnecting devices
4) SAN management Software

1) Node Ports :-

In Fibre Channel network, the end devices such as host, storage Array and tape libraries are reffered to as node.
Each node requires one or more ports to provide physical interface for communicating with other nodes.
These port is integral part of HBA. Each port has 2 links named as Transmit link and receive link. It is a full-duplex mode communication.

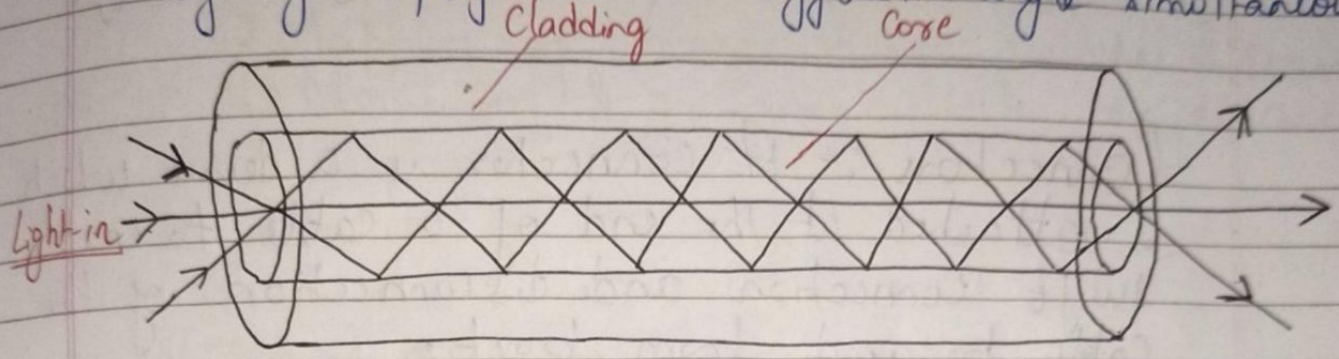


2) Cables and Connectors :-

SAN implementation use optical fiber cabling. Copper can be used for shorter distance for back-end connectivity because it provides an acceptable signal-to-noise ratio for distance up to 30 meters. Optical Cable carry data in form of light.

Type of Cable :-

i) Multimode fiber :- It carries multiple beam of light projected at different angle simultaneously.



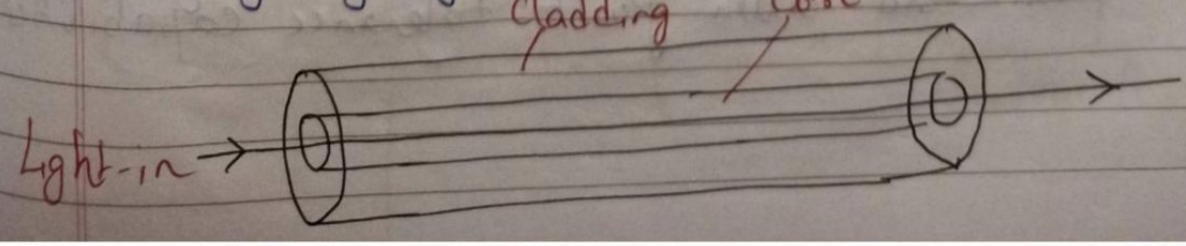
Based on bandwidth, multimode fiber is classified into 3 category :-

ⓐ OM_1 (62.5 μm)
ⓑ OM2 (50 μm)
ⓒ OM_3 (50 μm)
Laser optimized

Disadvantages :- In MMF, multiple beam traveling inside a cable tend to disperse and collide. This collision weaken the strength of the light after certain distance which is known as modal dispersion.

It is typically used for short distance.

ii) Single-mode Fiber (SMF) :- It carry a single ray of light projected at the center of the core.



SMF is used for long distance cable runs. It provide minimum attenuation over maximum distance (10 km). Diameter range of core = 7-11 microns (common 9 microns).

Connectors :- A connector is a device which is attached at the end of a cable to enable swift connection and disconnection of the cable to and from port.

Types :-

a) Standard Connector

b) Lucent Connector

c) Straight tip Connector

3) Interconnecting Devices :- FC hubs, Switch and directors are 3 common devices used in SAN as interconnecting devices.

HUB are used as a communication devices in FCAL. Switch are more intelligent than Hubs and directly route data from one physical port to another. Directors are high-end switches with high port count and better fault tolerance capabilities.

4) SAN Management Software :- It manages the interconnecting devices. It can manage all the resource from central location.

