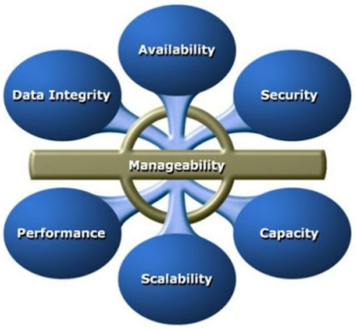
UNIT 1

1) List the characteristics expected of a data center and also list the ways of managing a data center.



Characteristics of DataCenters:

Data integrity: Data integrity refers to mechanisms, such as error correction codes or parity bits, which ensure that data is stored and retrieved exactly as it was received.

Availability: Availability of information as and when required should be ensured. Unavailability of information can severely affect business operations, lead to substantial financial losses, and damage the reputation of an organization.

Security: Policies and procedures should be established, and control measures should be implemented to prevent unauthorized access to and alteration of information.

Scalability: Organizations may need to deploy additional resources such as compute systems, new applications, and databases to meet the growing requirements. Data center resources should scale to meet the changing requirements, without interrupting business operations.

Capacity: Data center operations require adequate resources to efficiently store and process large and increasing amounts of data. When capacity requirements increase, additional capacity should be provided either without interrupting the availability or with minimal disruption. Capacity may be managed by adding new resources or by reallocating existing resources.

Performance: Data center components should provide optimal performance based on the required service levels.

Manageability: A data center should provide easy, flexible, and integrated management of all its components. Efficient manageability can be achieved through automation for reducing manual intervention in common, repeatable tasks.

Managing a Datacenter

Any Datacenter should be properly managed by the organisation to make the business running without disruptions. The activities carried out to ensure the efficient functioning of a data center can be broadly categorized under the following key management processes.

Planning: It is a process of estimating the amount of IT resources required to support business operations and meet the changing resource requirements. Planning leverages the data collected during monitoring and enables improving the overall utilization and performance of resources. It also enables estimation of future resource requirements. Data center managers also determine the impact of incidents and devise contingency plans to resolve them.

Provisioning: It is the process of configuring and allocating the resources that are required to carry out business operations. For example, servers are provisioned to run applications and storage capacity is provisioned to a server. Provisioning primarily includes resource management activities to meet capacity, availability, performance, and security requirements.

Monitoring: It is a continuous process of gathering information on various resources in the data center. The process involves monitoring parameters such as configuration, availability, capacity, performance, and security of resources.

Maintenance: It is a set of standard repeatable activities for operating the data center. It involves ensuring the proper functioning of resources and resolving incidents such as malfunctions, outages, and equipment loss. It also involves handling identified problems or issues within the data center and incorporating changes to prevent future problem occurrence.

Reporting: It is a process of collating and presenting the monitored parameters such as resource performance, capacity, and utilization of resources. Reporting enables data center managers to analyze and improve the utilization of data center resources and identify problems. It also helps in establishing business justifications and chargeback of costs associated with data center operations.

2) Explain the interface protocols of host to storage for communications.

Integrated Device Electronics (IDE)/Advanced Technology Attachment (ATA): It is a popular interface protocol standard used for connecting storage devices, such as disk drives and optical drives. This protocol supports parallel transmission and therefore is also known as Parallel ATA (PATA) or simply ATA.

IDE/ATA has a variety of standards and names. In a master-slave configuration, an ATA interface supports two storage devices per connector. However, if the performance of the drive is important, sharing a port between two devices is not recommended.

Serial ATA (SATA): The serial version of this protocol supports single bit serial transmission and is known as Serial ATA (SATA). High performance and low cost SATA has largely replaced PATA in the newer systems. SATA revision 3.2 provides a data transfer rate up to 16 Gb/s.

Small Computer System Interface (SCSI): SCSI has emerged as a preferred connectivity protocol in high-end servers. This protocol supports parallel transmission and offers improved performance, scalability, and compatibility compared to ATA. However, the high cost associated with SCSI limits its popularity among home or personal desktop users. Over the years, SCSI has been enhanced and now includes a wide variety of related technologies and standards. SCSI supports up to 16 devices on a single bus and provides data transfer rates up to 640 MB/s.

Serial attached SCSI (SAS): It is a point-to-point serial protocol that provides an alternative to parallel SCSI. A newer version (SAS 3.0) of serial SCSI supports a data transfer rate up to 12 Gb/s.

Fibre Channel (FC): Fibre Channel is a widely-used protocol for high-speed communication to the storage device. The Fibre Channel interface provides gigabit network speed. It provides a serial data transmission that operates over copper wire and optical fiber. The latest version of the FC interface '16FC' allows transmission of data up to 16 Gb/s.

Internet Protocol (IP): IP is a network protocol that has been traditionally used for server-to-server traffic. With the emergence of new technologies, an IP network has become a viable option for server-to-storage communication. IP offers several advantages in terms of cost and maturity and enables organizations to leverage their existing IP-based network. iSCSI and FCIP protocols are common examples that leverage IP for server-to-storage communication.

3) Explain the concept of Host Access to Data.

Data is accessed and stored by applications using the underlying infrastructure.

The key components of this infrastructure are the **operating system** (or file system), **connectivity**, and **storage**.

The storage device can be **internal** and (or) **external** to the host. In either case, the host controller card accesses the storage devices using predefined protocols, such as IDE/ATA, SCSI, or Fibre Channel (FC).

