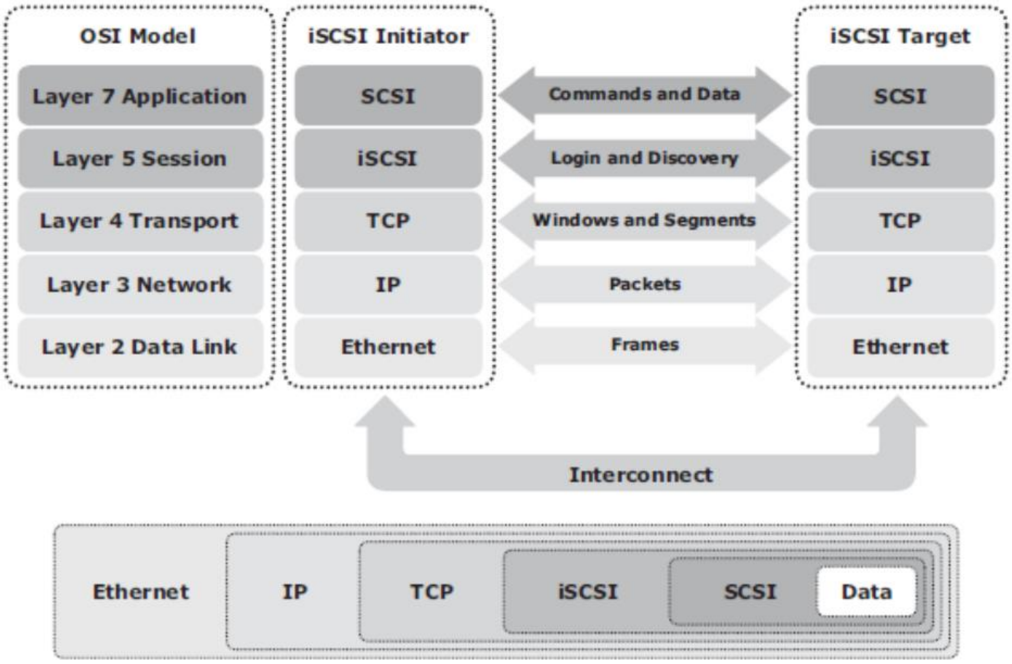
MODULE 3 QB -PP

1) Explain iSCSI Protocol Stack with neat diagram.

Ans)



- SCSI is the command protocol that works at the application layer of the Open System Interconnection (OSI) model.
- The initiators and targets use SCSI commands and responses to talk to each other.
- The SCSI command descriptor blocks, data and status messages are encapsulated into TCP/IP.
- It is then transmitted across the network between the initiators and targets.
- iSCSI is the session-layer protocol that initiates a reliable session between devices that recognize SCSI commands and TCP/IP.
- The iSCSI session-layer interface is responsible for handling login, authentication, target discovery and session management.
- TCP is used with iSCSI at the transport layer to provide reliable transmission.
- TCP controls message flow, windowing, error recovery and retransmission.
- It relies upon the network layer of the OSI model to provide global addressing and connectivity.
- The Layer 2 protocols at the data link layer of this model enable node-to-node communication through a physical network.

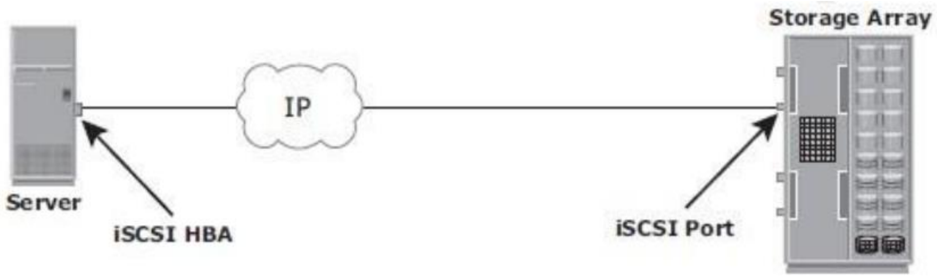
2) Explain iSCSI topologies.

