SRM INSTITUTE OF SCIENCE AND TECHNOLOGY,
CHENNAI.

18CSE360T INFORMATION STORAGE AND MANAGEMENT

UNIT – II

Virtualization and Cloud Computing, Fiber Channel: Overview, SAN and its Evolution, Components of FC SAN, FC Connectivity, FC Architecture, IPSAN-iSCSI components, iSCSI Protocol Stacki SCSI Names, NAS: General Purpose Servers versus NAS Devices, Benefits of NAS- File Systems and Network File Sharing, Components of NAS, NAS I/O Operation, NAS Implementations, NAS File Sharing Protocols, Object Based Storage Devices, Content Addressed Storage, Configuration and Tracing of FC scan and iSCSI scan.

Fiber Channel: Overview

Fibre Channel (FC) is a high-speed network technology that interconnects network elements and allows them to communicate with one another.

The International Committee for Information Technology Standards (INCITS) T11 Technical Committee sets FC standards.

FC networks provide high-performance characteristics such as lossless transport combined with flexible network topology.

FC is primarily used in storage area networks (SANs) because it provides reliable, lossless, in-order frame transport between initiators and targets.

FC components include initiators, targets, and FC-capable switches that interconnect FC devices and may also interconnect FC devices with Fibre Channel over Ethernet (FCoE) devices.

Initiators originate I/O commands. Targets receive I/O commands. For example, a server can initiate an I/O request to a storage device target.

- The Juniper Networks QFX3500 Switch has native FC ports as well as Ethernet access ports, and can function as an FCoE-FC gateway or as an FCoE transit switch.
- All other QFX Series switches and EX4600 switches have Ethernet access ports and can function as an FCoE transit switch.
- FCoE transports native FC frames over an Ethernet network by encapsulating the unmodified frames in Ethernet. It also provides protocol extensions to discover FCoE devices through the Ethernet network.
- FCoE requires that the Ethernet network support data center bridging (DCB) extensions that ensure lossless transport and allow the Layer 2 Ethernet domain to meet the requirements of FC transport.
- The FCoE-FC gateway functionality is a licensed feature on the QFX Series that is available only on QFX3500 switches. As an FCoE-FC gateway, the switch connects FCoE devices on an Ethernet network to a SAN FC switch.

SAN and its Evolution

A SAN carries data between servers (or hosts) and storage devices through Fibre Channel network.

A SAN enables storage consolidation and enables storage to be shared across multiple servers.

This improves the utilization of storage resources compared to direct-attached storage architecture and reduces the total amount of storage an organization needs to purchase and manage.

With consolidation, storage management becomes centralized and less complex, which further reduces the cost of managing information.

SAN also enables organizations to connect geographically dispersed servers and storage

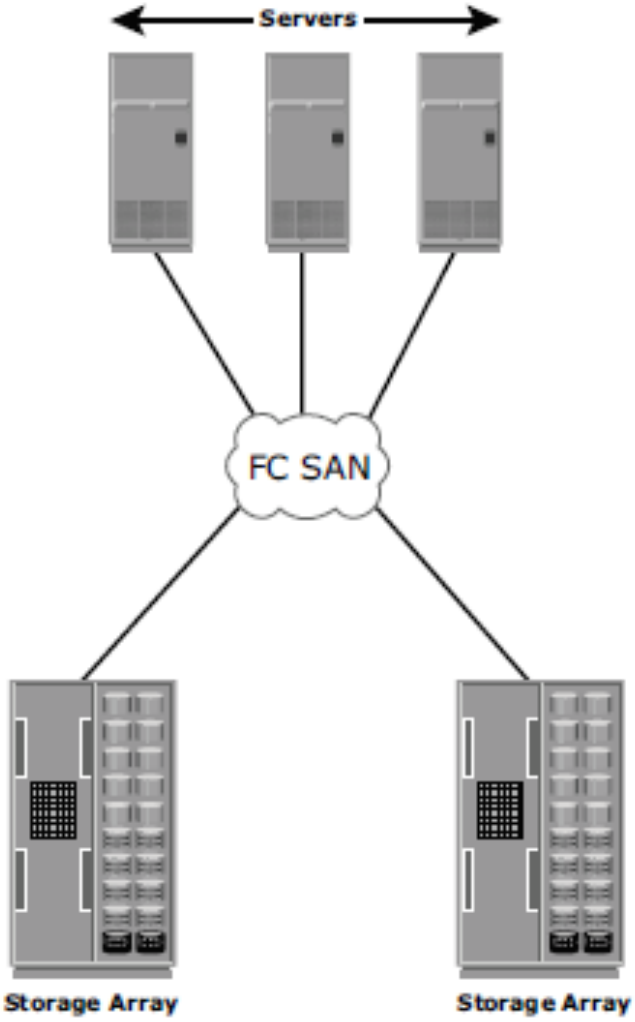
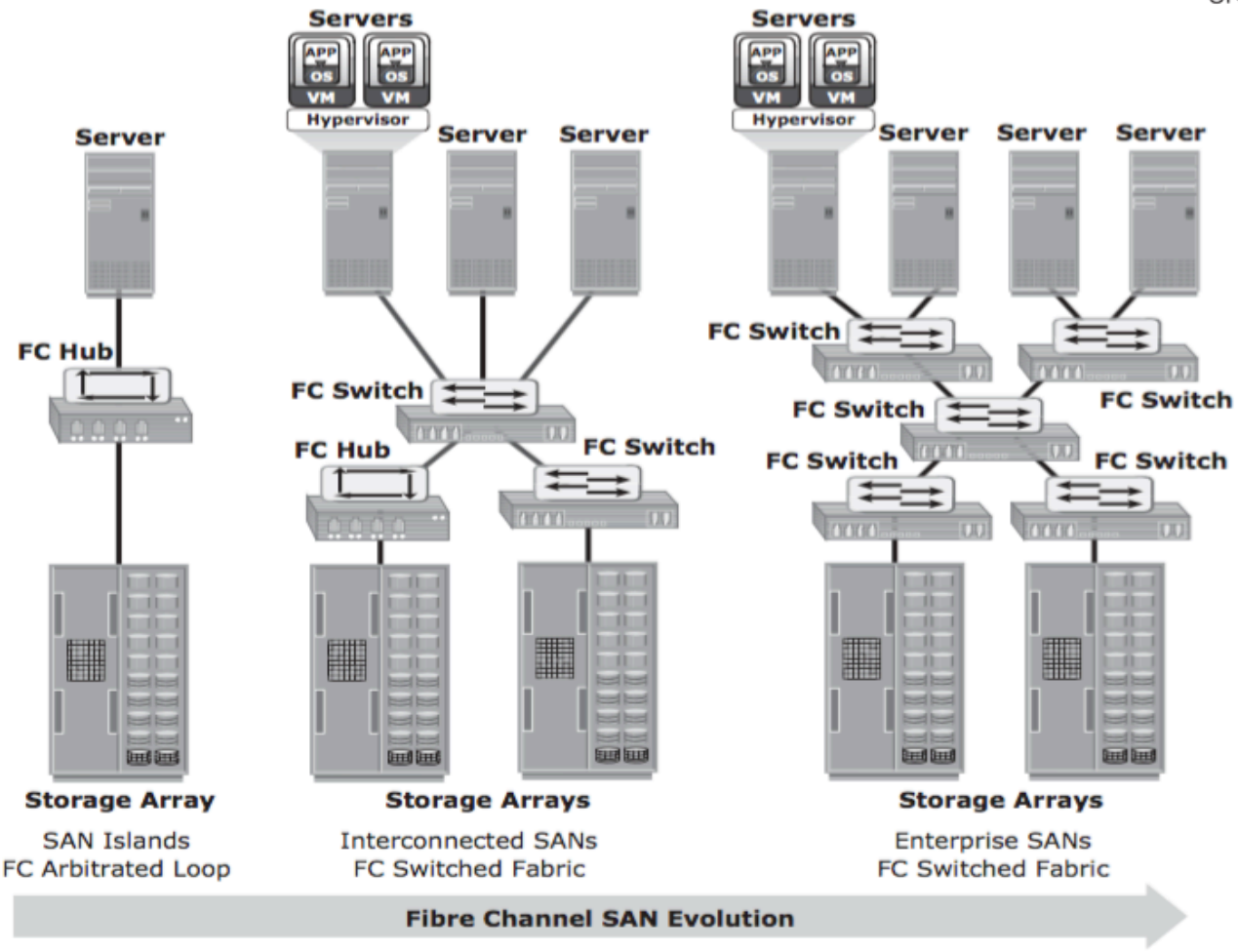


Figure 6-1: SAN implementation

- The FC SAN was a simple grouping of hosts and storage devices connected to a network using an FC hub as a connectivity device.
- This configuration of an FC SAN is known as a Fibre Channel Arbitrated Storage Networking Technologies Loop (FC-AL).
- Use of hubs resulted in isolated FC-AL SAN islands because hubs provide limited connectivity and bandwidth.
- The inherent limitations associated with hubs gave way to high-performance FC switches.
- Use of switches in SAN improved connectivity and performance and enabled FC SANs to be highly scalable.
- This enhanced data accessibility to applications across the enterprise.


Server
FC Hub
Storage Array
SAN Islands
FC Arbitrated Loop
Servers
APP
OS
VM
Hypervisor
Server
Server
FC Switch
FC Hub
FC Switch
Storage Arrays
Interconnected SANs
FC Switched Fabric
Servers
Server
Server
Server
FC Switch
FC Switch
FC Switch
FC Switch
Storage Arrays
Enterprise SANs
FC Switched Fabric
Fibre Channel SAN Evolution

Components of FC SAN

- FC SAN is a network of servers and shared storage devices. Servers and storage are the end points or devices in the SAN (called nodes).
- FC SAN infrastructure consists of node ports, cables, connectors, and interconnecting devices (such as FC switches or hubs), along with SAN management software.
  - Node Ports
  - Cables and Connectors
  - Interconnect Devices
  - SAN Management Software

1. Node port:

In fiber channel, devices like,

Host

Storage

Tape Libraries are referred as **nodes**

Nodes consists of ports for transmission between other nodes. Ports operate in **Full-duplex** data transmission mode with transmit(Tx) and Receive(Rx) link.