IDE/ATA and SCSI are popularly used in small and personal computing environments for accessing internal storage. FC and iSCSI protocols are used for accessing data from an external storage device (or subsystems).

External storage devices can be connected to the host directly or through the storage network. When the storage is connected directly to the host, it is referred as direct-attached storage (DAS), which is detailed later in this chapter. Understanding access to data over a network is important because it lays the foundation for storage networking technologies.

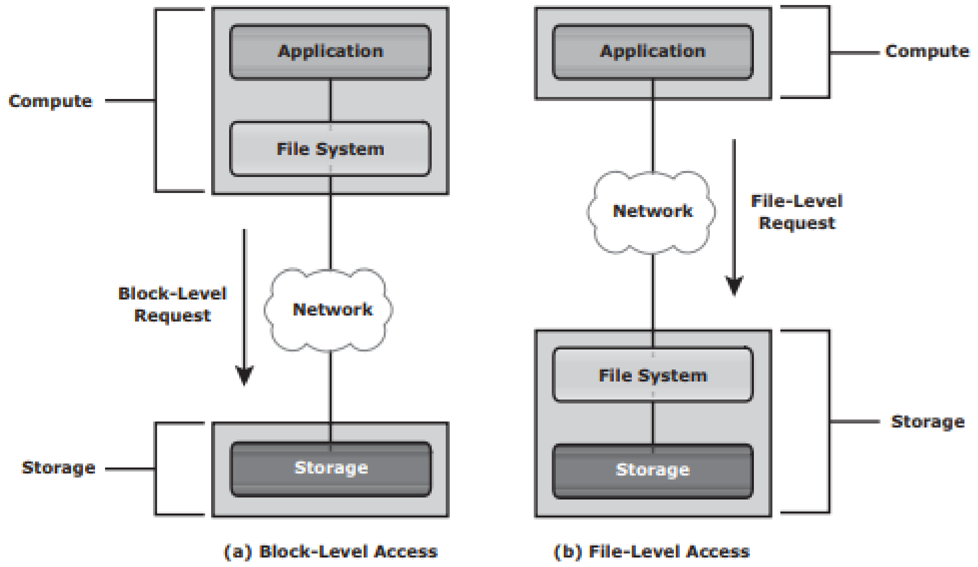
Data can be accessed over a network in one of the following ways: **block level, file level, or object level.** In general, the application requests data from the file system (or operating system) by specifying the filename and location.

The file system maps the file attributes to the logical block address of the data and sends the request to the storage device.

The storage device converts the logical block address (LBA) to a cylinder-head-sector (CHS) address and fetches the data. In a block-level access, the file system is created on a host, and data is accessed on a network at the block level,

as shown in Figure (a). In this case, raw disks or logical volumes are assigned to the host for creating the file system. In a file-level access, the file system is created on a separate file server or at the storage side, and the file-level request is sent over a network,

as shown in Figure (b). Because data is accessed at the file level, this method has higher overhead, as compared to the data accessed at the block level. Object-level access is an intelligent evolution, whereby data is accessed over a network in terms of self-contained objects with a unique object identifier. Details of storage networking technologies and deployments are covered in Section II of this book, "Storage Networking Technologies."



4) Justify, zone bit recording in modern disks, write leveling in flash drives, also the need for queue optimization while writing to disk, cache valuating.

Cache vaulting — The process of dumping the contents of cache into a dedicated set of physical disks during a power failure.

Queue: The location where an I/O request waits before it is processed by the I/O controller.

Disk I/O Controller: Processes I/Os waiting in the queue one by one

Average response time (TR) = Service time (TS) / (1 – Utilization)

5) Discuss the two types of Direct –Attached Storage.

DAS is an acronym of **Direct Attached Storage** and is a storage system where servers are directly connected to the storage device. In DAS, **block-level access protocol** is used to access data by applications.

Some of the examples of Direct Attached Storage (DAS) are **tape libraries, directly connected external hard disk, internal HDD of server**, etc. Even home personal computers have direct-attach storage in the form of internal HDD.

Type of Direct Attached Storage (DAS)

Direct Attached Storage (DAS) is classified into 2 types viz. **Internal DAS or External DAS**. This classification is done on the **basis of the location of the storage device**.

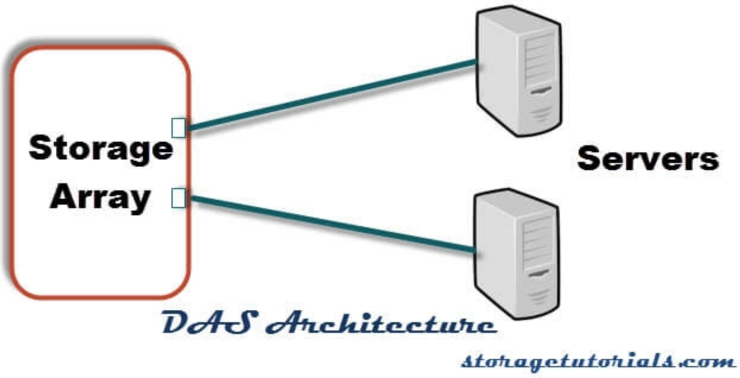
Internal DAS

In internal DAS design, **the storage device is internally connected to the server** by a serial or parallel bus. For high-speed connectivity over a shorter distance, a physical bus is used and this is also one of the disadvantages of the physical bus.

Also, most internal buses can support only a limited number of devices, and they occupy a large amount of space inside the server, making maintenance of other components difficult.