Ans) Two topologies of iSCSI implementations are:

1) Native
2) Bridged

1) Native:

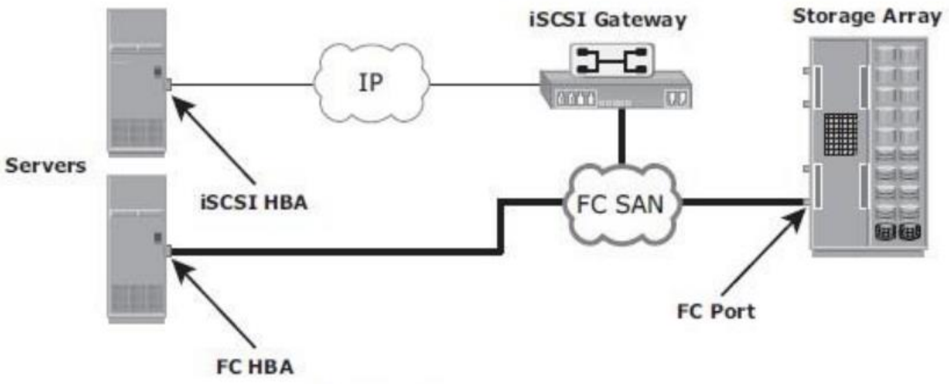
- Native topology does not have FC components.
- FC components are not required for iSCSI connectivity if an iSCSI-enabled array is used.
- The array has one or more iSCSI ports configured with an IP address and is connected to a standard Ethernet switch.
- After an initiator is logged on to the network, it can access the available LUNs on the storage array.
- A single array port can service multiple hosts or initiators as long as the array port can handle the amount of storage traffic generated by those hosts.



(a) Native iSCSI Connectivity

2) Bridged:

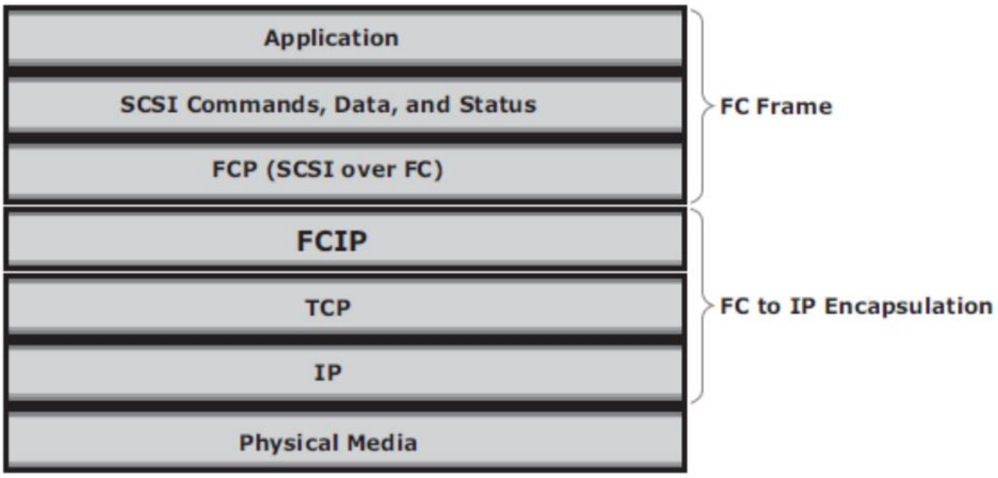
- A bridged iSCSI implementation includes FC components in its configuration.
- In this case, the array does not have any iSCSI ports.
- Therefore, an external device, called a gateway or a multiprotocol router must be used.
- This external device will facilitate the communication between the iSCSI host and FC storage.
- The gateway converts IP packets to FC frames and vice versa.
- The bridge devices contain both FC and Ethernet ports to facilitate the communication between the FC and IP environments.
- Here, the iSCSI initiator, with the gateway’s IP address, is configured as its target destination.
- On the other side, the gateway is configured as an FC initiator to the storage array.



(b) Bridged iSCSI Connectivity

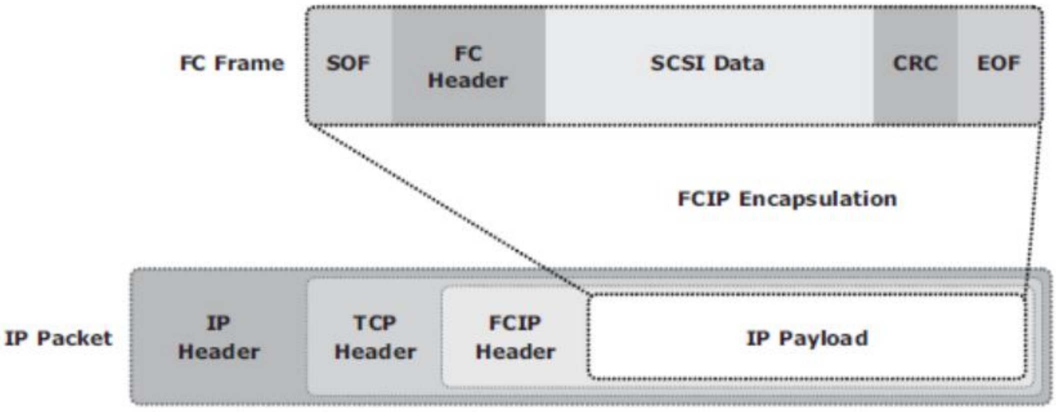
3) Explain FCIP Protocol Stack with a neat diagram.