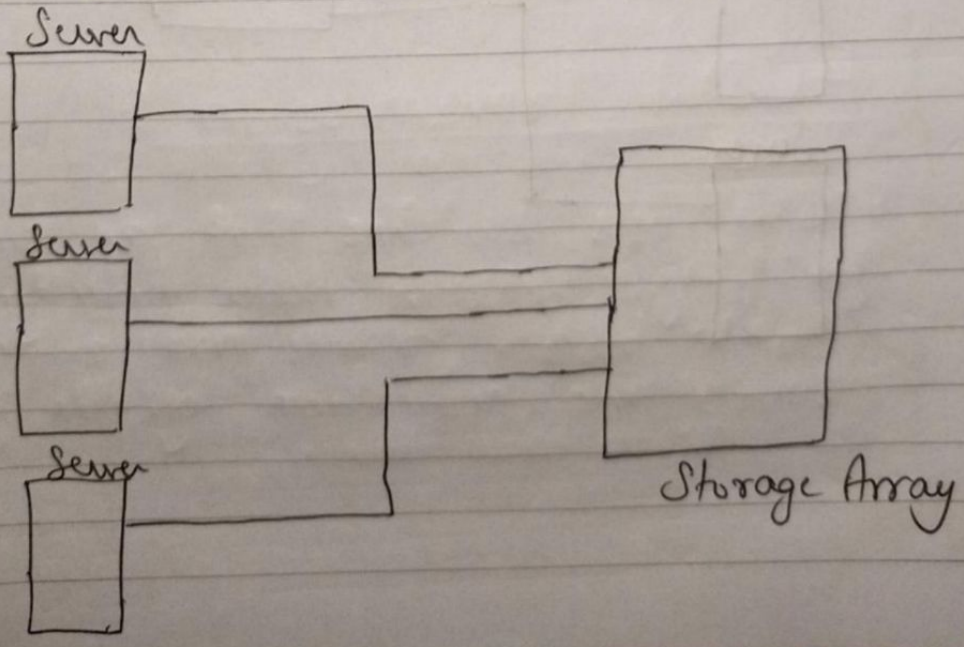
function :-

i) Mapping of storage devices, switches & servers.
ii) Monitoring & generating alerts for discovered devices.

FC Connectivity :-

1) Point-to-Point
2) Fiber Channel Arbitrated Loop
3) Fiber Channel Switched Fabric

1) Point-to-Point :- It is the simplest FC configuration in which two devices are directly connected to each other.



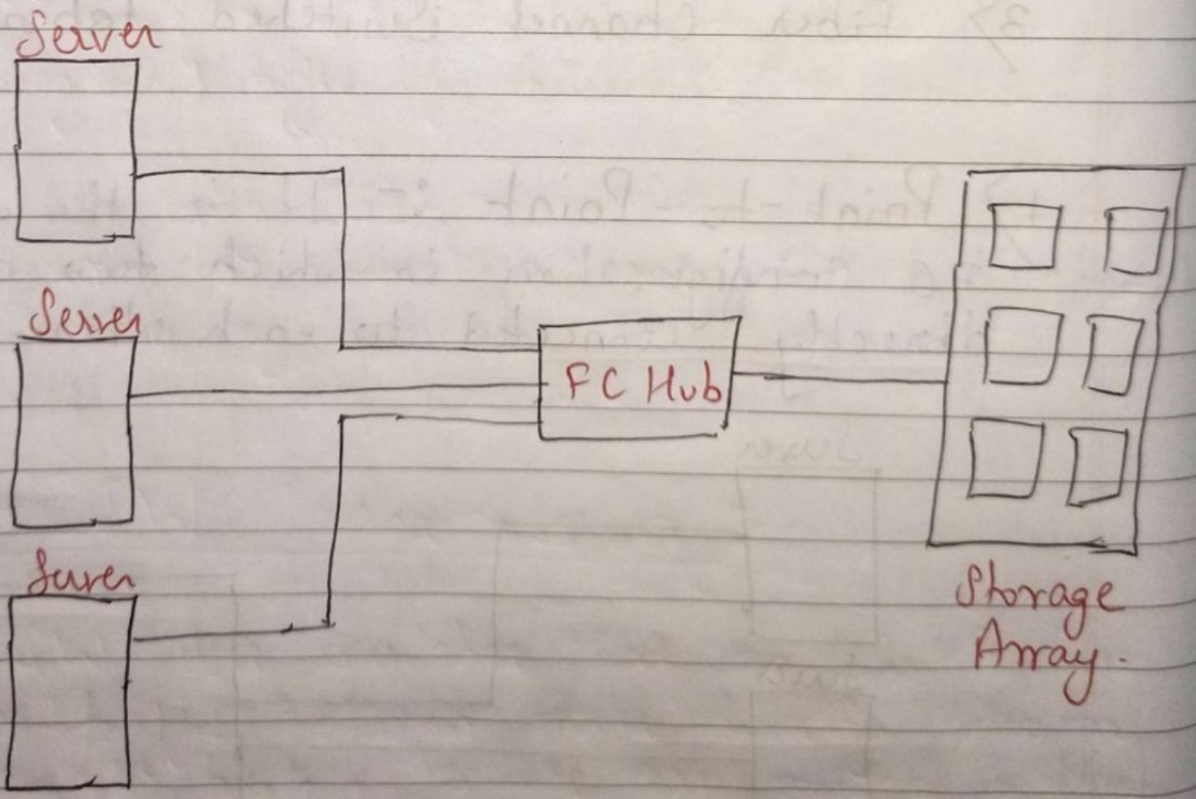
This connection provides dedicated connection for data transmission between nodes.

Limitations :-

(i) Difficult to scaled
(ii) Limited Connectivity.

2) Fiber Channel Arbitrated Loop :-

In FC-AL configuration, devices are attached to a shared loop. It has the characteristic of a token ring topology and a physical star topology.