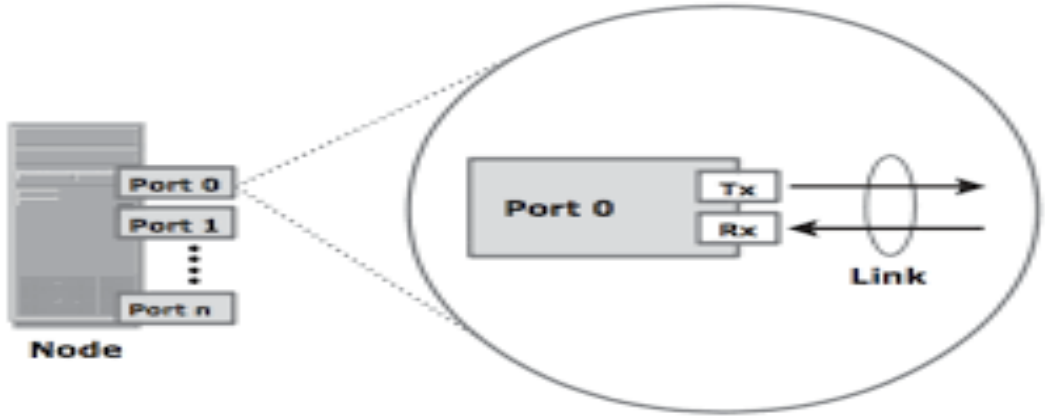


Figure 5-3: Nodes, ports, and links

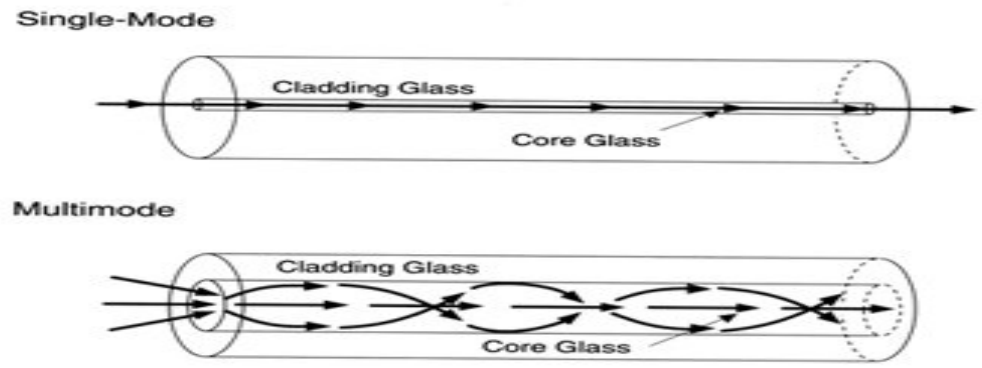
2. Cables:

SAN implements optical fiber cabling. Copper cables are used for short distance connectivity and optical cables for long distance connection establishment.

There are 2 types of optical cables:

Multi-mode fiber

Single-mode fiber



Multi-mode fiber:

Also called as MMF, as it carries multiple rays of light projected at different angles simultaneously onto the core of the cable.

In MMF transmission, light beam travelling inside the cable tend to disperse and collide.

This collision, weakens the signal strength after it travels certain distance, and it is called as **modal dispersion**.

MMF cables are used for distance up-to 500 meters because of signal degradation(attenuation) due to modal dispersion.

Single-mode fiber:

Also called SMF, as it carries a single beam of light through the core of the fiber.

Small core in the cable reduces modal dispersion.

SMF cables are used for distance up-to 10 kilometers due to less attenuation.

SMF is costlier than MMF.

Other than these cables, Standard Connectors (SC) and Lucent Connectors (LC) are commonly used fiber cables with data transmission speed up-to 1 Gbps and 4 Gbps respectively.

3. Interconnection Devices:

The commonly used interconnection devices in SAN are:

Hubs

Switches and

Directors

Hubs are communication devices used in fiber cable implementations. They connect nodes in loop or star topology.

Switches are more intelligent than hubs. They directly route data from one port to other. They are cheap and their performance is better than hubs.

Directors are larger than switches, used for data center implementations. Directors have high fault tolerance and high port count than switches.

4. SAN Management Software:

This software manages the interface between the host, interconnection devices and storage arrays.

It includes key management functions like mapping of storage devices, switches, and logical partitioning of SAN, called **zoning**.

It also manages the important components of SAN like storage devices and interconnection devices.

FC Connectivity

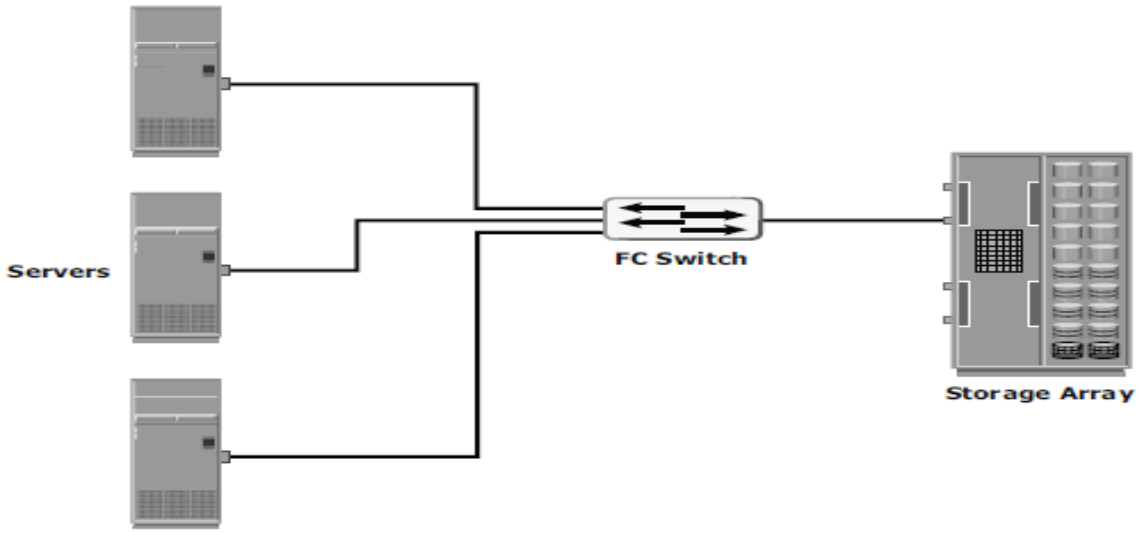
- The FC architecture supports three basic interconnectivity options:
  - point-to-point,
  - Arbitrated loop, and
  - Fiber Channel switched fabric

Point-to-Point

- A single link connects two ports in this topology.
- This topology is inexpensive but it doesn't require a hub.
- To create point to point configuration, you can provide multiple 'N' ports on each node.
- Each point to point connection provides the full bandwidth supported by 'N' ports. Depending on the type of the link (multi-mode or single-mode fiber), the two nodes can be separated

Arbitrated Loop

- It is a high-speed fiber channel [FC] topology in which fiber channel ports/hubs use arbitration to establish a point-to-point circuit and prevent multiple ports/hubs from sending frames at the same time.
- Here devices are connected in a one-way ring. So, when ports/hubs in a loop topology have information to transmit, they must send out an arbitration signal to decide, which port/hub can use the channel.
- The port in control of the channel then sends an ‘open’ arbitrated signal to the destination port and transmits its information. Since all the ports in the loop are connected, every port will see and pass along the data, but ignore the data unless it is addressed to that particular port.
- FC-AL can join up to 126 ports on one controller.
- It is still used internally in many fiber channel switches but rarely to connect hosts to storage these days.
- FC- hubs provide bypass circuits that prevent the loop from breaking if one device fails or is removed.


Servers
FC Switch
Storage Array

Fibre Channel Switched Fabric

This is the topology, that is very much in use nowadays.

The network of switches in a fiber channel habitat is referred to as a fabric.

Ports on one node can communicate with ports on other nodes attached to the same fabric. With the fabric topology, many connections can be alert at a time.

The any-to-any connection service and peer-peer communication service provided by a fabric is fundamental to fiber channel architecture. Fiber channel can hold-up both channel and network protocol simultaneously.