External DAS

In external DAS design, **the server is associated directly to the external storage device**. In most cases, the connection between the server and the storage device happens over Small Computer System Interface (SCSI) or Fibre Channel protocol (FCP).



External das

6) Explain various parameters that effect the disk performance.

Disk Service Time

Disk service time is the time taken by a disk to complete an I/O request. Components that contribute to the service time on a disk drive are **seek time, rotational latency, and data transfer rate.**

Seek Time

The seek time (also called access time) describes the time taken to position the R/W heads across the platter with a radial movement (moving along the radius of the platter). Therefore, the lower the seek time, the faster the I/O operation. Disk vendors publish the following seek time specifi cations:

- ➔ **Full Stroke**: The time taken by the R/W head to move across the entire width of the disk, from the innermost track to the outermost track.
- ➔ **Average**: The average time taken by the R/W head to move from one random track to another, normally listed as the time for one-third of a full stroke.
- ➔ **Track-to-Track**: The time taken by the R/W head to move between adjacent tracks. Each of these specifi cations is measured in milliseconds.

Rotational Latency

To access data, the actuator arm moves the R/W head over the platter to a particular track while the platter spins to position the requested sector under the R/W head. The time taken by the platter to rotate and position the data under the R/W head is called rotational latency.

This latency depends on the rotation speed of the spindle and is measured in milliseconds. The average rotational latency is one-half of the time taken for a full rotation.

Similar to the seek time, rotational latency has more impact on the reading/writing of random sectors on the disk than on the same operations on adjacent sectors.

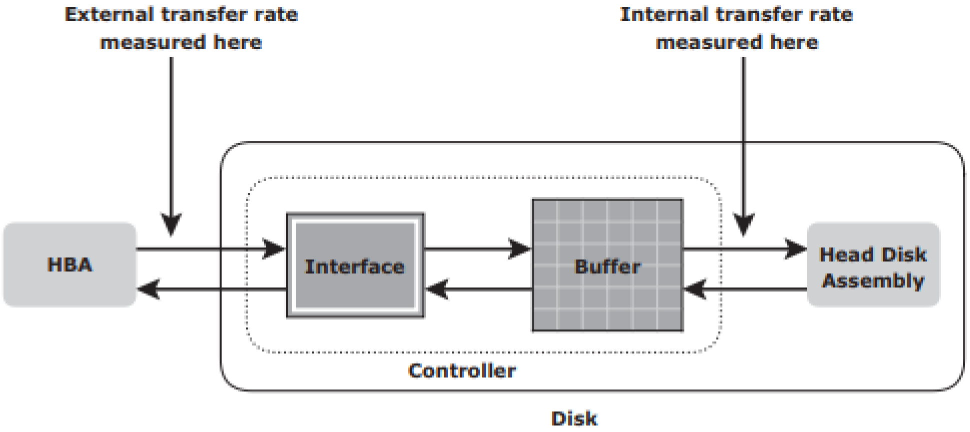
Average rotational latency for a 15,000 rpm (or 250 rps)

drive = 0.5/250 = 2 milliseconds.

Data Transfer Rate

The data transfer rate (also called transfer rate) refers to the average amount of data per unit time that the drive can deliver to the HBA. It is important to first understand the process of read/write operations to calculate data transfer rates.

In a read operation, the data first moves from disk platters to R/W heads; then it moves to the drive's internal buffer. Finally, data moves from the buffer through the interface to the host HBA.


External transfer rate measured here
Internal transfer rate measured here
HBA
Interface
Buffer
Head Disk Assembly
Controller
Disk

Disk I/O Controller Utilization

Utilization of a disk I/O controller has a significant impact on the I/O response time.

Queue: The location where an I/O request waits before it is processed by the I/O controller

Disk I/O Controller: Processes I/Os waiting in the queue one by one

The I/O requests arrive at the controller at the rate generated by the application. This rate is also called the arrival rate.

These requests are held in the I/O queue, and the I/O controller processes them one by one, as The I/O arrival rate, the queue length, and the time taken by the I/O controller to process each request determines the I/O response time. If the controller is busy or heavily utilized, the queue size will be large and the response time will be high.

7) List different data formats in which data delusion is taking place.

The data center infrastructure includes **hardware** components, such as computers, storage systems, network devices, and power backups,

software components, such as applications, operating systems, and management software. It also includes environmental controls, such as air conditioning, fire suppression, and ventilation.

8) Calculate the number of disks required for an application given that the application requires 4000 IOPS and storage of 3.0Tbytes. Physical disk that is available is of 120 IOPS and storage capacity of 140 GB also consider utilisation at 70% Explain disk latency and throughput.

the number of disks required to meet the capacity requirements will be

3 TB/140 GB = 22 disks.

To meet the application IOPS requirements, the number of disks required is 4,000/120 = 33.33 ❑≡❑ 33

the number of IOPS a disk drive can perform should be calculated based on 70- percent disk utilization.

Considering this, the number of IOPS a disk can perform at 70 percent utilization is 120 * 0.7 = 84 IOPS. Therefore,

the number of disks required to meet the application IOPS requirement will be 4,000/84 = 48

As a result, the number of disks required to meet the application requirements will be

Max (22, 48) = 48 disks

9) Discuss hot spare disks and their utility.

A hot spare refers to a spare drive in a RAID array that temporarily replaces a failed disk drive by taking the identity of the failed disk drive. With the hot spare, one of the following methods of data recovery is performed depending on the RAID implementation:

➔ If parity RAID is used, the data is rebuilt onto the hot spare from the parity and the data on the surviving disk drives in the RAID set.