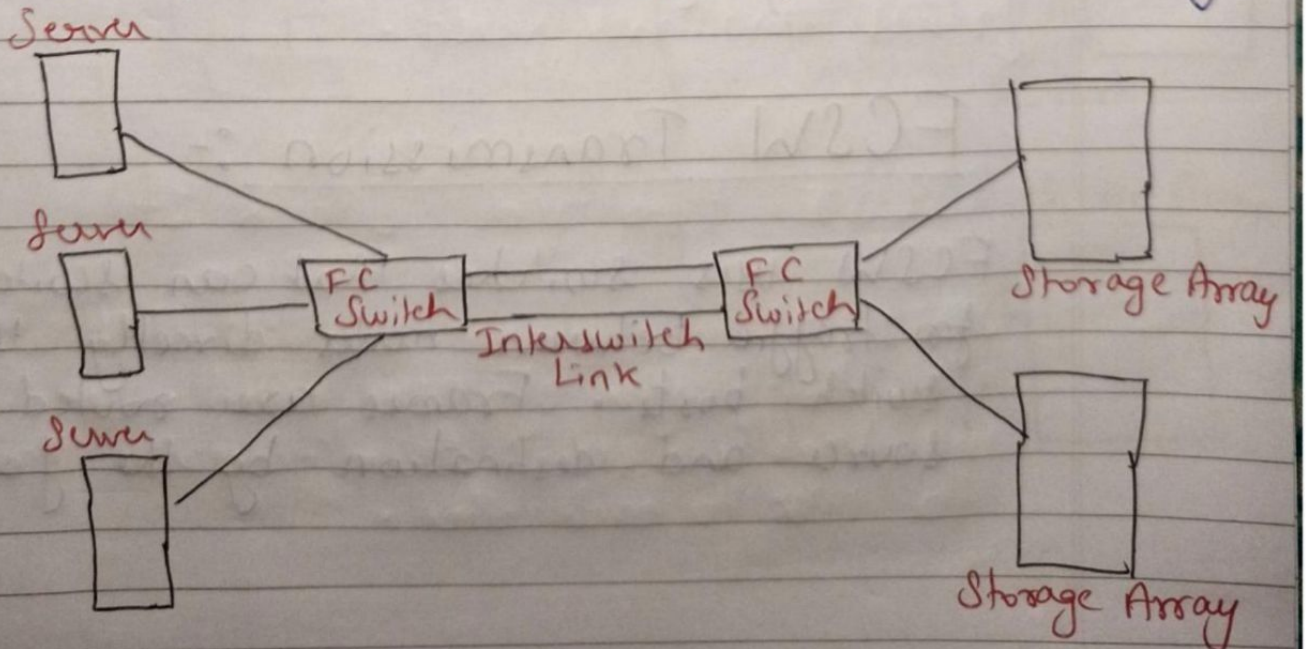
Drawback :-

1) It shares the loop and only one device can perform I/O operation at a time. Because each device in a loop must wait for it turn to proces an I/O request, the overall performance in FC-AL environment is low.

2) FCAL use only 8 bit of 24 bit Fiber channel addressing and enable 127 devices and since one addres is reserved so 126 node can be connected to loop.

3) Adding and removing a device result in loop re-initialization, which can cause a momentary pause in loop traffic.

3) Fiber channel Switched Fabric :- Unlike loop configuration, Fiber channel switched Fabric (FCSW) network provides dedicated data path and scalability.



The addition or removal of a device in a switched fabric is minimally disruptive, it does not affect the ongoing traffic between other devices.

FCSW is also refered to as fabric connect. A fabric is a logical space in which all node communicate with one another in a network.

Each node in fabric has a unique 24 bit fabric address for communication.

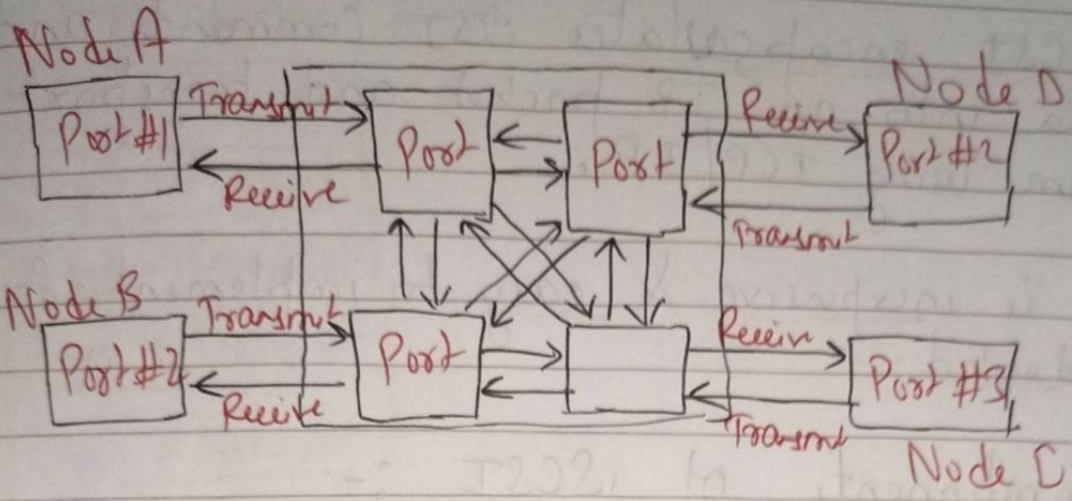
The link between two switches is known as InterSwitch Link (ISL).

ISL enable switch to be connected together to form a single larger fabric. ISL is used to transfer host-to-storage data and fabric management traffic from 1 switch to another.

By using ISL, a switched fabric can be expanded to connect a large number of node.