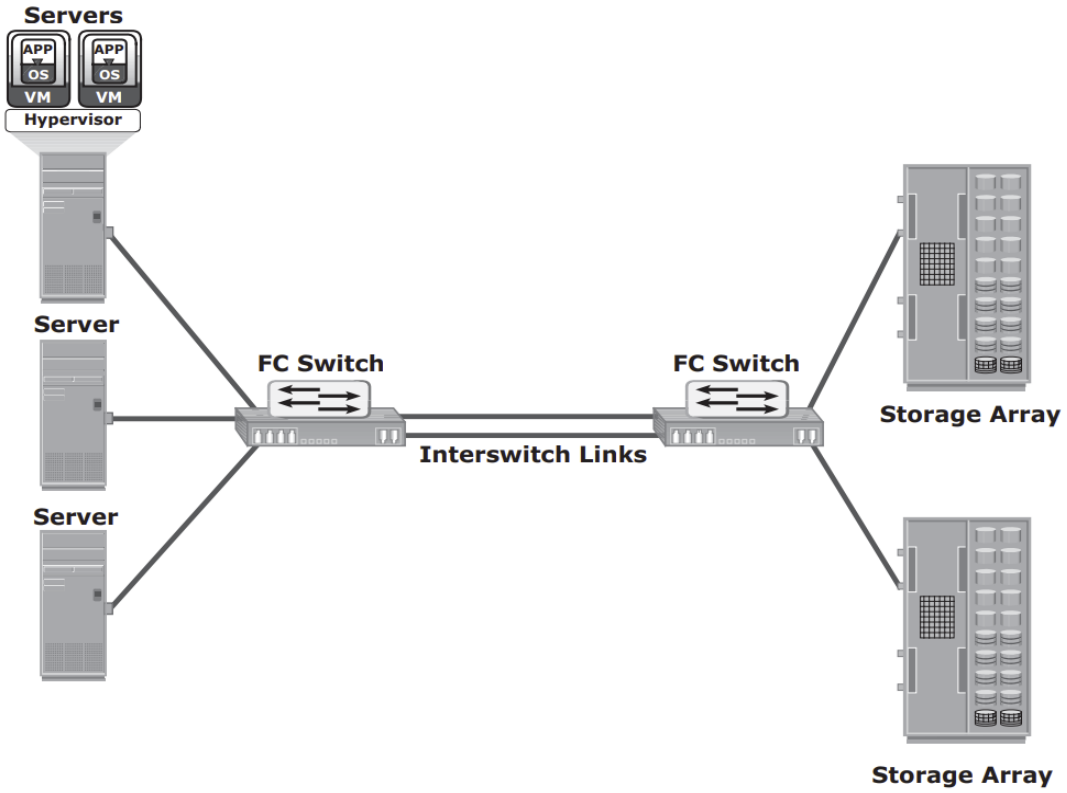


Figure 5-8: Fibre Channel switched fabric

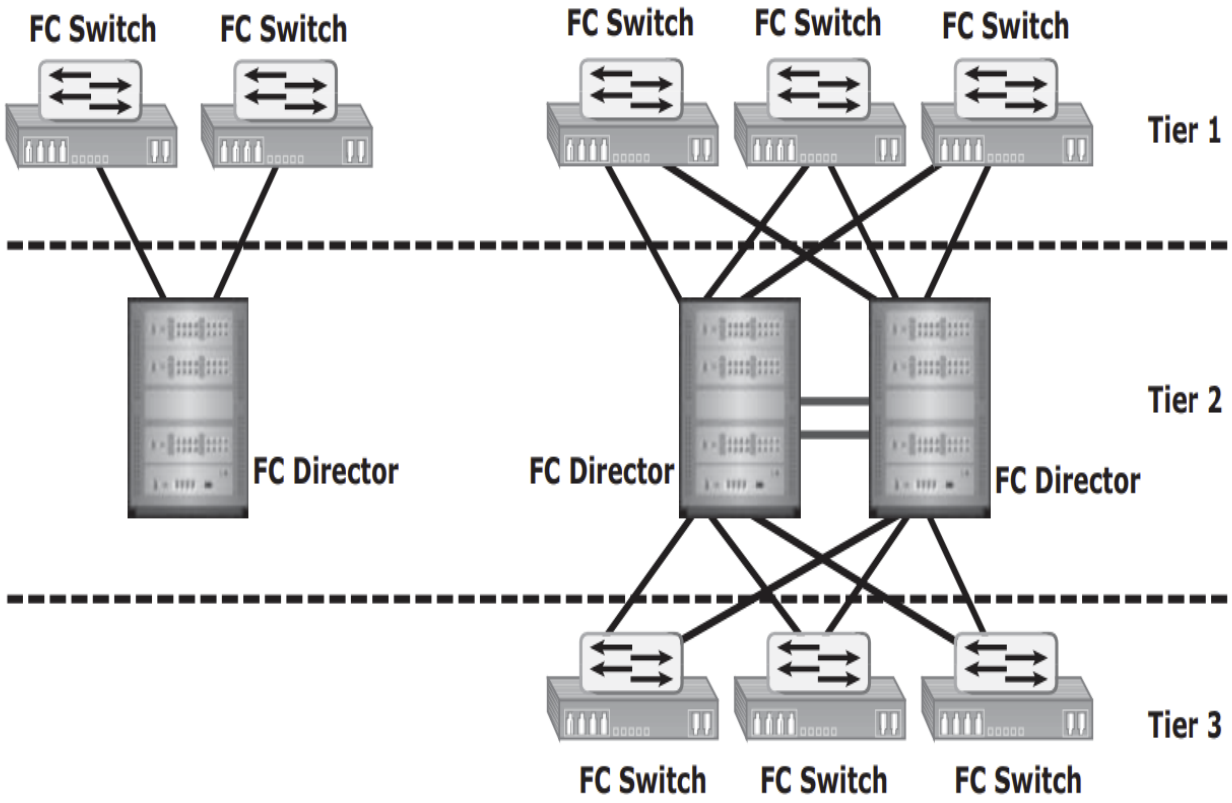


Figure: Tiered structure of Fibre Channel switched fabric

FC Architecture

The FC architecture represents true channel/network integration and captures some of the benefits of both channel and network technology.

FC SAN uses the Fiber Channel Protocol (FCP) that provides both channel speed for data transfer with low protocol overhead and scalability of network technology.

The key advantages of FCP are as follows:

Sustained transmission bandwidth over long distances.

Support for a larger number of addressable devices over a network. Theoretically, FC can support more than 15 million device addresses on a network.

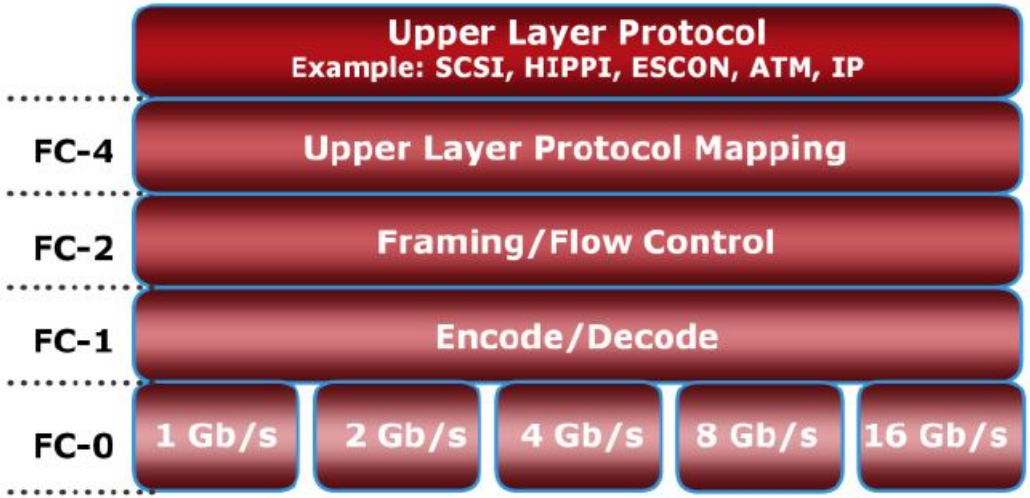
Support speeds up to 16 Gbps (16 GFC)

Fiber Channel Protocol Stack

FCP defines the communication protocol in five layers:

FC-0 through FC-4 (except FC-3 layer, which is not implemented).

In a layered communication model, the peer layers on each node talk to each other through defined protocols



FC-0. This is the lowest level of the Fiber Channel (FC) physical standard, covering the physical characteristics of the interface and media.

FC-1. This is the middle level of the FC physical standard. It defines the 8-bit to 10-bit encoding/decoding and transmission protocol.

FC-2. This is the highest level of FC physical standard, defining the rules for signaling protocol and describing transfer of frames, sequences, and exchanges.

FC-4. This is the hierarchical level in the Fiber Channel standard that specifies the mapping of upper layer protocols. Some of the protocols include SCSI, High Performance Parallel Interface (HIPPI) Framing Protocol, Enterprise Storage Connectivity (ESCON), Asynchronous Transfer Mode (ATM), and IP.

Fibre Channel Addressing

The first field of the FC address contains the domain ID of the switch.

A domain ID is a unique number provided to each switch in the fabric.

Although this is an 8-bit field, there are only 239 available addresses for domain ID because some addresses are deemed special and reserved for fabric management services.

For example, FFFFFC is reserved for the name server, and FFFFFE is reserved for the fabric login service.

The area ID is used to identify a group of switch ports used for connecting nodes.

An example of a group of ports with a common area ID is a port card on the switch.

The last field, the port ID, identifies the port within the group. Therefore, the maximum possible number of node ports in a switched fabric is calculated as:

239 domains ¥ 256 areas ¥ 256 ports = 15,663,104

Figure 6-14: 24-bit FC address of N_port

World Wide Names

Each device in the FC environment is assigned a 64-bit unique identifier called the World Wide Name (WWN).

The Fibre Channel environment uses two types of WWNs:

World Wide Node Name (WWNN) and

World Wide Port Name (WWPN).

World Wide Name – Array															
5	0	0	6	0	1	6	0	0	0	6	0	0	1	B	2
0101	0000	0000	0110	0000	0001	0110	0000	0000	0000	0110	0000	0000	0001	1011	0010
Company ID 24 bits							Port	Model seed 32 bits							

World Wide Name - HBA															
1	0	0	0	0	0	0	0	c	9	2	0	d	c	4	0
	Reserved 12 bits			Company OUI 24 bits						Company Specific 24 bits					

FC Frame

An FC frame (Figure 5-15) consists of five parts:

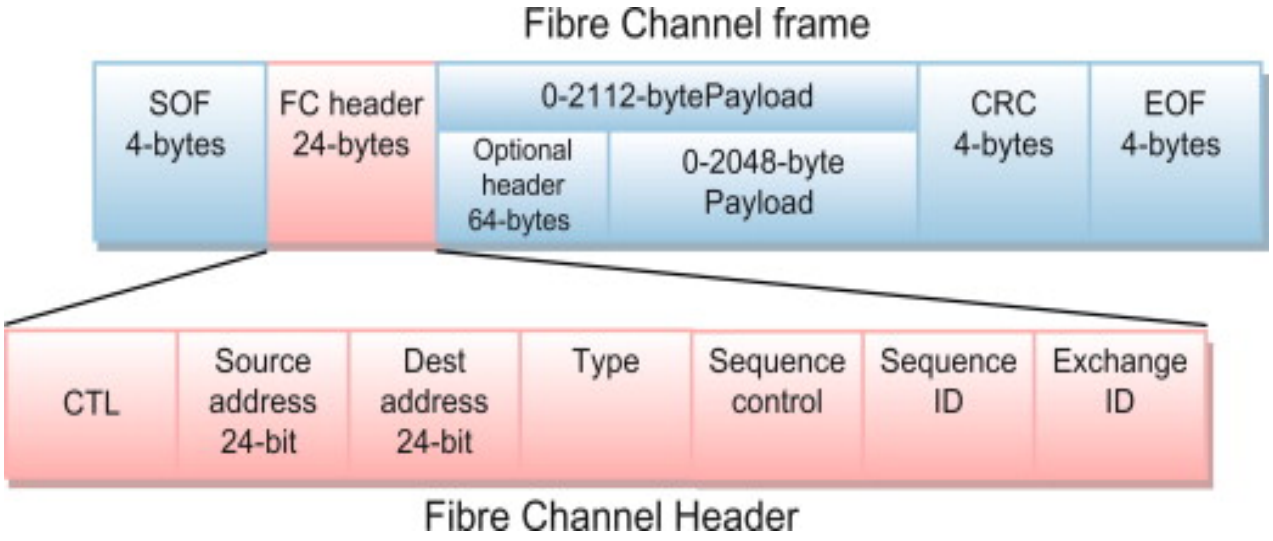
start of frame (SOF),

frame header,

data field,

cyclic redundancy check (CRC), and

end of frame (EOF).



IP SAN - Components of iSCSI

- An initiator (host), target (storage or iSCSI gateway), and an IP-based network are the key iSCSI components.
- If an iSCSI-capable storage array is deployed, then a host with the iSCSI initiator can directly communicate with the storage array over an IP network.
- However, in an implementation that uses an existing FC array for iSCSI communication, an iSCSI gateway is used
- These devices perform the translation of IP packets to FC frames and vice versa, thereby bridging the connectivity between the IP and FC environments.

iSCSI Protocol Stack

SRM UNIVERSITY
(Under section 3 of UGC Act 1956)

- 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 and 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

iSCSI Protocol Stack

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.