Ans)



FCIP protocol stack

- Applications generate SCSI commands and data, which are processed by various layers of the protocol stack.
- The upper layer protocol SCSI includes the SCSI driver program that executes the read and write commands.
- Below the SCSI layer is the Fibre Channel Protocol (FCP) layer, which is simply a Fibre Channel frame whose payload is SCSI.
- The FCP layer rides on top of the Fibre Channel transport layer.
- This enables the FC frames to run natively within a SAN fabric environment.



FCIP encapsulation

- Encapsulation of FC frame into an IP packet could cause the IP packet to be fragmented.
- This happens when the data link cannot support the maximum transmission unit (MTU) size of an IP packet.
- When an IP packet is fragmented, the required parts of the header must be copied by all fragments.
- When a TCP packet is segmented, normal TCP operations are responsible for receiving and re-sequencing the data before passing it on to the FC processing portion of the device.

4) List and explain the benefits of NAS.

Ans)

1) **C**omprehensive access to information

2) **I**mproved efficiency

3) **I**mproved flexibility

4) **C**entralized storage

5) **S**implified management

6) **S**calability

7) **H**igh availability

8) **S**ecurity

9) **L**ow cost

10) **E**ase of deployment

(SLICE CHISS)

1) Comprehensive access to information:

- Enables efficient file sharing and supports many-to-one and one-to-many configurations.
- The many-to-one configuration enables a NAS device to serve many clients simultaneously.
- The one-to-many configuration enables one client to connect with many NAS devices simultaneously.

2) Improved efficiency:

NAS delivers better performance compared to a general-purpose file server because NAS uses an operating system specialized for file serving.

3) Improved flexibility:

- Compatible with clients on both UNIX and Windows platforms using industry-standard protocols.
- NAS is flexible and can serve requests from different types of clients from the same source.

4) Centralized storage:

Centralizes data storage to minimize data duplication on client workstations and ensure greater data protection.

5) Simplified management:

Provides a centralized console that makes it possible to manage file systems efficiently.

6) Scalability:

Scales well with different utilization profiles and types of business applications because of the high performance and low latency design.

7) High availability:

- Offers efficient replication and recovery options, enabling high data availability.
- NAS uses redundant components that provide maximum connectivity options.
- A NAS device supports clustering technology for failover.

8) Security:

Ensures security, user authentication and file locking with industry-standard security schemas.

9) Low cost:

NAS uses commonly available and inexpensive Ethernet components.

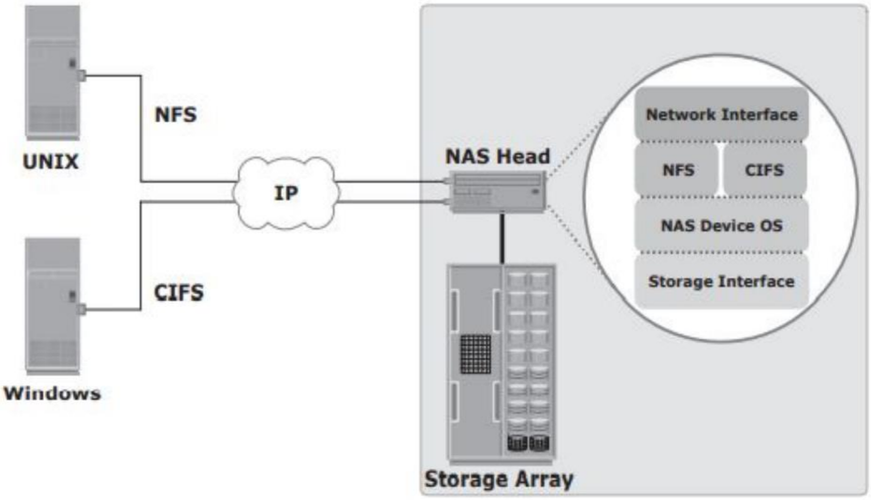
10) Ease of deployment:

Configuration at the client is minimal, because the clients have required NAS connection software built in.