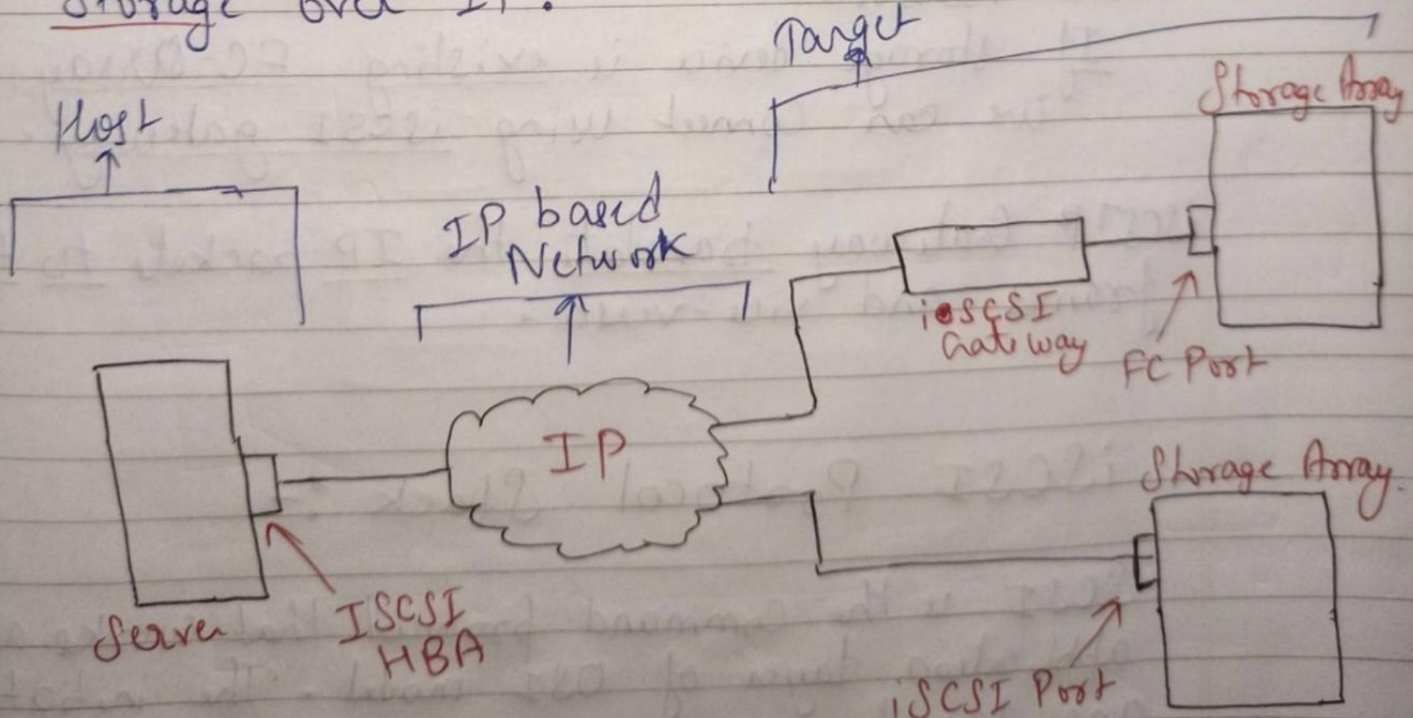
FCSW Transmission :-

FCSW uses switches that can switch data ~~for~~ traffic between nodes directly through switch ports. Frames are routed between source and destination by the fabric.



iSCSI (Internet SCSI) :-

iCSCI is an IP based protocol that established and manages the connection between host and Storage over IP.



* iSCSI encapsulates SCSI Commands and data into an IP packet and transport them using TCP/IP.

* It is inexpensive & easy to implement. So widely adopted.

* Components of iSCSI :-

(a) Initiator (host)
(b) Target
(c) IP based Network :

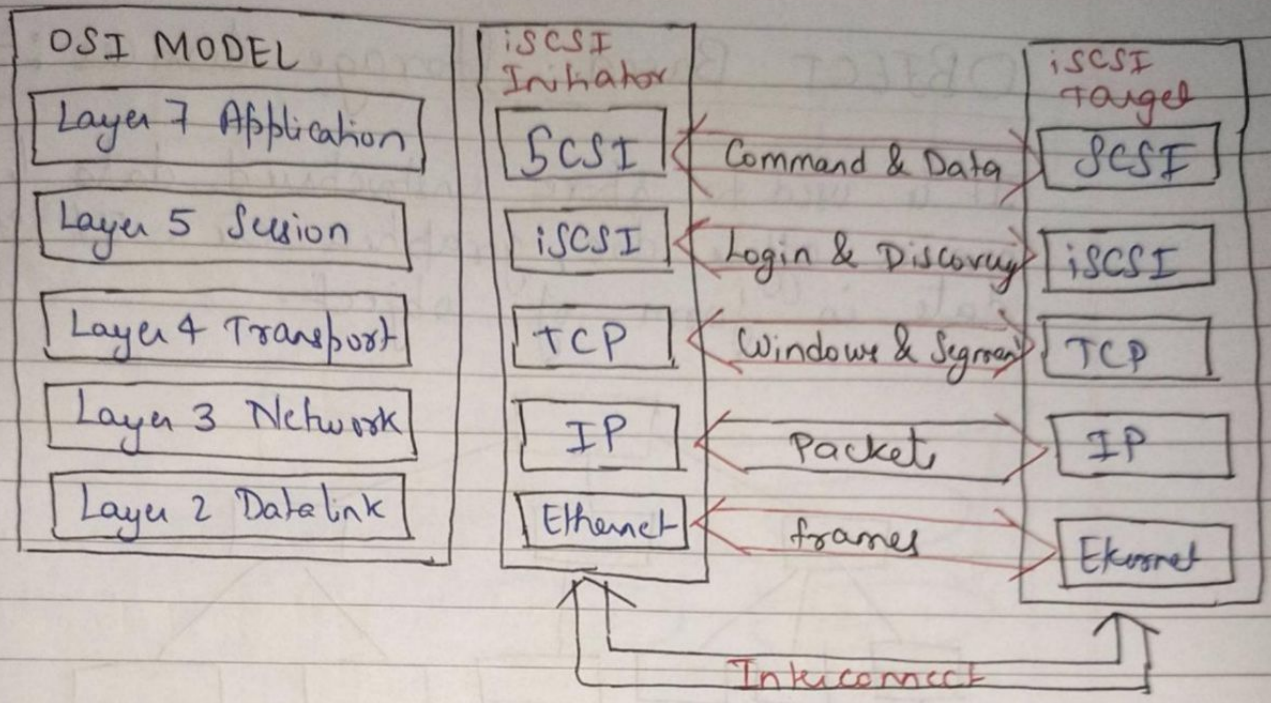
If storage device is iSCSI capable then we can directly connect storage device to IP network