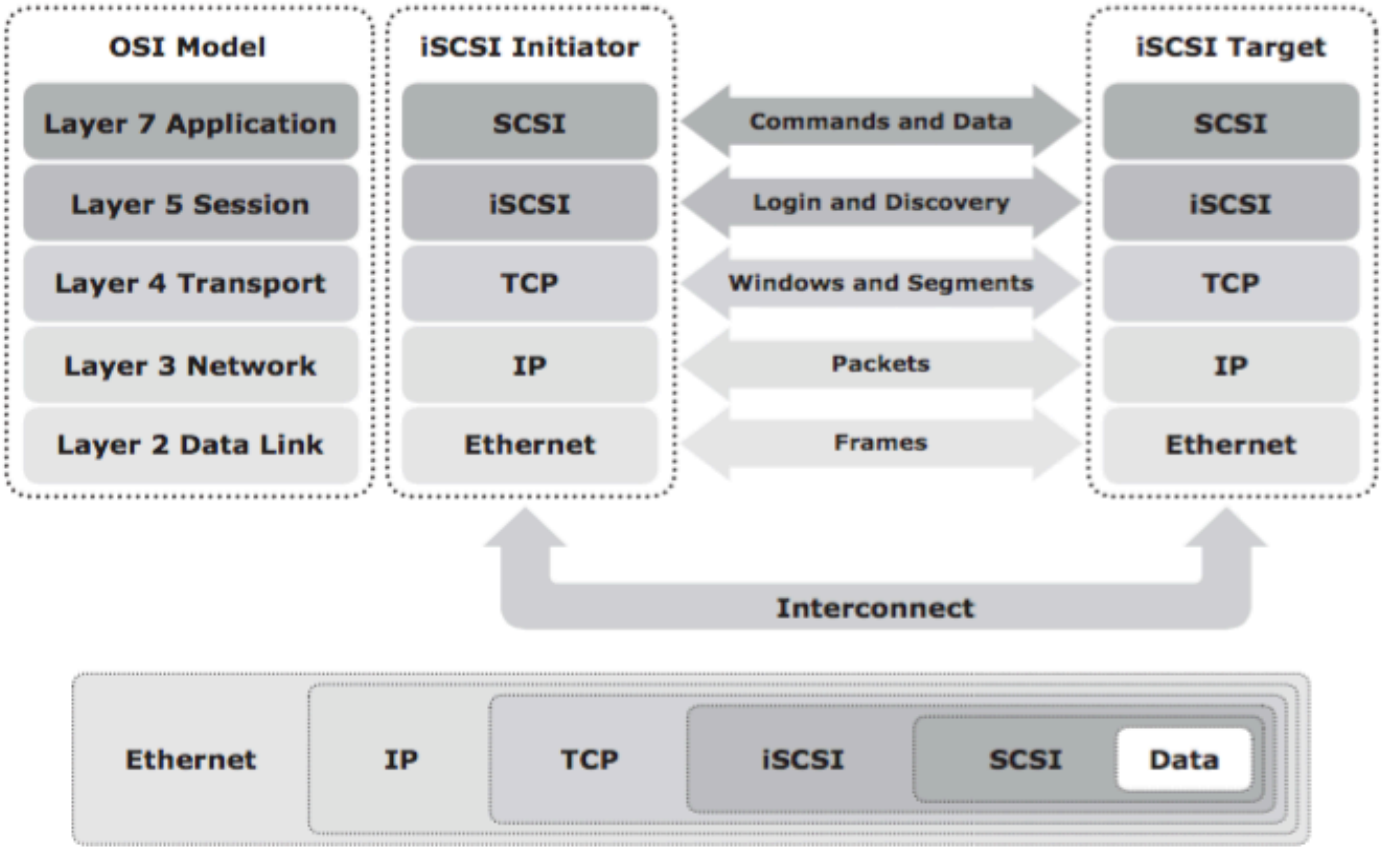


Figure 6-3: iSCSI protocol stack

iSCSI Names

A unique worldwide iSCSI identifier, known as an iSCSI name, is used to identify the initiators and targets within an iSCSI network to facilitate communication.

iSCSI Qualified Name (IQN) - An organization must own a registered domain name to generate iSCSI Qualified Names. An example of an IQN is iqn.2008-02.com.example:optional_string.

Extended Unique Identifier (EUI): An EUI is a globally unique identifier based on the IEEE EUI-64 naming standard. An EUI is composed of the eui prefix followed by a 16-character hexadecimal name, such as eui.0300732A32598D26.

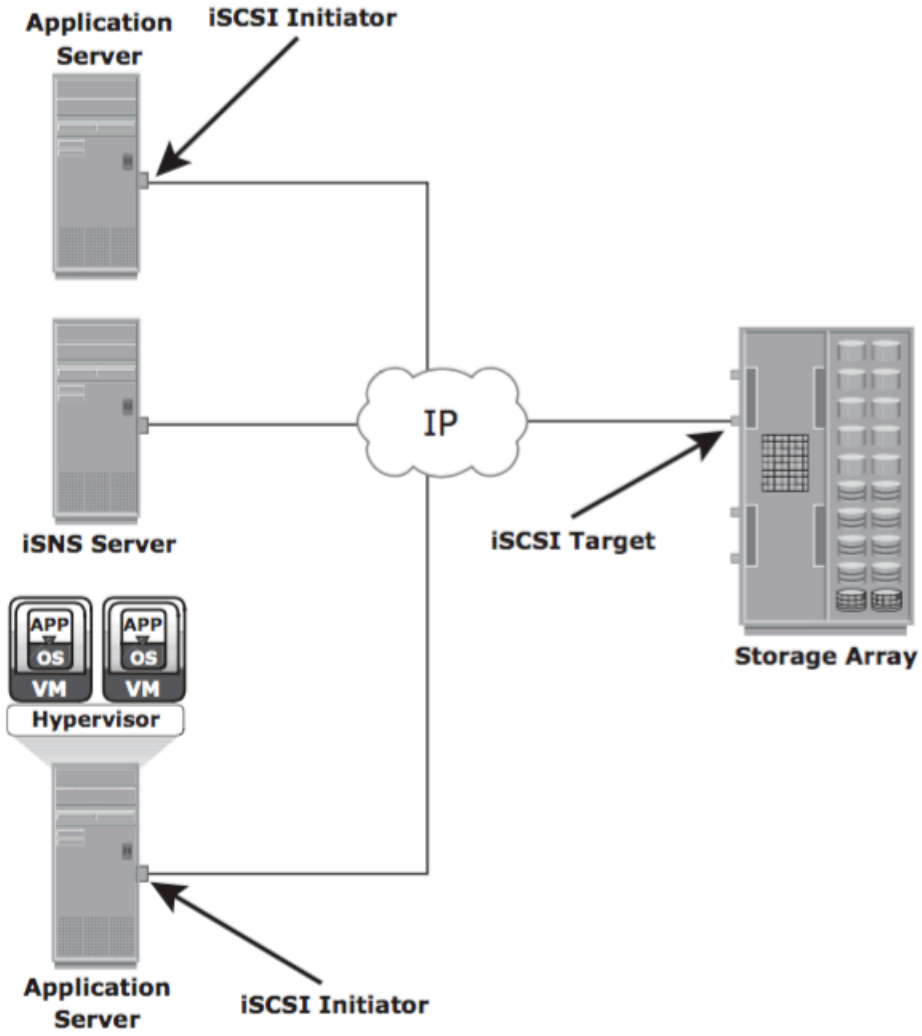


Figure 6-6: Discovery using iSNS

NAS: General Purpose Servers versus NAS Devices

- A NAS device is optimized for file-serving functions such as storing, retrieving, and accessing fi les for applications and clients.
- A general-purpose server can be used to host any application because it runs a general-purpose operating system.
- Unlike a general-purpose server, a NAS device is dedicated to file-serving.
- It has specialized operating system dedicated to file serving by using industry-standard protocols.
- Some NAS vendors support features, such as native clustering for high availability

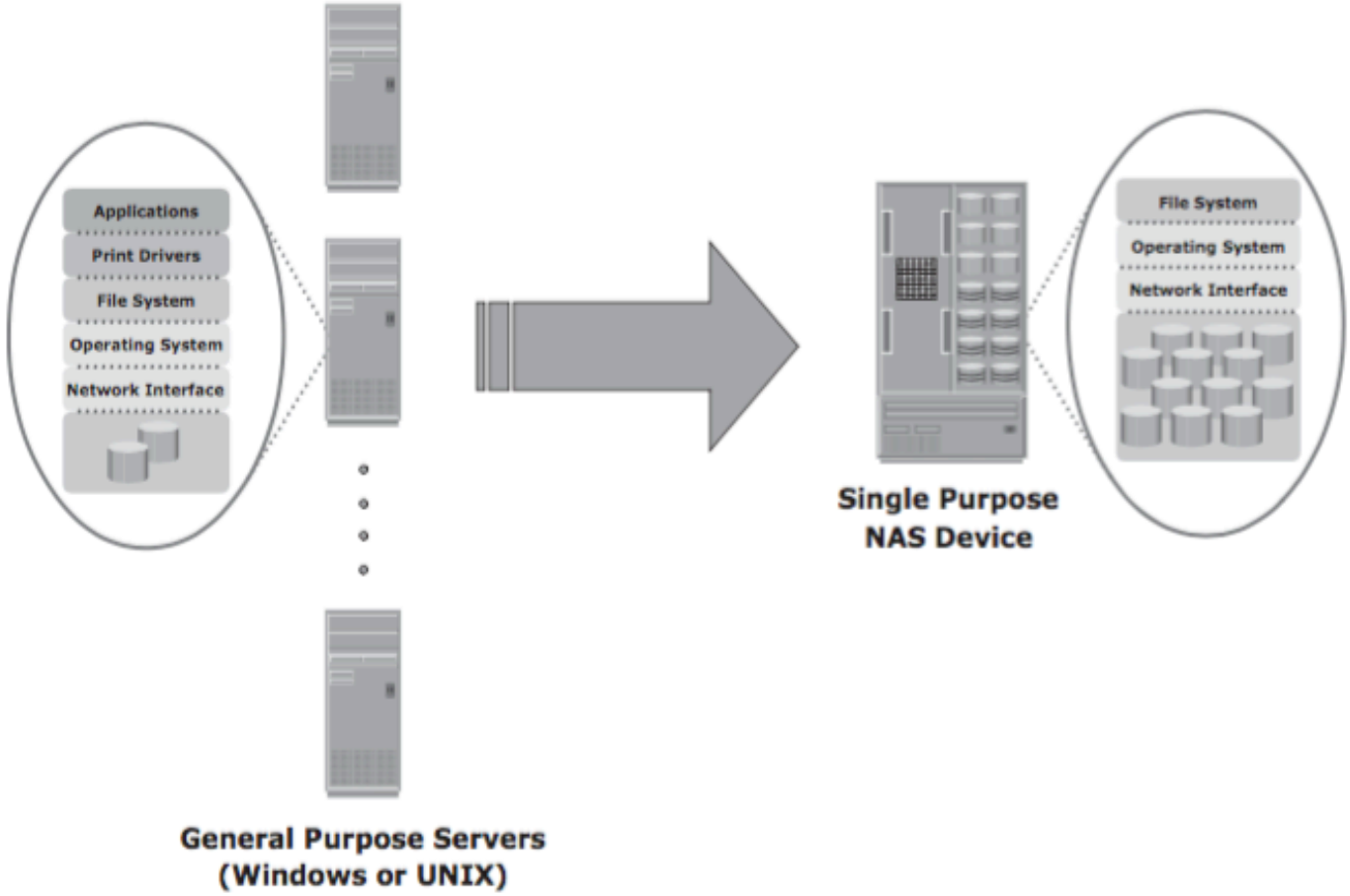


Figure 7-1: General purpose server versus NAS device

Benefits of NAS

NAS offers the following benefits:

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

Benefits of NAS Cont…

Centralized storage:

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

Simplified management:

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

Scalability:

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

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.