➔ If mirroring is used, the data from the surviving mirror is used to copy the data onto the hot spare.

When a new disk drive is added to the system, data from the hot spare is copied to it. The hot spare returns to its idle state, ready to replace the next failed drive. Alternatively, the hot spare replaces the failed disk drive permanently. This means that it is no longer a hot spare, and a new hot spare must be configured on the array

A hot spare should be large enough to accommodate data from a failed drive. Some systems implement multiple hot spares to improve data availability.

UNIT 2

10) Describe techniques used by Raid levels for achieving redundancy and increasing disk performance.

LEVELS	BRIEF DESCRIPTION
RAID 0	Striped set with no fault tolerance
RAID 1	Disk mirroring
Nested	Combinations of RAID levels. Example: RAID 1 + RAID 0
RAID 3	Striped set with parallel access and a dedicated parity disk
RAID 4	Striped set with independent disk access and a dedicated parity disk

RAID 5	Striped set with independent disk access and distributed parity
RAID 6	Striped set with independent disk access and dual distributed parity

11) Calculate the number of disks required for an application given that the application requires 3800 IOPS and storage of 3.0Tbytes. Physical disk that is available is of 140 IOPS and storage capacity of 140 GB? The application requires Raid 6 to be implemented and assume that no of reads are 60% of the total IOPS required by the application? Also assume the optimum utilization level of disk is 70%.

the number of disks 3 TB/140 GB = 22 disks.

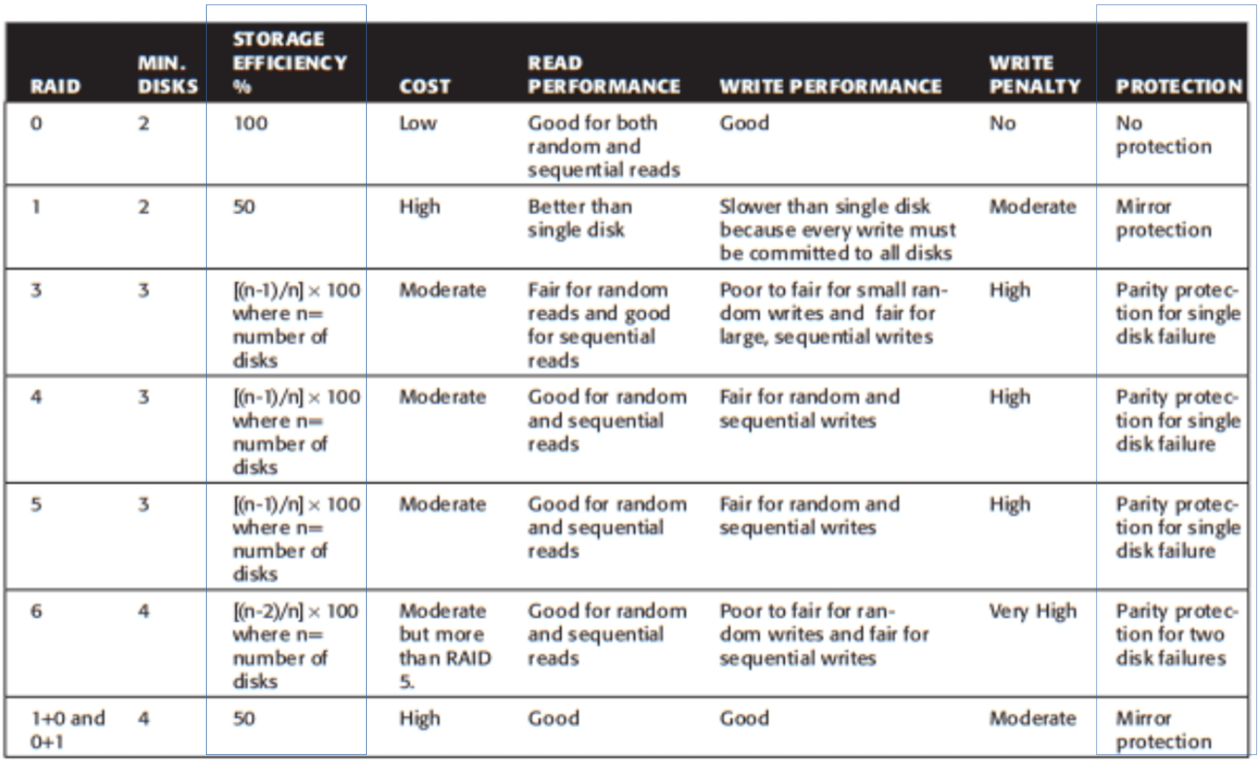
the number of disks required is 3,800/140 = 27

the number of IOPS a disk can perform at 70 percent utilization is 140 * 0.7 = 98 IOPS.

the number of disks required to meet the application IOPS requirement will be 3,800/98 = 39

Max (22, 39) = 39 disks

12) State the number of disks, parity information, write penalties of different Raid levels.