If storage device is existing FC-Array, then we can connect using iSCSI gateway.

iSCSI Gateway translate the IP packets to FC frames and vice-versa.

iSCSI Protocol Stack :-

SCSI is the command protocol that works at application layer of OSI model. The initiator and targets use SCSI Commands and responses to talk to each other.



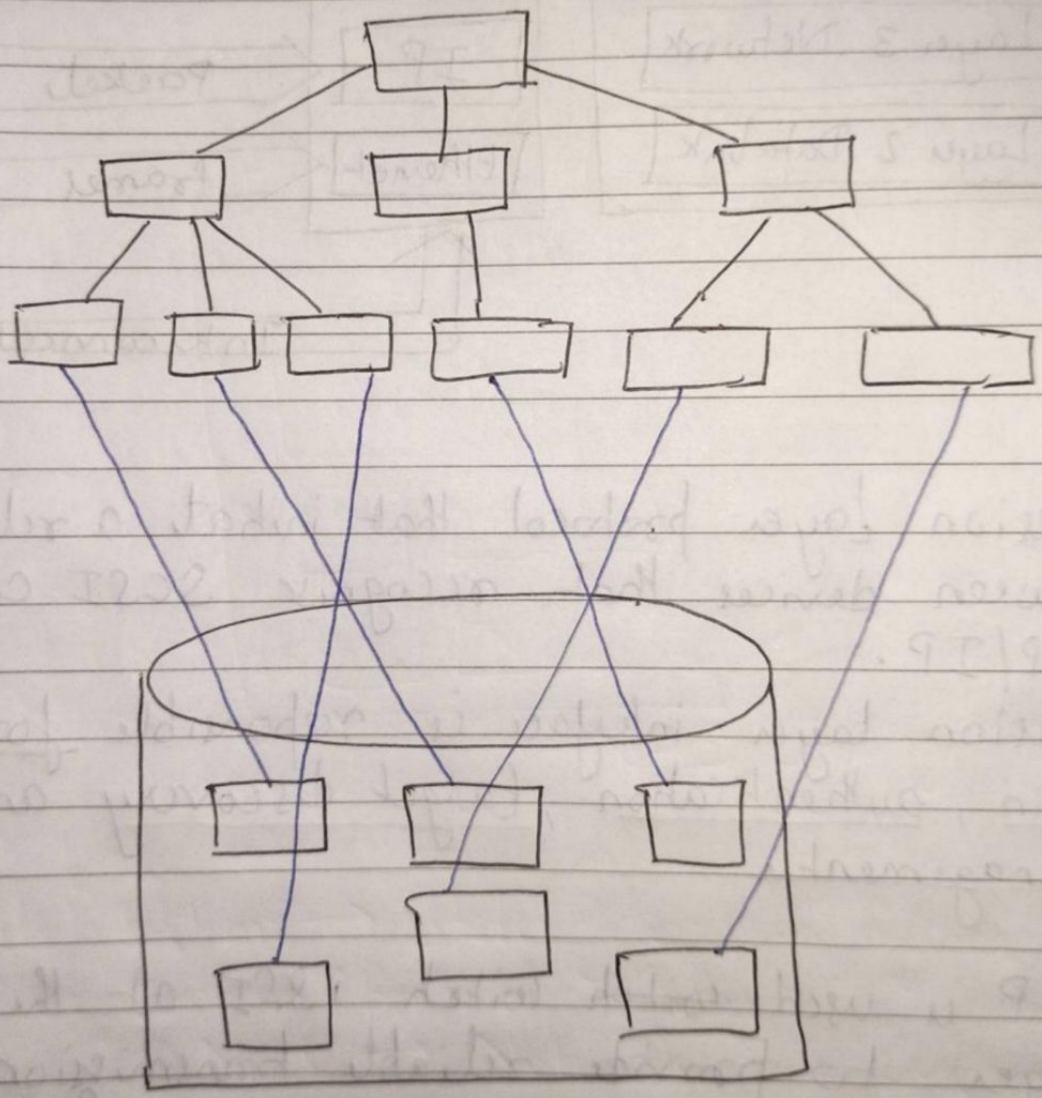
iSCSI is Session Layer protocol that initiate a reliable session between devices that recognise SCSI command & TCP/IP.
Session layer interface is responsible for handling login, authentication, target discovery and session management.

TCP is used ~~with~~ with iSSI at the transport layer to provide reliable transmission. TCP Control message flow, windowing & retransmission. TCP relies on the network layer to provide the global addressing and connectivity.