Benefits of NAS Cont…

Security:

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

Low cost:

NAS uses commonly available and inexpensive Ethernet components.

Ease of deployment:

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

File systems and Network file sharing

A ***file system*** is a structured way to store and organize data files. Many file systems maintain a file access table to simplify the process of searching and accessing files.

Accessing a File System:

A file system must be mounted before it can be used.

In most cases, the operating system mounts a local file system during the boot process.

The mount process creates a link between the file system on the NAS and the operating system on the client.

When mounting a file system, the operating system organizes files and directories in a tree-like structure and grants the privilege to the user to access this structure.

The tree is rooted at a mount point.

The mount point is named using operating system conventions.

File systems and Network file sharing

SRM UNIVERSITY
(Under section 3 of UGC Act 1956)

Network File Sharing

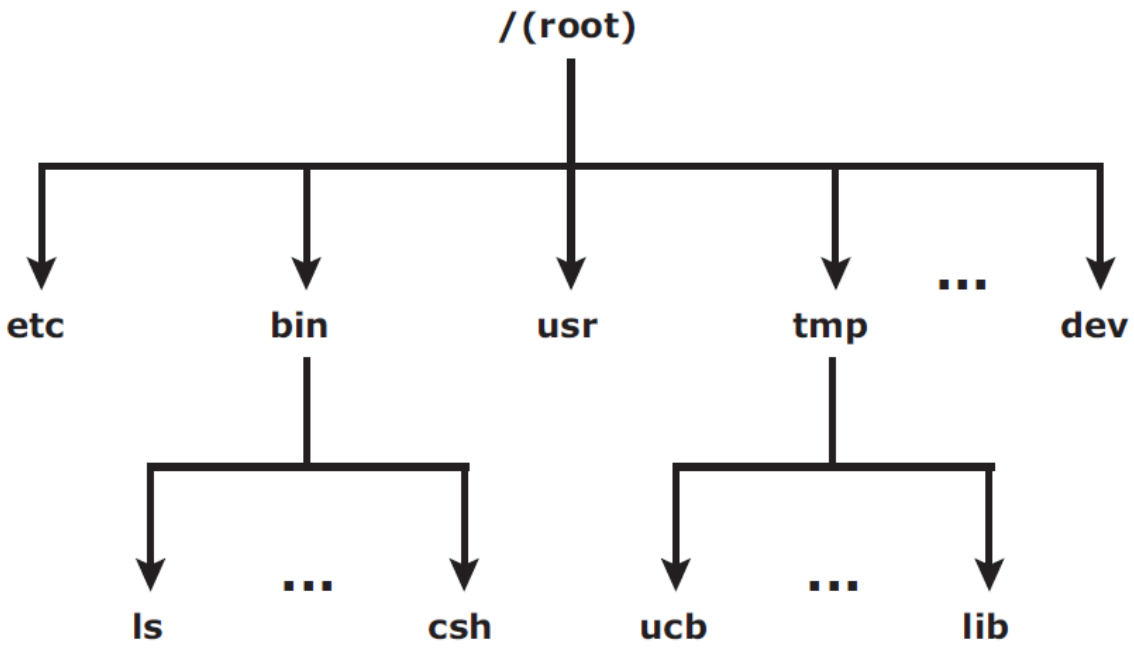
Network file sharing refers to storing and accessing files over a network.

In a file-sharing environment, the user who **creates a file** (the creator or owner of a file) determines the **type of access** (such as read, write, execute, append, and delete) to be given to other users and controls changes to the file.

When multiple users try to access a shared file at the same time, a locking scheme is required to maintain data integrity and, at the same time, make this sharing possible.

File systems and Network file sharing

UNIX directory structure



File systems and Network file sharing

Examples of file-sharing methods,

File transfer protocol (FTP) - client-server protocol that enables data transfer over a network.

Distributed File System (DFS) - file system that is distributed across several hosts.

*A **name service***, such as Domain Name System (DNS), and directory services such as Microsoft Active Directory, and Network Information Services (NIS), helps users identify and access a unique resource over the network

A ***name service protocol*** such as the Lightweight Directory Access Protocol (LDAP) creates a namespace

The peer-to-peer (P2P) model - file sharing model uses a peer-to-peer network

Components of NAS

A NAS device has two key components:

Storage - the storage could be external to the NAS device and shared with other hosts

NAS head - NAS head includes the following components:

- CPU and memory
- One or more network interface cards (NICs), which provide connectivity to the client network.
- An optimized operating system for managing the NAS functionality.

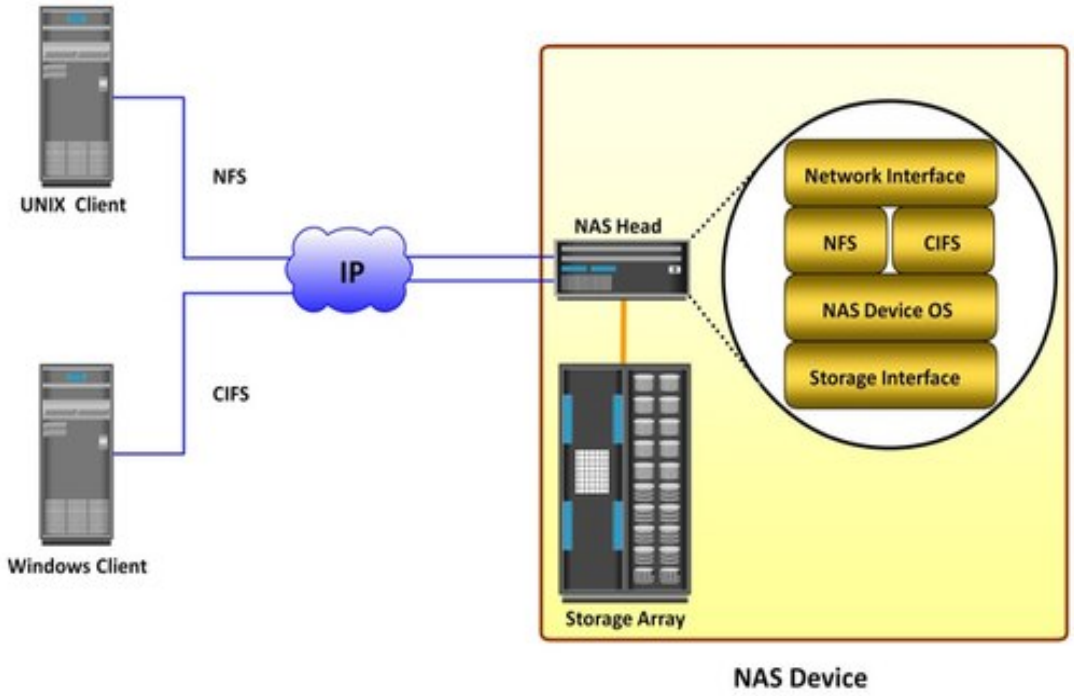
Components of NAS

A NAS device has two key components:

NAS head - NAS head includes the following components:

- NFS (Network File System), CIFS (Common Internet File System), and other protocols for file sharing
- Industry-standard storage protocols and ports to connect and manage physical disk resources

Components of NAS



NAS Device

NAS I/O Operation

NAS provides file-level data access to its clients. File I/O is a high-level request that specifies the file to be accessed.

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

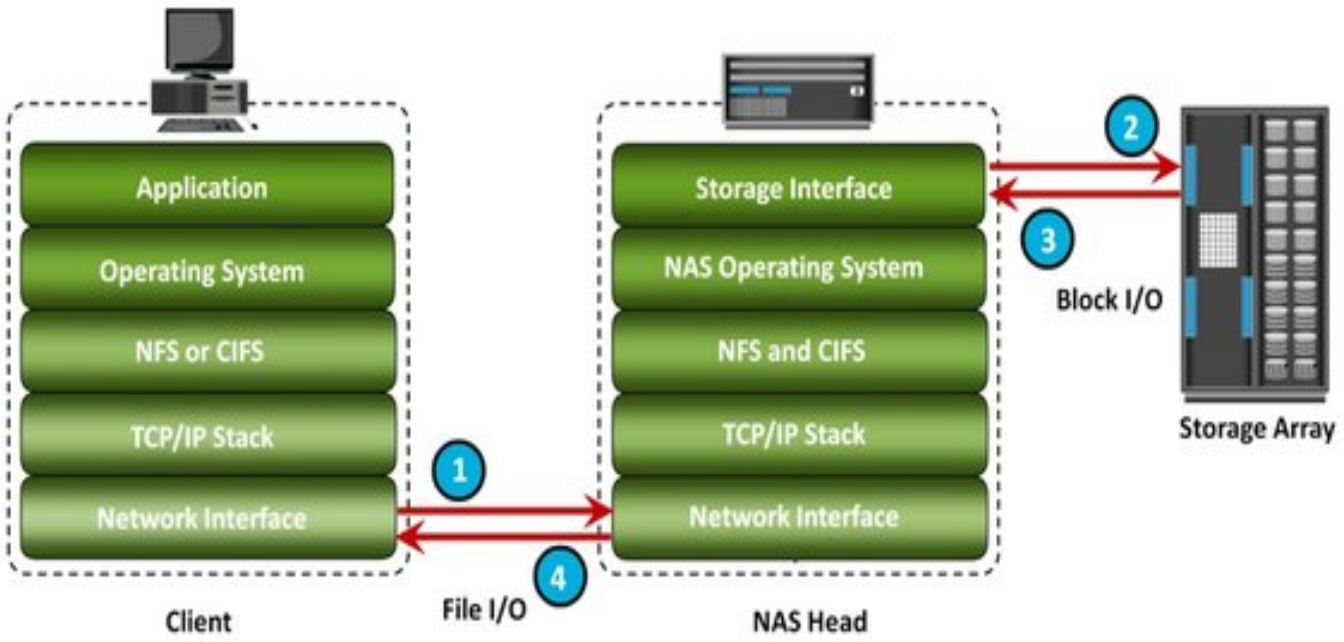
The requestor (client) packages an I/O request into TCP/IP and forwards it through the network stack. The NAS device receives this request from the network.