5) Explain components of NAS with neat diagram.

Ans)

- A NAS device has two key components: NAS head and storage.
- In some NAS implementations, the storage could be external to the NAS device and shared with other hosts.



The NAS head includes the following components:

1) CPU and memory

2) One or more network interface cards (NICs):

- It provides connectivity to the client network.
- Examples of network protocols supported by NIC include Gigabit Ethernet, Fast Ethernet, ATM and Fiber Distributed Data Interface (FDDI).

3) An optimized operating system:

- It is used for managing the NAS functionality.
- It translates file-level requests into block-storage requests and further converts the data supplied at the block level to file data.

4) NFS, CIFS and other protocols:

- It is used for file sharing.

5) Industry-standard storage protocols and ports:

- It is used to connect and manage physical disk resources.

The NAS environment includes clients accessing a NAS device over an IP network using file-sharing protocols.

6) Explain NAS implementation in detail.

Ans) Three common NAS implementations are:

1) The **Unified** NAS

2) The **Gateway** NAS

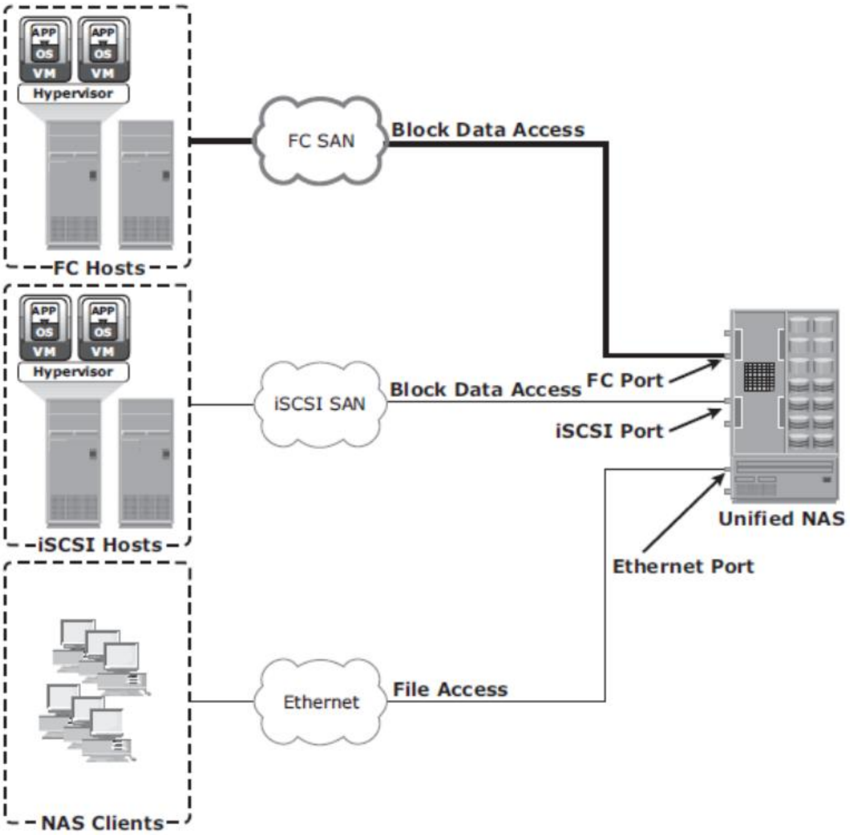
3) The **Scale-out** NAS

Unified NAS:

- Unified NAS performs file serving and storing of file data.
- It also provides access to block-level data.
- It supports both CIFS and NFS protocols for file access.
- It supports both iSCSI and FC protocols for block level access.

Unified NAS Connectivity:

- Each NAS head in a unified NAS has front-end Ethernet ports, which connect to the IP network.
- The front-end ports provide connectivity to the clients and service the file I/O requests.
- Each NAS head has back-end ports, to provide connectivity to the storage controllers.