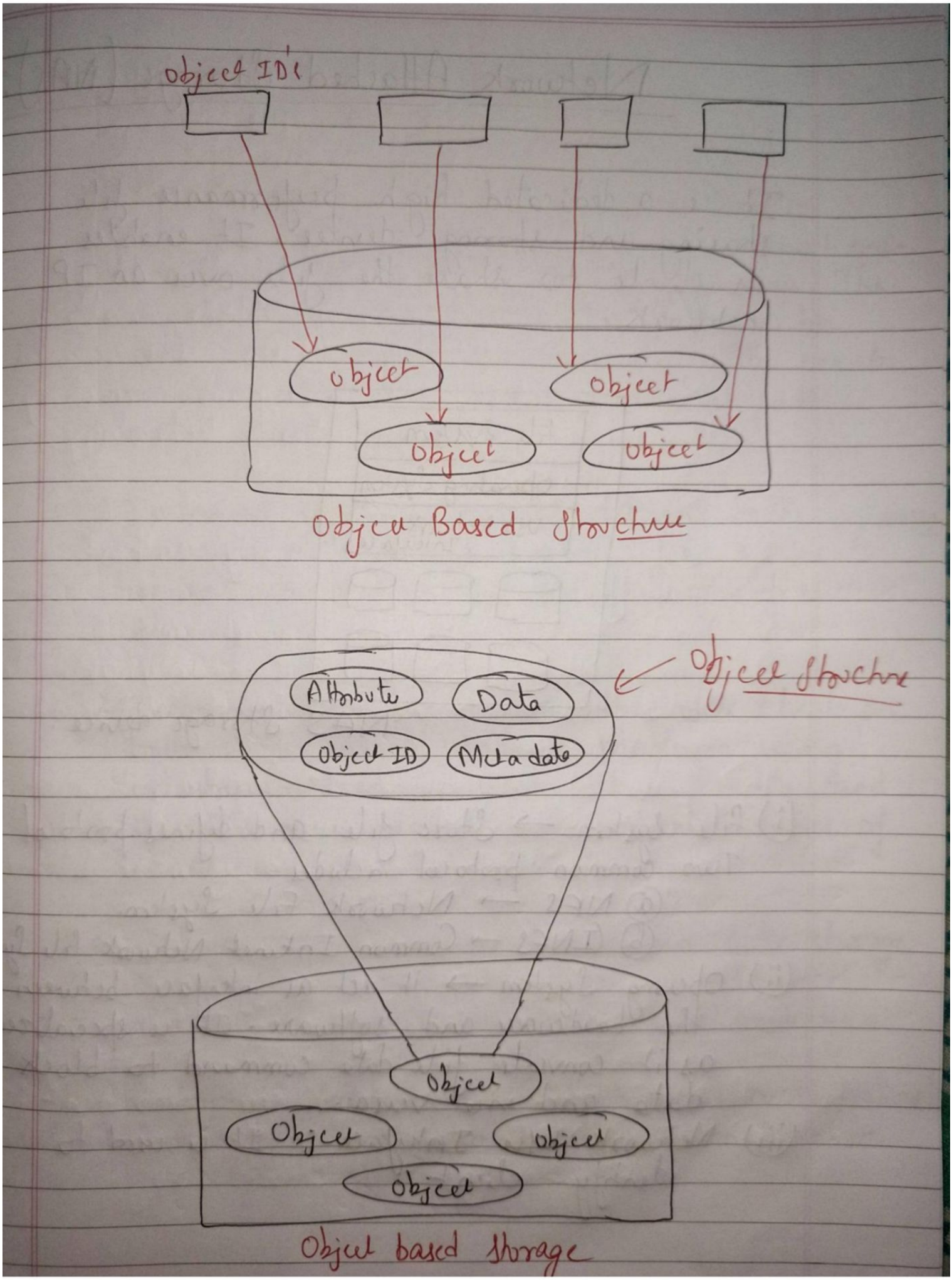
The layer 2 protocol at the data link layer of this model enable node-to-node communication through a physical network.

OBJECT Based Storage devices :-

It is used to store unstructured data like movies office doc, graphics etc. It store date in form of object.

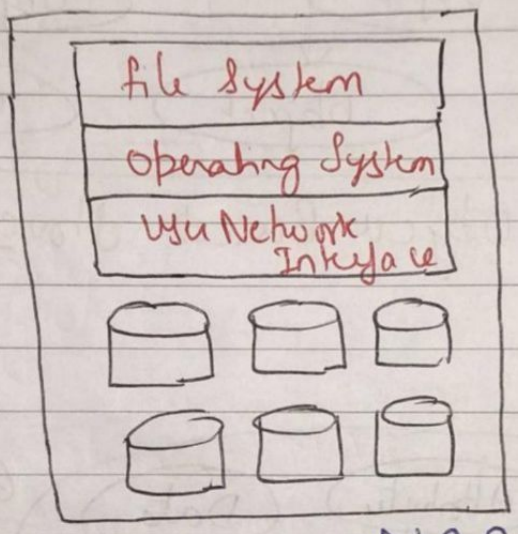


Hierichal file System.



Network Attached Storage (NAS):

It is a dedicated high performance file sharing and storing device. It enables its clients to share the file over an IP network.



NAS Storage device.

(i) file system → Store file and defines protocol
Two common protocol includes
(a) NFS → Network file System.
(b) CINFS → Common Internet Network file System

(ii) Operating System → it act as interface between the hardware and software. It is specialized as it converts file data command to block data and vice versa.

(iii) Network Nw Interface :- It is used to identify client

Benifits of NAS :-

1) Comprehensive access to Information :- Enables efficient file sharing and support one-to-many and many-to-one configuration. The many-to-one ~~enba~~ enables NAS device to serve many client simultaneously. The one-to many enables one client to connect with many NAS devices.