RAID	MIN. DISKS	STORAGE EFFICIENCY %	COST	READ PERFORMANCE	WRITE PERFORMANCE	WRITE PENALTY	PROTECTION
0	2	100	Low	Good for both random and sequential reads	Good	No	No protection
1	2	50	High	Better than single disk	Slower than single disk because every write must be committed to all disks	Moderate	Mirror protection
3	3	[(n-1)/n] × 100 where n= number of disks	Moderate	Fair for random reads and good for sequential reads	Poor to fair for small random writes and fair for large, sequential writes	High	Parity protection for single disk failure
4	3	[(n-1)/n] × 100 where n= number of disks	Moderate	Good for random and sequential reads	Fair for random and sequential writes	High	Parity protection for single disk failure
5	3	[(n-1)/n] × 100 where n= number of disks	Moderate	Good for random and sequential reads	Fair for random and sequential writes	High	Parity protection for single disk failure
6	4	[(n-2)/n] × 100 where n= number of disks	Moderate but more than RAID 5.	Good for random and sequential reads	Poor to fair for random writes and fair for sequential writes	Very High	Parity protection for two disk failures
1+0 and 0+1	4	50	High	Good	Good	Moderate	Mirror protection

Parity is a method to protect striped data from disk drive failure without the cost of mirroring.

13) Examine the various cache algorithms used for writing and for flushing of cache.

The most commonly used algorithms are discussed in the following list:

Least Recently Used (LRU): An algorithm that continuously monitors data access in cache and identifies the cache pages that have not been accessed for a long time. LRU either frees up these pages or marks them for reuse. This algorithm is based on the assumption that data that has not been accessed for a while will not be requested by the host. However, if a page contains write data that has not yet been committed to disk, the data is first written to disk before the page is reused.

Most Recently Used (MRU): This algorithm is the opposite of LRU, where the pages that have been accessed most recently are freed up or marked for reuse. This algorithm is based on the assumption that recently accessed data may not be required for a while.

The cache utilization level, drives the mode of flushing to be used:

Idle flushing: Occurs continuously, at a modest rate, when the cache utilization level is between the high and low watermark.

High watermark flushing: Activated when cache utilization hits the high watermark. The storage system dedicates some additional resources for flushing. This type of flushing has some impact on I/O processing.

Forced flushing: Occurs in the event of a large I/O burst when cache reaches 100 percent of its capacity, which significantly affects the I/O response time. In forced flushing, system flushes the cache on priority by allocating more resources.

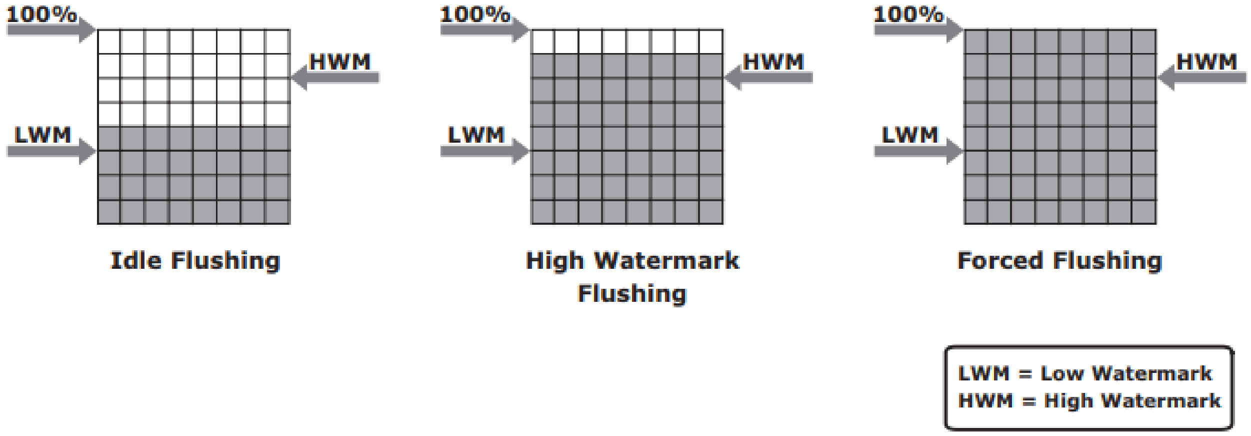


Figure 4-4: Types of flushing

14) State difference between traditional provisiong and virtual provisioning with a neat diagram.

Administrators typically allocate storage capacity based on anticipated storage requirements.

This generally results in the over provisioning of storage capacity, which then leads to higher costs and lower capacity utilization. Administrators often over-provision storage to an application for various reasons, such as, to avoid frequent provisioning of storage if the LUN capacity is exhausted, and to reduce disruption to application availability.

Over provisioning of storage often leads to additional storage acquisition and operational costs. Virtual provisioning addresses these challenges. Virtual provisioning improves storage capacity utilization and simplifies storage management. Figure 4-9 shows an example, comparing virtual provisioning with traditional storage provisioning.