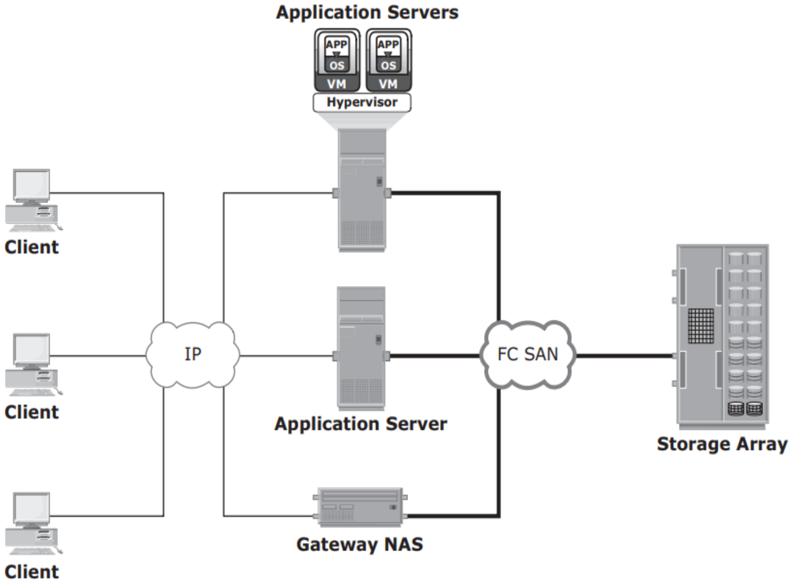
Unified NAS connectivity

Gateway NAS:

- A gateway NAS device consists of one or more NAS heads.
- It uses external and independently managed storage.
- Similar to unified NAS, the storage is shared with other applications that use block-level I/O.
- The gateway NAS is more scalable compared to unified NAS.

Gateway NAS Connectivity:

- In a gateway solution, the front-end connectivity is similar to that in a unified storage solution.
- Communication between the NAS gateway and the storage system is achieved through a traditional FC SAN.
- Implementation of both unified and gateway solutions requires analysis of the SAN environment.



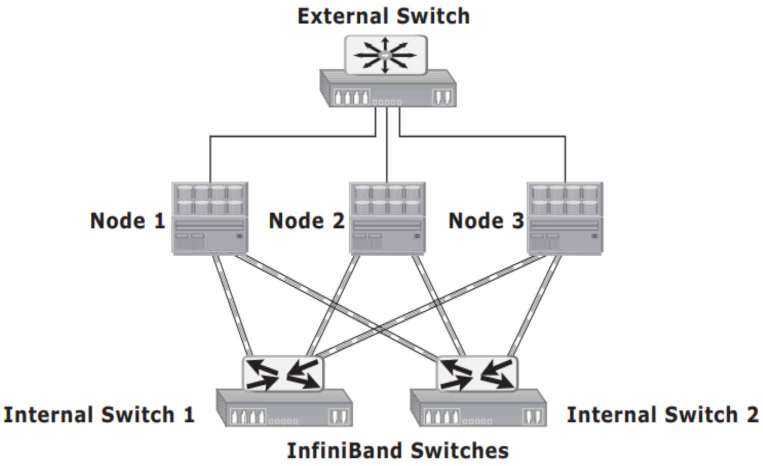
Gateway NAS connectivity

Scale-Out NAS:

- Scale-out NAS enables grouping multiple nodes together to construct a clustered NAS system.
- It provides the capability to scale its resources by simply adding nodes to a clustered NAS architecture.
- The cluster works as a single NAS device and is managed centrally.
- It also provides ease of use, low cost and theoretically unlimited scalability.
- Scale-out NAS creates a single file system that runs on all nodes in the cluster.

Scale-Out NAS Connectivity:

- Scale-out NAS clusters use separate internal and external networks for back-end and front-end connectivity respectively.
- Each node in the cluster connects to the internal network.
- The internal network offers high throughput and low latency.
- The internal network uses high-speed networking technology, such as InfiniBand or Gigabit Ethernet.



Scale-out NAS with dual internal and single external networks

7) Explain NAS file sharing protocols. Write four comparisons between them.

Ans) Two common NAS file sharing protocols are:

1) NFS – Network File System protocol

2) CIFS – Common Internet File System protocol

1) NFS:

- NFS is a client-server protocol for file sharing that is commonly used on UNIX systems.
- NFS was originally based on the connectionless User Datagram Protocol (UDP).
- It uses a machine-independent model to represent user data.
- It also uses Remote Procedure Call (RPC) as a method of inter-process communication between two computers.
- The NFS protocol provides a set of RPCs to access a remote file system for the following operations:
  - Searching files and directories
  - Opening, reading, writing to and closing a file
  - Changing file attributes
  - Modifying file links and directories

- Currently, three versions of NFS are in use:

  1) NFS version 2 (NFSv2)

  2) NFS version 3 (NFSv3)

  3) NFS version 4 (NFSv4)

2) CIFS:

- CIFS is a client-server application protocol that enables client programs to make requests for files and services on remote computers over TCP/IP.
- It is a public or open, variation of Server Message Block (SMB) protocol.
- It enables remote clients to gain access to files on a server.
- CIFS provides the following features to ensure data integrity:
  - ➢ It uses file and record locking to prevent users from overwriting the work of another user on a file or a record.
  - ➢ It supports fault tolerance.
  - ➢ It can automatically restore connections and reopen files that were open prior to an interruption client.