The NAS device converts the I/O request into an appropriate physical storage request, which is a block-level I/O, and then performs the operation on the physical storage.

When the NAS device receives data from the storage, it processes and repackages the data into an appropriate fi le protocol response.

The NAS device packages this response into TCP/IP again and forward it to the client through the network.

NAS I/O Operation



NAS Implementations

Three common NAS implementations are

unified,

Gateway, and

Scale-out.

The ***unified*** NAS consolidates NAS-based and SAN-based data access within a unified storage platform and provides a unified management interface for managing both the environments.

In a ***gateway*** implementation, the NAS device uses external storage to store and retrieve data, and unlike unified storage, there are separate administrative tasks for the NAS device and storage.

The ***scale-out*** NAS implementation pools multiple nodes together in a cluster. A node may consist of either the NAS head or storage or both. The cluster performs the NAS operation as a single entity.

Unified NAS

- Unified NAS performs file serving and storing of file data, along with providing access to block-level data. It supports both CIFS and NFS protocols for file access and 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 fi le I/O requests.

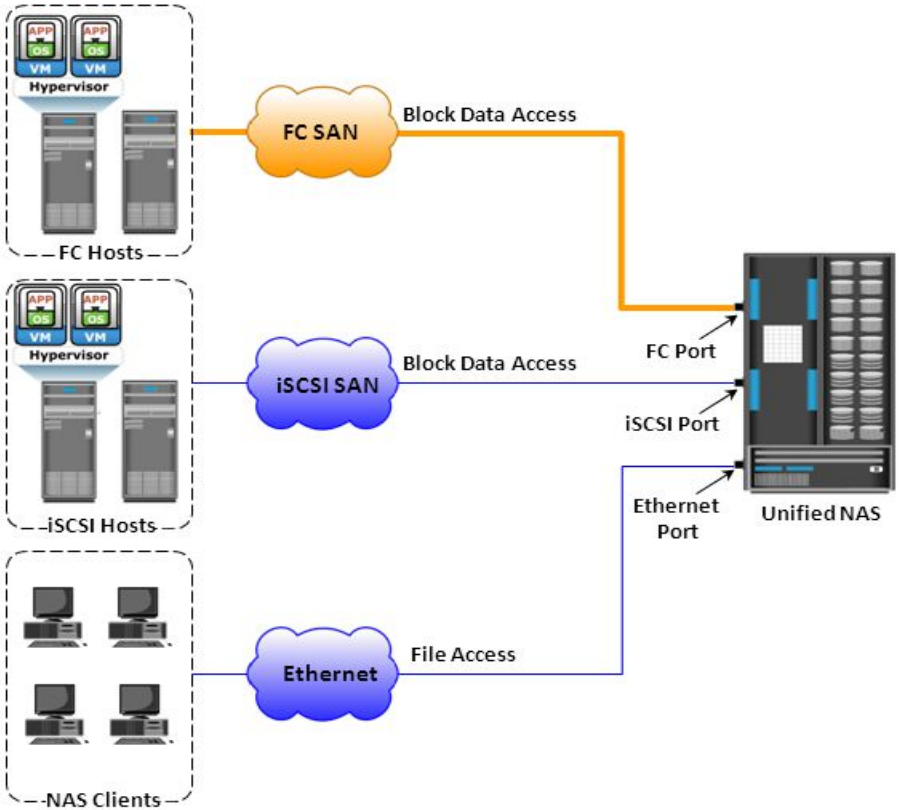
Gateway NAS

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

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 in a gateway solution is achieved through a traditional FC SAN.

Unified NAS Connectivity



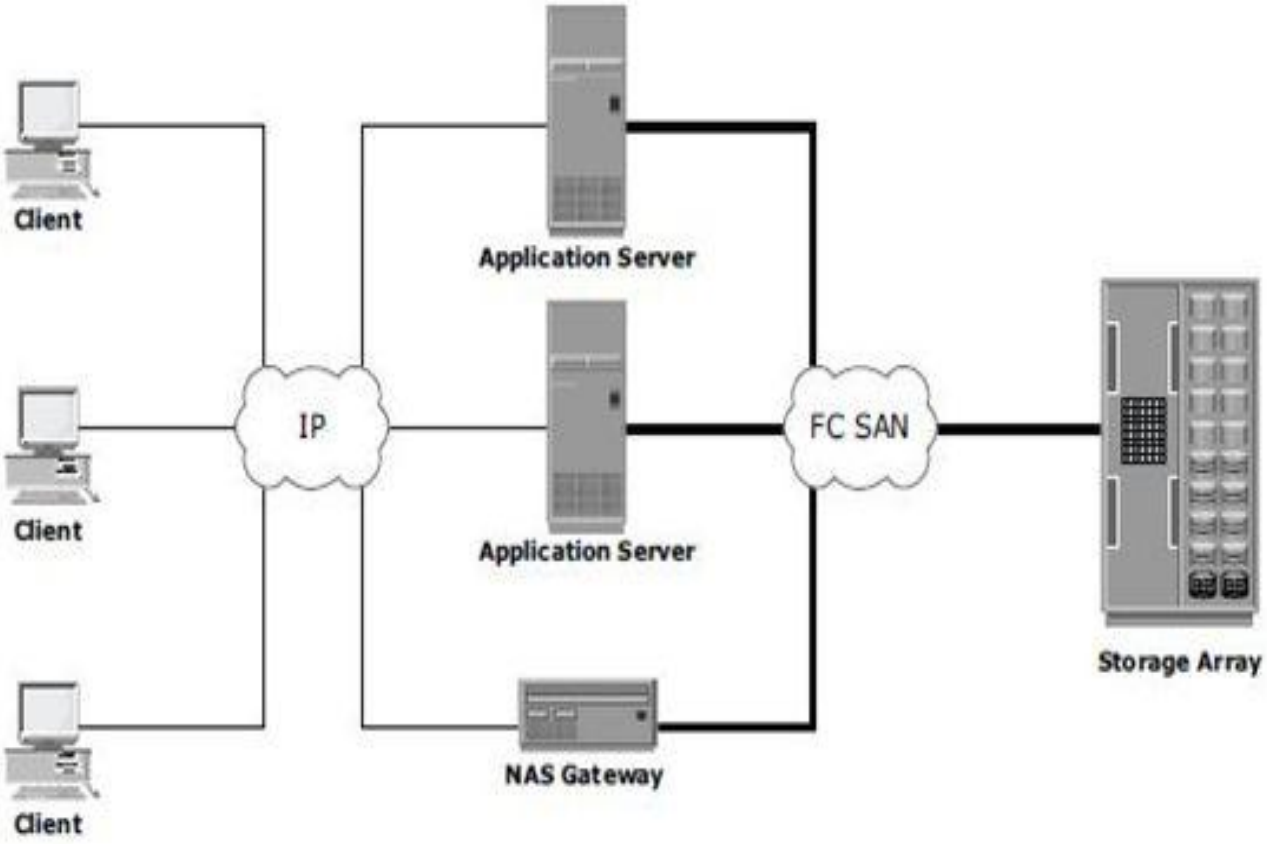


Figure: Gateway NAS connectivity

Scale-Out NAS

Both unified and gateway NAS implementations provide the capability to scale up their resources based on data growth and rise in performance requirements.

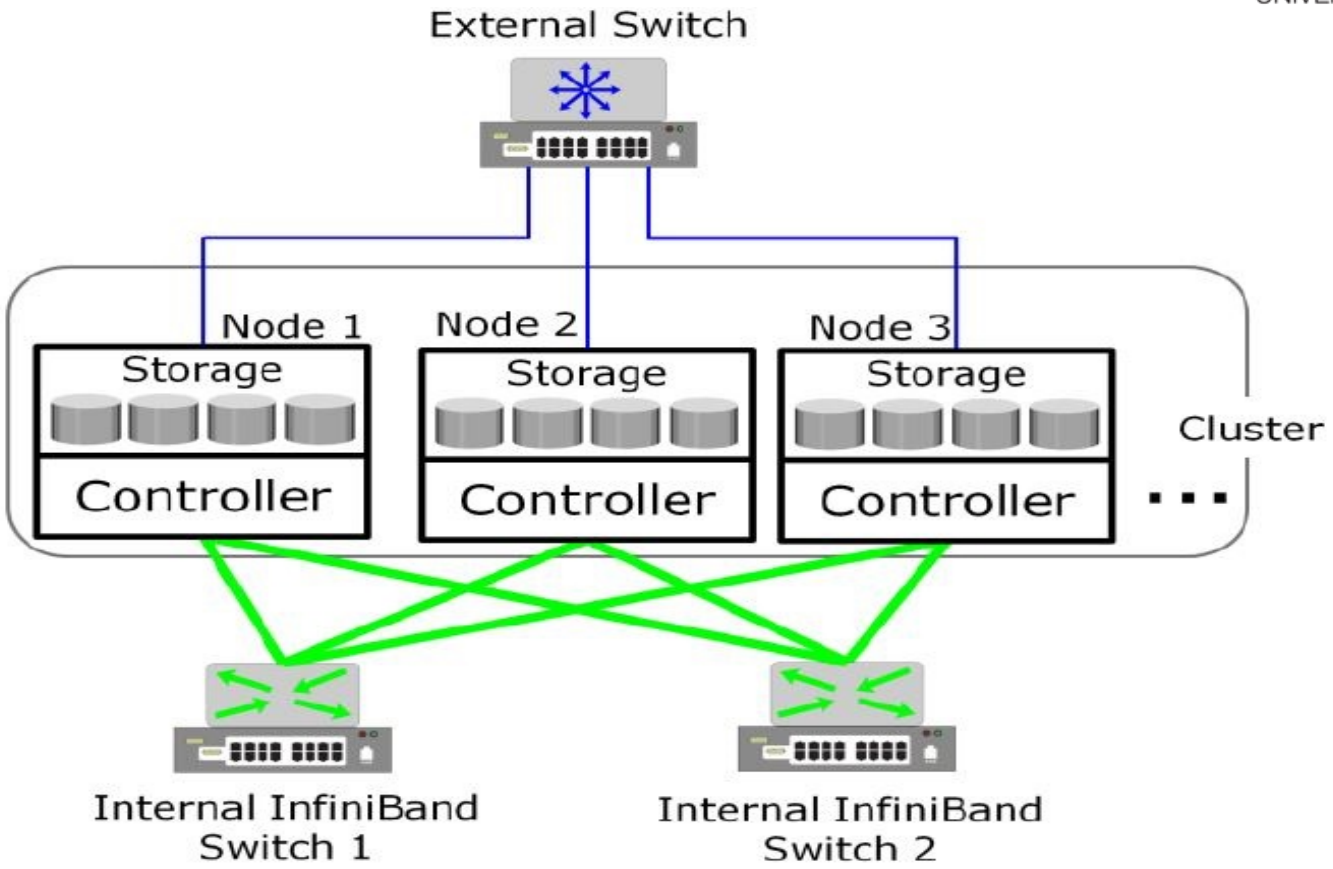
Scaling up these NAS devices involves adding CPUs, memory, and storage to the NAS device.