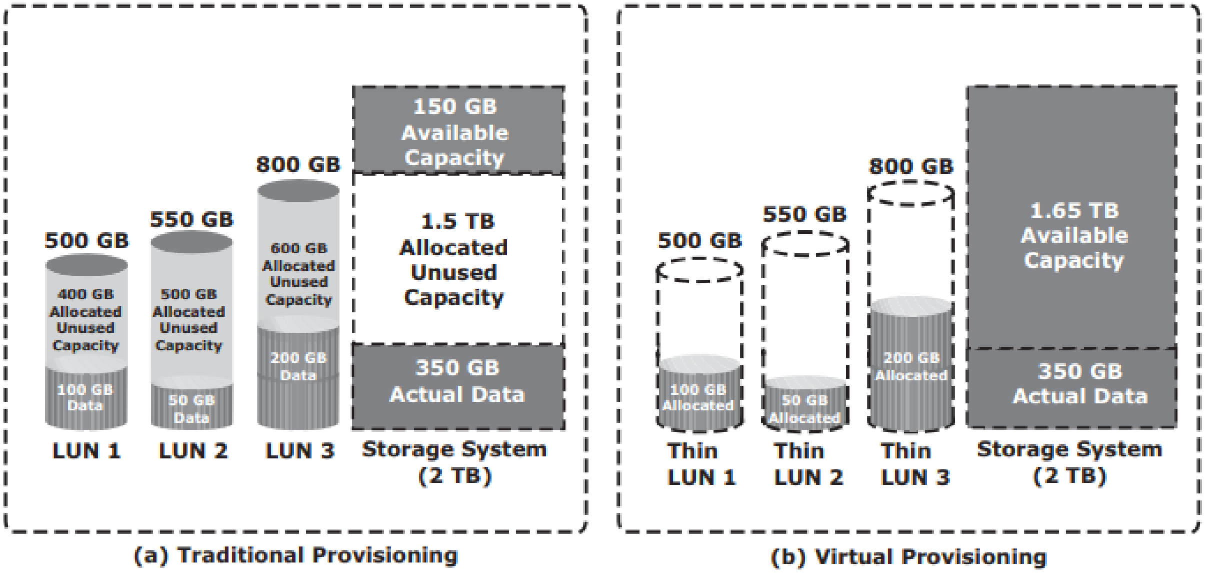


Figure 4-9: Traditional versus virtual provisioning

With traditional provisioning, three LUNs are created and presented to one or more hosts (see Figure 4-9 [a]). The total storage capacity of the storage system is 2 TB. The allocated capacity of LUN 1 is 500 GB, of which only 100 GB is consumed, and the remaining 400 GB is unused. The size of LUN 2 is 550 GB, of which 50 GB is consumed, and 500 GB is unused. The size of LUN 3 is 800 GB, of which 200 GB is consumed, and 600 GB is unused. In total, the storage system has 350 GB of data, 1.5 TB of allocated but unused capacity, and only 150 GB of remaining capacity available for other applications.

Now consider the same 2 TB storage system with virtual provisioning (see Figure 4-9 [b]). Here, three thin LUNs of the same sizes are created. However, there is no allocated unused capacity. In total, the storage system with virtual provisioning has the same 350 GB of data, but 1.65 TB of capacity is available for other applications, whereas only 150 GB is available in traditional storage provisioning

15) Discuss MetaLUN and Lun Masking.

MetaLUN is a method to expand LUNs that require additional capacity or performance. A metaLUN can be created by combining two or more LUNs.

A metaLUN consists of a base LUN and one or more component LUNs. MetaLUNs can be either concatenated or striped. Concatenated expansion simply adds additional capacity to the base LUN. In this expansion, the component LUNs are not required to be of the same capacity as the base LUN. All LUNs in a concatenated metaLUN must be either protected (parity or mirrored) or unprotected (RAID 0). RAID types within a metaLUN can be mixed. For example, a RAID 1/0 LUN can be concatenated with a RAID 5 LUN. However, a RAID 0 LUN can be concatenated only with another RAID 0 LUN. Concatenated expansion is quick but does not provide any performance benefit.

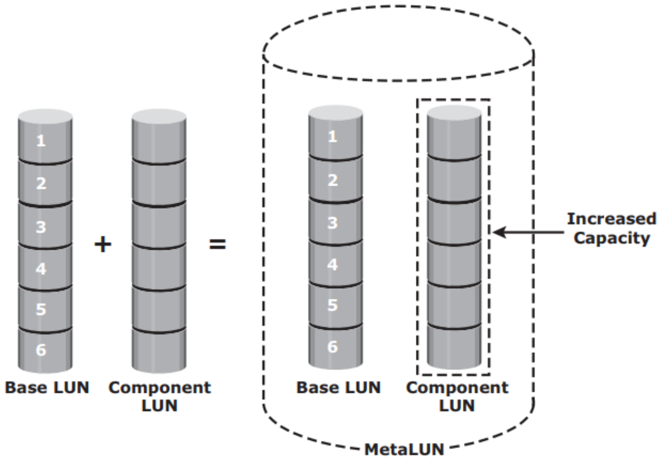


Figure 4-6: Concatenated metaLUN

Striped expansion restripes the base LUN's data across the base LUN and component LUNs. In striped expansion, all LUNs must be of the same capacity and RAID level. Striped expansion provides improved performance due to the increased number of drives being striped

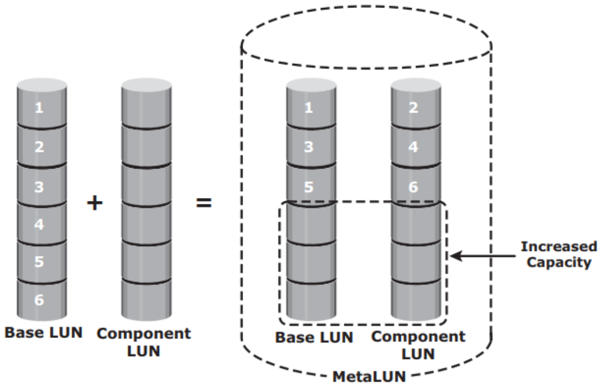


Figure 4-7: Striped metaLUN

LUN masking is a process that provides data access control by defining which LUNs a host can access. The LUN masking function is implemented on the storage array. This ensures that volume access by hosts is controlled appropriately, preventing unauthorized or accidental use in a shared environment. For example, consider a storage array with two LUNs that store data of the sales and finance departments. Without LUN masking, both departments can easily see and modify each other's data, posing a high risk to data integrity and security. With LUN masking, LUNs are accessible only to the designated hosts.