NFS	CIFS
1) NFS is primarily used in Unix systems.	1) CIFS is primarily used in Windows systems. Using Samba, it can support Linux and macOS systems as well.
2) NFS uses a host-based authentication model.	2) CIFS uses a user-based authentication model.
3) NFS provides limited support for file attributes, such as permissions, ownership and timestamps.	3) CIFS offers comprehensive support for file attributes, including permissions, ownership and timestamps.
4) NFS has a low protocol overhead, which results in higher performance.	4) CIFS has a higher protocol overhead, which results in lower performance.

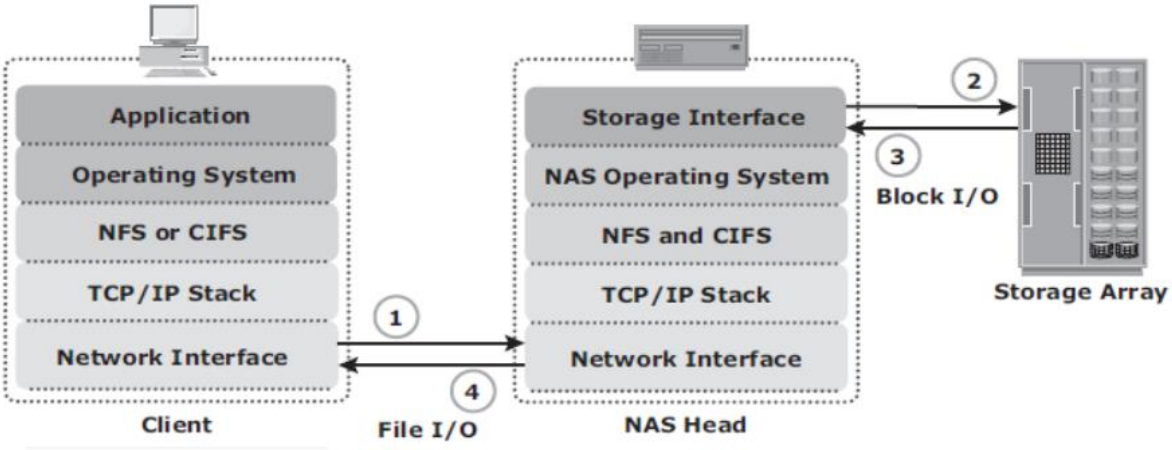
8) Explain NAS I/O operation.

Ans)

- NAS provides file-level data access to its clients.
- File I/O is a high-level request that specifies the file to be accessed.
- For example, a client may request a file by specifying its name, location or other attributes.

The process of handling I/Os in a NAS environment is as follows:

- The requestor (client) packages an I/O request into TCP/IP and forwards it through the network stack.
- The NAS device receives this request from the network.
- The NAS device converts the I/O request into an appropriate physical storage request, which is a block-level I/O.
- Operations are performed on the physical storage.
- When the NAS device receives data from the storage, it processes and repackages the data into an appropriate file protocol response.
- The NAS device packages this response into TCP/IP again and forwards it to the client through the network.



NAS I/O operation

9) Write a short note on FCIP Performance and Security.

Ans)

- Performance, reliability and security should always be taken into consideration when implementing storage solutions.
- The implementation of FCIP is also subject to the same considerations.
- From the perspective of performance, configuring multiple paths between FCIP gateways eliminates single points of failure and provides increased bandwidth.
- Insufficient bandwidth can slow down the IP network over long distances.
- If the IP network experiences problems, it can affect the stability of the SAN because FCIP creates a single network connection.
- These instabilities include a segmented fabric, excessive RSCNs and host timeouts.
- FC switch vendors have improved FCIP by adding features that enhance stability, like the ability to separate FCIP traffic into its own virtual fabric.
- Security is also a consideration in an FCIP solution because the data is transmitted over public IP channels.
- Various security options are available to protect the data based on the router’s support.
- IPSec is one such security measure that can be implemented in the FCIP environment.