Scalability is limited by the capacity of the NAS device to house and use additional NAS heads and storage.

Scale-Out NAS Connectivity

Scale-out NAS clusters use separate internal and external networks for back-end and front-end connectivity respectively.

An internal network provides connections for intra cluster communication, and an external network connection enables clients to access and share file data.



Scale-out NAS with dual internal and single external networks

NAS File Sharing Protocols

- NAS devices enable users to share file data across different operating environments and provide a means for users to migrate transparently from one operating system to another.

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

NAS File Sharing Protocols cont….

Three versions of NFS are in use:

NFS version 2 (NFSv2): Uses UDP to provide a stateless network connection between a client and a server. Features, such as locking, are handled outside the protocol.

NFS version 3 (NFSv3): The most commonly used version, which uses UDP or TCP, and is based on the stateless protocol design. It includes some new features, such as a 64-bit file size, asynchronous writes, and additional file attributes to reduce refetching.

NFS version 4 (NFSv4): Uses TCP and is based on a stateful protocol design. It offers enhanced security. The latest NFS version 4.1 is the enhancement of NFSv4 and includes some new features, such as session model, parallel NFS (pNFS), and data retention.

NAS File Sharing Protocols cont….

SRM UNIVERSITY
(Under section 3 of UGC Act 1956)

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.

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 and can automatically restore connections and reopen files that were open prior to an interruption.

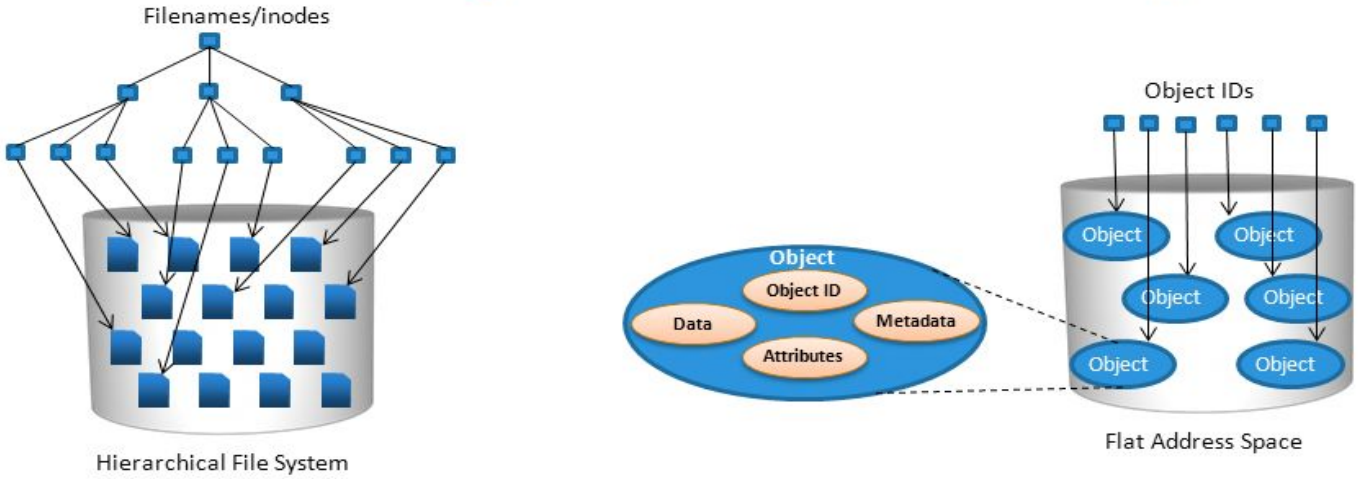
Object-Based Storage Devices

An OSD is a device that organizes and stores unstructured data, such as movies, office documents, and graphics, as objects.

Object-based storage provides a scalable, self-managed, protected, and shared storage option.

OSD stores data in the form of objects. OSD uses flat address space to store data. Therefore, there is no hierarchy of directories and files; as a result, a large number of objects can be stored in an OSD system

Hierarchical File System Vs. Flat Address Space



- Hierarchical file system organizes data in the form of files and directories
- Object-based storage devices store the data in the form of objects
  - It uses flat address space that enables storage of large number of objects
  - An object contains user data, related metadata, and other attributes
  - Each object has a unique object ID, generated using specialized algorithm

Object-Based Storage Architecture

An I/O in the traditional block access method passes through various layers in the I/O path.

The I/O generated by an application passes through the file system, the channel, or network and reaches the disk drive.

When the file system receives the I/O from an application, the file system maps the incoming I/O to the disk blocks.

The block interface is used for sending the I/O over the channel or network to the storage device.

The I/O is then written to the block allocated on the disk drive.

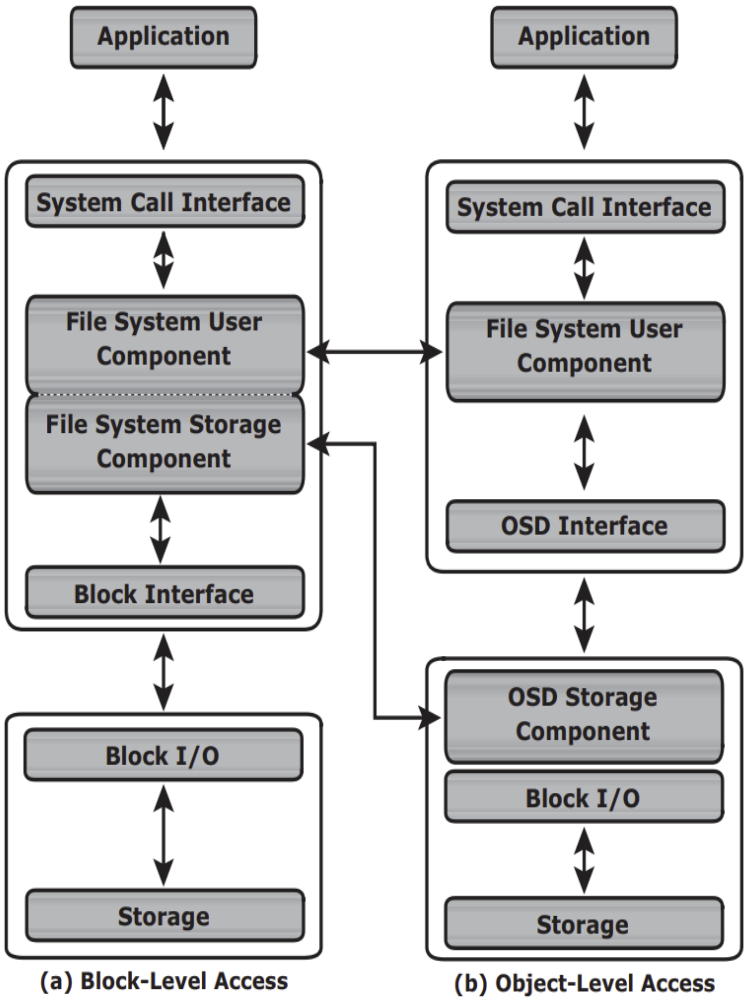


Figure 8-3: Block-level access versus object-level access

Components of OSD

The OSD system is typically composed of three key components:

- nodes
- private network and
- storage.

The OSD system is composed of one or more **nodes**.

A node is a server that runs the OSD operating environment and provides services to store, retrieve, and manage data in the system.

The OSD node has two key services:

- metadata service - The metadata service is responsible for generating the object ID from the contents (and can also include other attributes of data) of a file. It also maintains the mapping of the object IDs and the file system namespace
- storage service - The storage service manages a set of disks on which the user data is stored. The OSD nodes connect to the storage via an internal network.

The internal network provides node-to-node connectivity and node-to-storage connectivity.

The application server accesses the node to store and retrieve data over an external network.

In some implementations, such as CAS, the metadata service might reside on the application server or on a separate server.

OSD typically uses low-cost and high-density disk drives to store the objects. As more capacity is required, more disk drives can be added to the system.

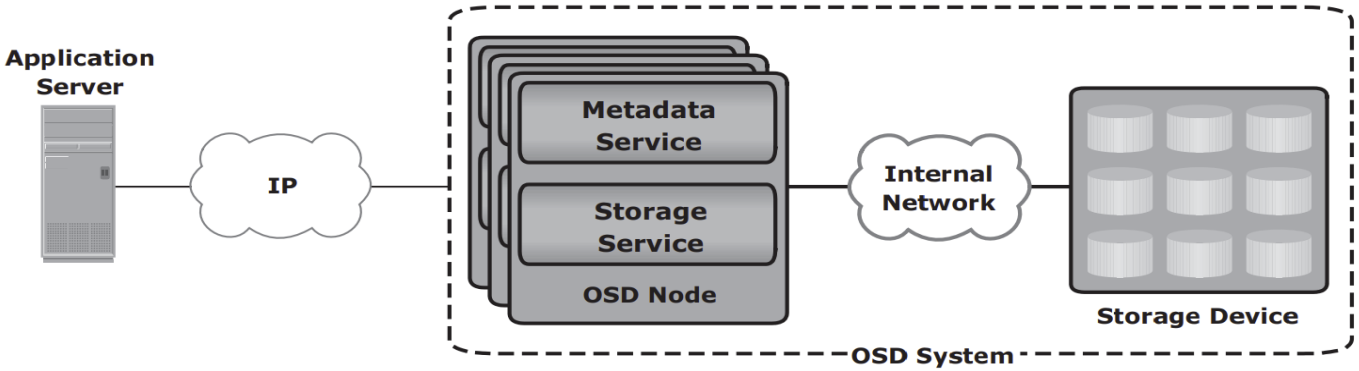


Figure 8-4: OSD components

Object Storage and Retrieval in OSD

The process of storing objects in OSD is illustrated. The data storage process in an OSD system is as follows:

The application server presents the file to be stored to the OSD node.

The OSD node divides the file into two parts: user data and metadata.

The OSD node generates the object ID using a specialized algorithm. The algorithm is executed against the contents of the user data to derive an ID unique to this data.

For future access, the OSD node stores the metadata and object ID using the metadata service.

The OSD node stores the user data (objects) in the storage device using the storage service.