UNIT 3

16) Discuss the various components of the FC - SAN network.

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

In a Fibre Channel network, the end devices, such as hosts, storage arrays, and tape libraries, are all referred to as nodes. Each node is a source or destination of information. Each node requires one or more ports to provide a physical interface for communicating with other nodes.

Cables and Connectors SAN

implementations use optical fiber cabling. Copper can be used for shorter distances for back-end connectivity because it provides an acceptable signal-tonoise ratio for distances up to 30 meters.

Optical fiber cables carry data in the form of light. There are two types of optical cables: multimode and single-mode. Multimode fiber (MMF) cable carries multiple beams of light projected at different angles simultaneously onto the core of the cable.

Interconnect Devices

FC hubs, switches, and directors are the interconnect devices commonly used in FC SAN.

- ➔ Hubs are used as communication devices in FC-AL implementations. Hubs physically connect nodes in a logical loop or a physical star topology.
- ➔ Switches are more intelligent than hubs and directly route data from one physical port to another
- ➔ Directors are high-end switches with a higher port count and better faulttolerance capabilities.

SAN Management Software

SAN management software manages the interfaces between hosts, interconnect devices, and storage arrays. The software provides a view of the SAN environment and enables management of various resources from one central console.

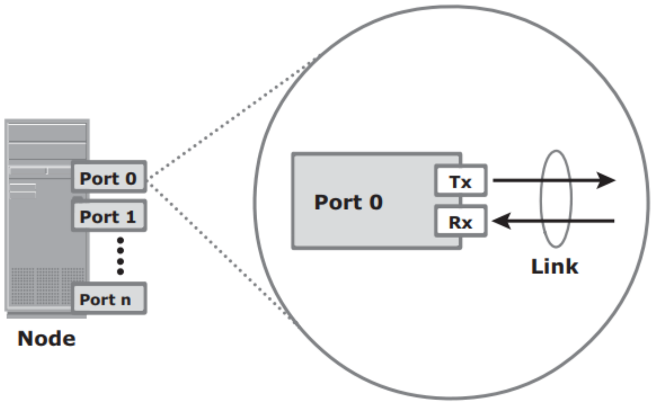


Figure 5-3: Nodes, ports, and links

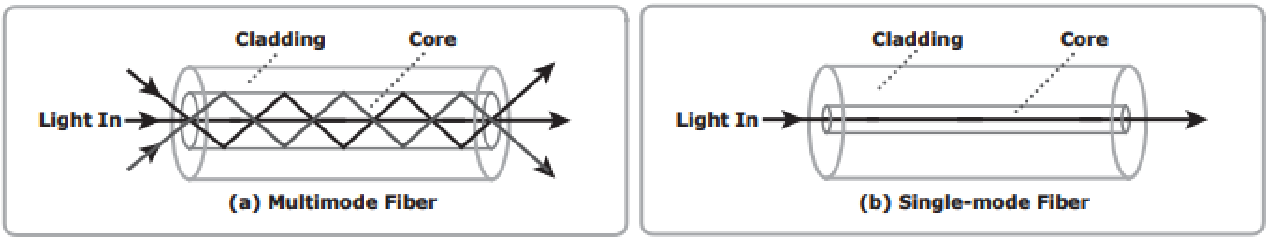


Figure 5-4: Multimode fiber and single-mode fiber

17) List and explain the different types of switched fabric ports.

Switched Fabric Ports

Ports in a switched fabric can be one of the following types:

N_Port: An end point in the fabric. This port is also known as the node port. Typically, it is a host port (HBA) or a storage array port connected to a switch in a switched fabric.

E_Port: A port that forms the connection between two FC switches. This port is also known as the expansion port. The E_Port on an FC switch connects to the E_Port of another FC switch in the fabric through ISLs.

F_Port: A port on a switch that connects an N_Port. It is also known as a fabric port.

G_Port: A generic port on a switch that can operate as an E_Port or an F_Port and determines its functionality automatically during initialization.

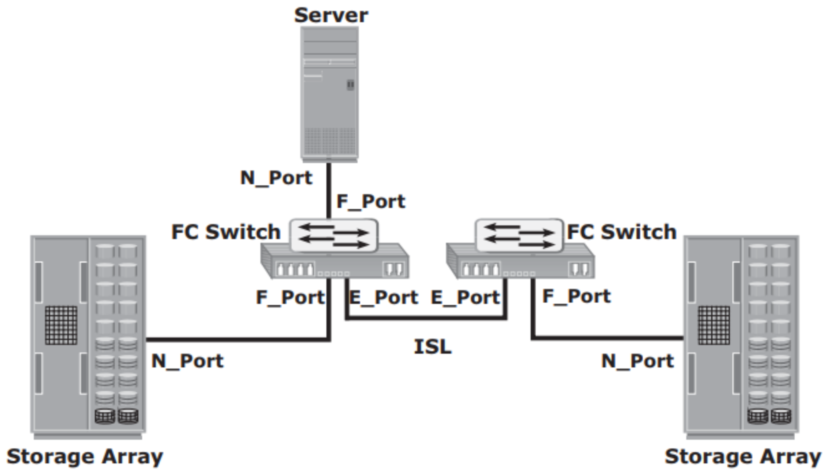


Figure 5-11: Switched fabric ports

18) Describe the application of iSCSI, FCIP and FCOE protocols.