2) Improved efficiency :- NAS delivers better performance compared to a general purpose file system because it uses an OS specified for file sharing.

3) Improves Flexibility :- Compatible with client on both Linux and Windows platform using industry standard protocol. It is flexible and can serve request from different types of client.

4) Centralized Storage :- Centralized data storage to minimize data duplication on client workstation and ensure greater data protection

5) Simplified Management :- It provides a centralize Console that make it possible to manage file system efficiently.

6) Scalability :- Scales well with different utilization profiles and types of business application because of high performance and low latency design

7) High availability :- Offers efficient replication and recovery options, enabling high data availability. NAS uses redundant component that provides maximum connectivity options. It support clustering technology for failover.

8) Security :- Ensure security, authentication and file locking

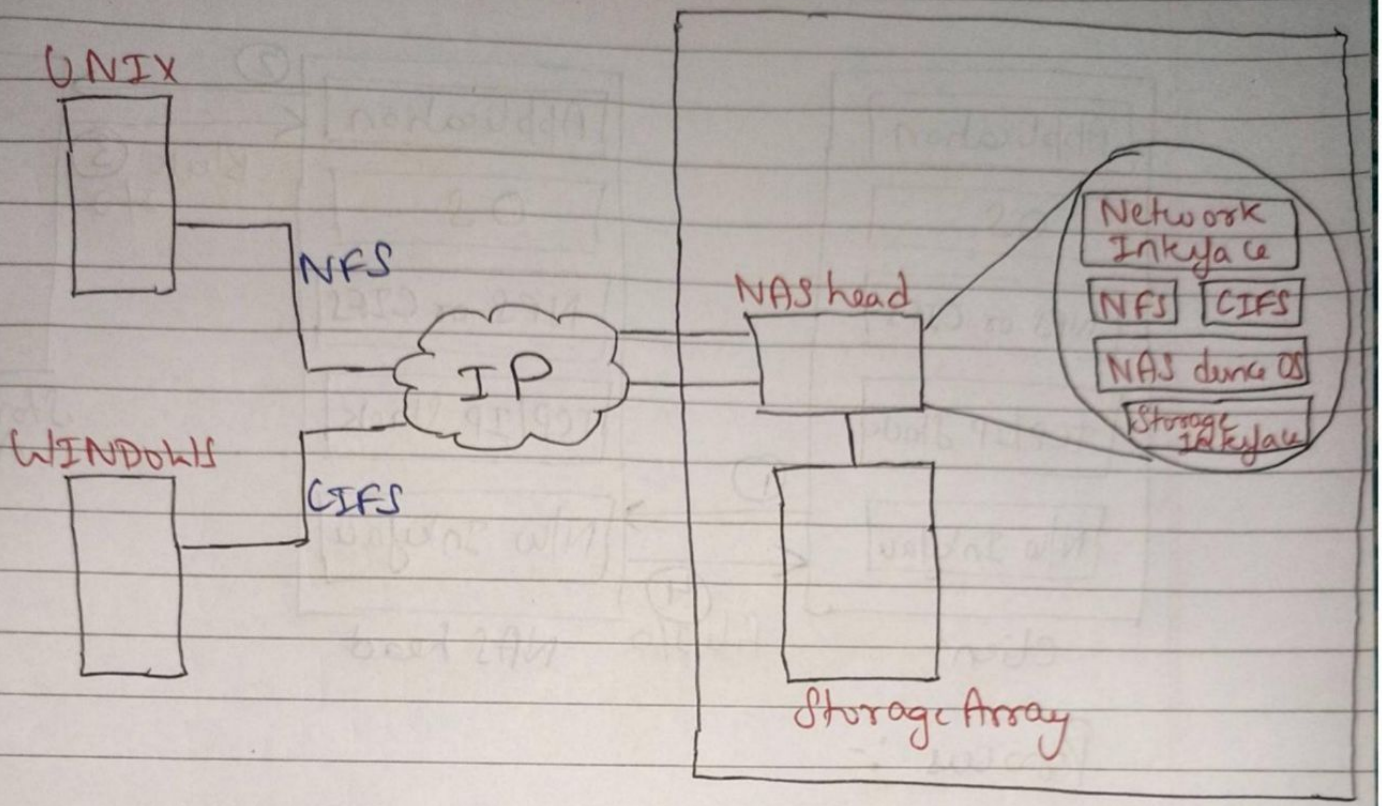
9) Low Costing :- NAS is commonly available and has inexpensive Ethernet component.

10) Ease of deployment :- Configuration at client is minimal, because the client have required NAS connection software built-in.

Components of NAS :-

A NAS device has two key component :-

(a) NAS head
(b) Storage.