An acknowledgment is sent to the application server stating that the object is stored.

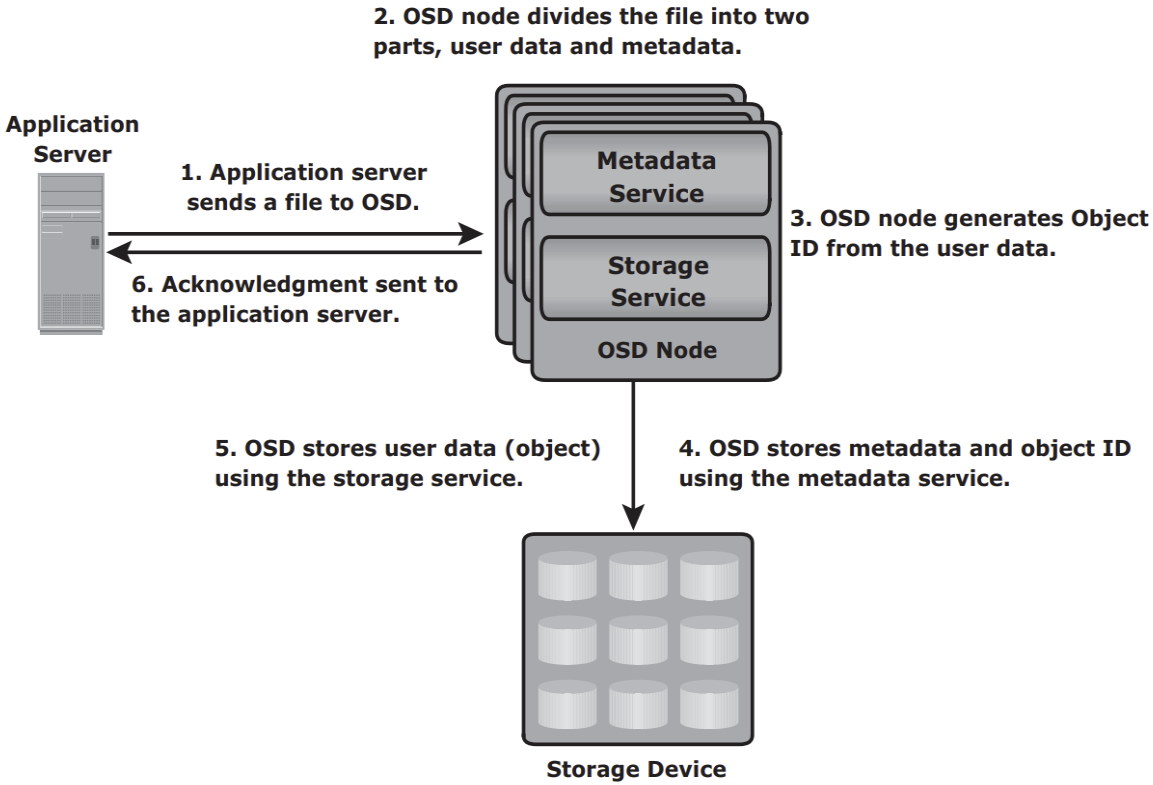


Figure 8-5: Storing objects on OSD

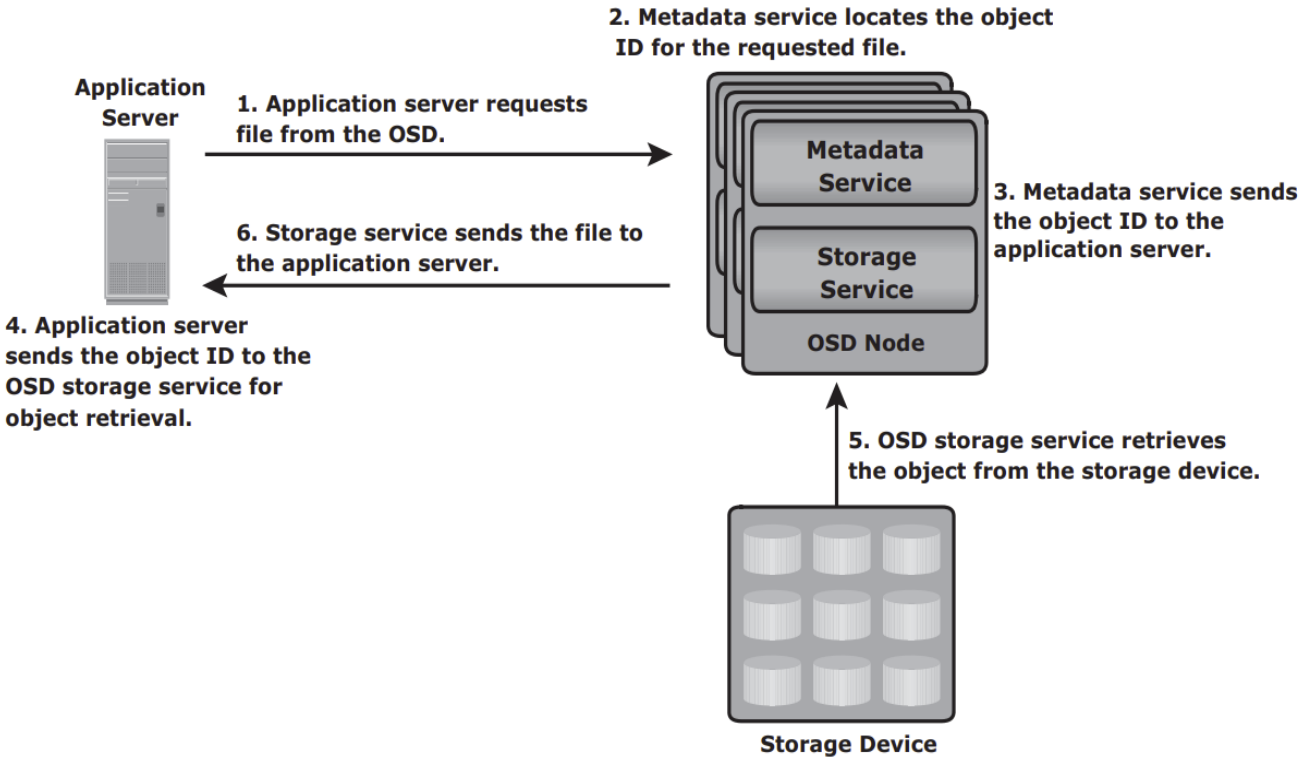


Figure 8-6: Object retrieval from an OSD system

Benefits of Object-Based Storage

Security and reliability: Data integrity and content authenticity are the key features of object-based storage devices. OSD uses specialized algorithms to create objects that provide strong data encryption capability. In OSD, request authentication is performed at the storage device rather than with an external authentication mechanism.

Platform independence: Objects are abstract containers of data, including metadata and attributes. This feature allows objects to be shared across heterogeneous platforms locally or remotely. This platform-independence capability makes object-based storage the best candidate for cloud computing environments.

Scalability: Due to the use of flat address space, object-based storage can handle large amounts of data without impacting performance. Both storage and OSD nodes can be scaled independently in terms of performance and capacity.

Manageability: Object-based storage has an inherent intelligence to manage and protect objects. It uses self-healing capability to protect and replicate objects. Policy-based management capability helps OSD to handle routine jobs automatically.

Content-Addressed Storage

- CAS is an object-based storage device designed for secure online storage and retrieval of fixed content.
- CAS stores user data and its attributes as an object.
- The stored object is assigned a globally unique address, known as a content address (CA).
- This address is derived from the object's binary representation.
- CAS provides an optimized and centrally managed storage solution.
- CAS provides all the features required for storing fixed content. The key features of CAS are as follows:
  - Content authenticity
  - Content integrity
  - Location independence
  - Single-instance storage (SIS)
  - Retention enforcement
  - Data protection

In the remote replication option, data objects are copied to a secondary CAS at the remote location. In this case, the objects remain accessible from the secondary CAS if the primary CAS system fails.

Fast record retrieval: CAS stores all objects on disks, which provides faster access to the objects compared to tapes and optical discs. n Load balancing: CAS distributes objects across multiple nodes to provide maximum throughput and availability.

Scalability: CAS allows the addition of more nodes to the cluster without any interruption to data access and with minimum administrative overhead.

Event notification: CAS continuously monitors the state of the system and raises an alert for any event that requires the administrator's attention. The event notification is communicated to the administrator through SNMP, SMTP, or e-mail.

Self diagnosis and repair: CAS automatically detects and repairs corrupted objects and alerts the administrator about the potential problem. CAS systems can be confi gured to alert remote support teams who can diagnose and repair the system remotely.

Audit trails: CAS keeps track of management activities and any access or disposition of data. Audit trails are mandated by compliance requirements

Configuration and Tracing of FC scan and iSCSI scan

The basic steps to configure a FC setup are as follows:

Configure FC switches. You can configure ports and zones according to the vendor-specific documentation for switches.

Configure storage devices. You can use LUN masking to enable specific LUNs to be seen by specific hosts. For more information about LUN masking, see your vendor-specific storage documentation.

Connect arrays, other storage devices, and Oracle Solaris hosts to a SAN.

Configured FC devices are made available to the host automatically during installation, boot time, and run time.

If a new logical unit is added to a storage device during runtime, the new logical unit is configured automatically only if there is I/O traffic to another logical unit in the same storage device. A logical unit cannot be configured automatically if there is no I/O traffic. You can use the cfgadm command to manually probe the device.

For example:

```
# cfgadm -c configure c3::10000000c94c0cec
```

Configuration and Tracing of FC scan and iSCSI scan

Configuring Authentication in an iSCSI-Based Storage Network

- In a secure environment, authentication for your iSCSI devices is not required because only trusted initiators can access the targets.
- In a less secure environment, the target cannot determine if a connection request is from a given host.
- In this case, the target can authenticate an initiator by using the Challenge-Handshake Authentication Protocol (CHAP).
- CHAP authentication uses the notion of challenge and response, which means that the target challenges the initiator to prove its identity.
- For the challenge and response method to work, the target must know the initiator's secret key, and the initiator must be set up to respond to a challenge.

Configuration and Tracing of FC scan and iSCSI scan

iSCSI supports unidirectional and bidirectional authentication as follows:

Unidirectional authentication enables the target to authenticate the identity of the initiator or the initiator to authenticate the identity of the target.

Bidirectional authentication adds a second level of security by adding authentication on both directions.

You can simplify CHAP secret key management by using a third-party RADIUS server, which acts as a centralized authentication service. When you use RADIUS, the RADIUS server stores the set of node names and matching CHAP secret keys. The system performing the authentication forwards the node name of the requester and the supplied secret of the requester to the RADIUS server. The RADIUS server confirms whether the secret key is the appropriate key to authenticate the given node name.