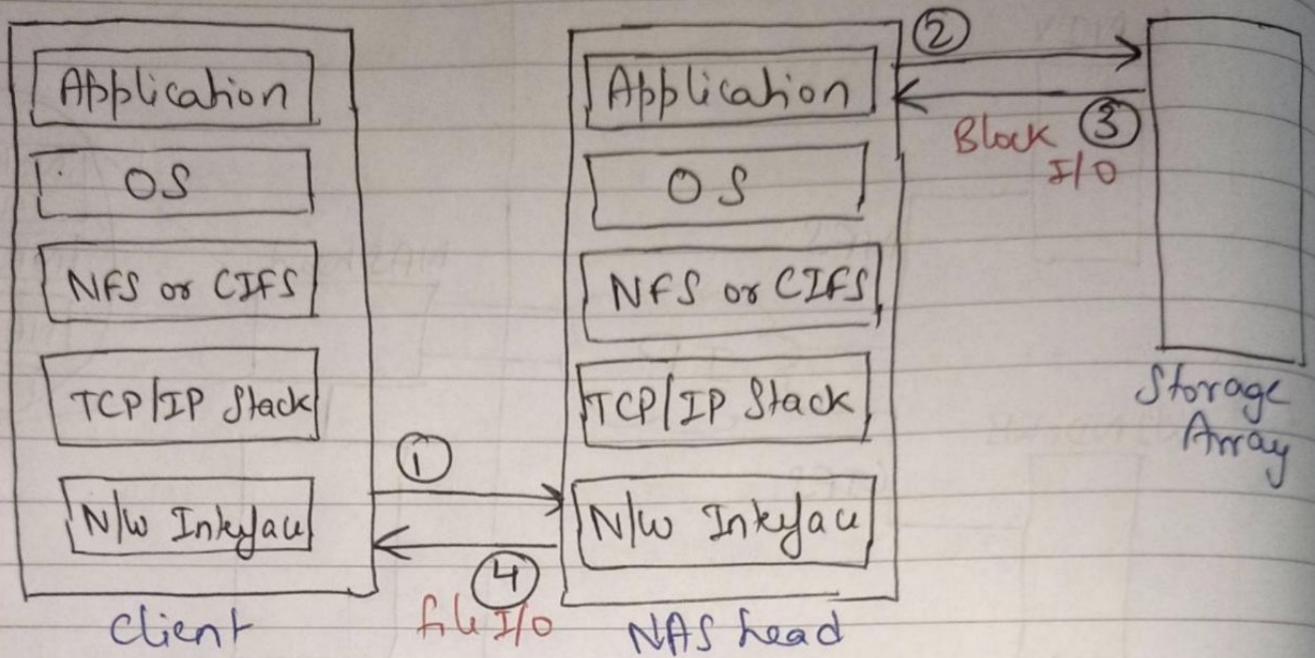


NAS head :- NAS head includes following :-

* CPU and memory
* Network Interface which provide Connectivity to client Network and also identify client
* NFS, CIFS are protocol for file sharing
* NAS device OS is used to convert file-level request to block-level request and vice-versa.
* Storage Interface to connect and manage physical disk resource.

NAS Input / Output Operation :-

NAS provide file level data access to it client. File I/O is a high-level request that specify the file to be accessed.



Process :-

1) Client package an I/O request and forward it to network stack through TCP/IP. The NAS device receives the request from the network.

2) The NAS device Converts the I/O request into appropiate storage request i.e block level I/O then peforms operation on physical storage.

3) When NAS receives data from storage it process repackaging the data into appropiat file ~~sha~~ protocol response

4) NAS device package this response into TCP/IP and forward it to client through Network

- NAS Implementations: ① Unified NAS Implementations
② Gateway Implementation
③ Scale out NAS Implementation.

① Unified NAS Implementation: → Consolidates NAS-based and SAN-based data access within a unified storage platform.
→ Performs file sharing and storing of file data.
→ Provides access to block level data.
→ Supports both CIFS & NFS protocols.
→ Contains one/more NAS heads and storage is a single system.
→ NAS heads are connected to storage controllers (SCs) which provide access to storage.

② Gateway Implementation: → NAS devices use external storage to store and retrieve data. This external storage is independently managed
→ More scalable compared to Unified NAS b/c NAS heads and storage arrays can be independently scaled up when required.

③ Scale Out NAS Implementation: → Pools multiple nodes together in a cluster
→ A node may consist of either NAS head or storage or both.
→ Provides the capability to scale out resources by simply adding nodes to a clustered NAS architecture.
→ Suitable to solve "Big Data" challenges.
→ Cluster works as a single NAS device and is managed centrally.
→ Nodes can be added to the cluster when more performance / capacity is needed, without causing any downtime.
→ ease of use, low-cost and unlimited scalability.
→ All info. is shared among nodes, so the entire file system is accessible by clients connecting to any node in the cluster.

* NAS file sharing Protocols: ① NFS
② CIFS.

→ NFS: ① Client server protocol for file sharing
② Commonly used on UNIX systems.
③ Originally based on connectionless UDP.
④ Uses a machine independent model to represent user-data.
⑤ Also uses Remote Procedure Call (RPC) as a method of Inter-process Communication b/w 2 computers.
⑥ Operations include: Searching, Opening, Reading, writing, Changing file attributes, modifying file links & directories.
⑦ Creates a connection b/w client & Remote system for data transfer.
⑧ Stateless (NFS V3 & earlier). Does not maintain any kind of table to store information about open files.
⑨ Currently 3 versions are in use.
→ NFS version 2: ① Uses UDP to provide stateless N/W connection.
→ NFS version 3: Uses UDP or TCP. Based on stateless protocol design.
→ NFS version 4: Uses TCP. Based on stateful protocol design. It offers enhanced security.

→ CIFS: ① Client-server application protocol that enables client programs to make requests for files & services on remote computers over TCP/IP.
② Enables remote clients to gain access to files on a server.
③ File names in CIFS are encoded using Unicode characters.
④ Enables file sharing by using special locks.
⑤ It uses file & record locking to prevent users from overwriting work of another user on a file or record.
⑥ Supports fault tolerance. It can automatically restore connections reopen files that were open prior to an interruption.
⑦ Stateful protocol.
⑧ User disruption is minimized.
⑨ Client receives a disconnection notification on server/NW failure.