ISCSI

- ➔ Server and storage consolidation.
- ➔ Accelerated Backup Operations.
- ➔ Seamless Remote Site Access and Storage Outsourcing.
- ➔ Network Storage Services via iSCSI.
- ➔ Multiple Cards to Single iSCSI Router.
- ➔ iSCSI HBA and Fibre Channel Tape Backup.

FCIP

19) Explain briefly how the FC architecture supports three basic interconnectivity.

Point-to-Point

Point-to-point is the simplest FC confi guration — two devices are connected directly to each other, as shown. This confi guration provides a dedicated connection for data transmission between nodes.

the point-to-point confi guration offers limited connectivity, because only two devices can communicate with each other at a given time. Moreover, it cannot be scaled to accommodate a large number of nodes. Standard DAS uses point-to-point connectivity.

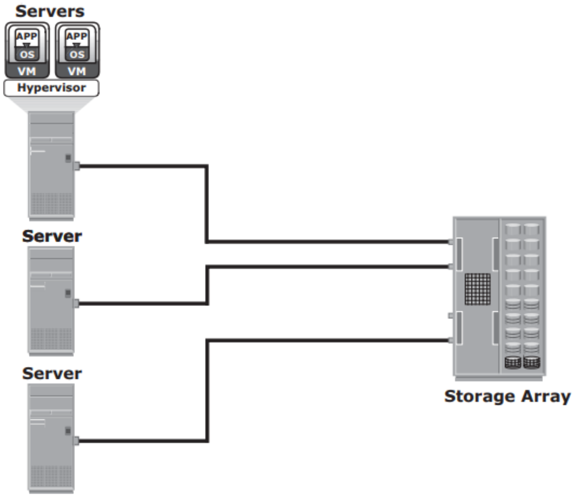


Figure 5-6: Point-to-point connectivity

Fibre Channel Arbitrated Loop

In the FC-AL confi guration, devices are attached to a shared loop. FC-AL has the characteristics of a token ring topology and a physical star topology. In FC-AL, each device contends with other devices to perform I/O operations. Devices on the loop must "arbitrate" to gain control of the loop. At any given time, only one device can perform I/O operations on the loop.

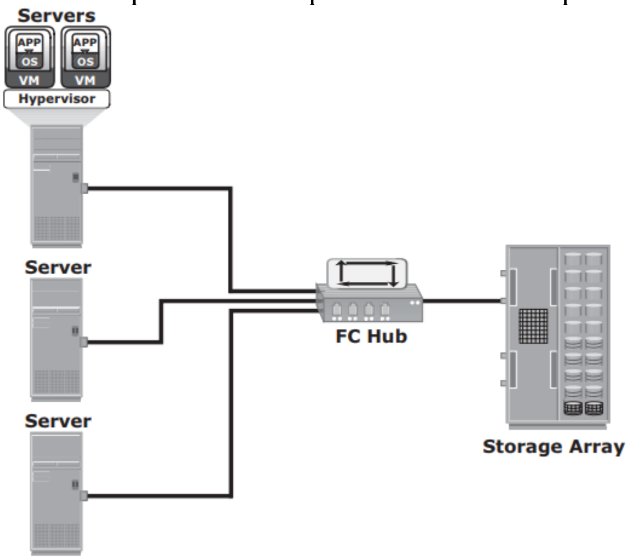


Figure 5-7: Fibre Channel Arbitrated Loop

Fibre Channel Switched Fabric

Unlike a loop confi guration, a Fibre Channel switched fabric (FC-SW) 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 traffi c between other devices. FC-SW is also referred to as

fabric connect. A fabric is a logical space in which all nodes communicate with one another in a network.

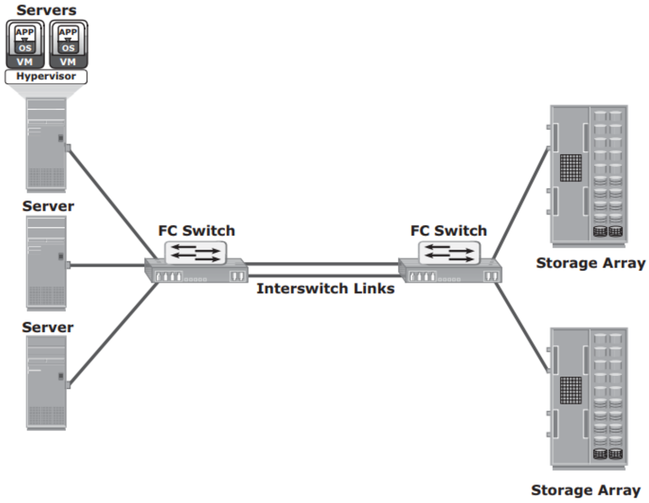


Figure 5-8: Fibre Channel switched fabric

20) With neat diagram, explain block-level storage virtualization.

➔ Block-level storage virtualization aggregates block storage devices (LUNs) and enables provisioning of virtual storage volumes, independent of the underlying physical storage.

➔ Virtual volumes are created from the storage pool and assigned to the hosts.

➔ Instead of being directed to the LUNs on the individual storage arrays, the hosts are directed to the virtual volumes provided by the virtualization layer.

➔ For hosts and storage arrays, the virtualization layer appears as the target and initiator devices, respectively.

➔ The virtualization layer maps the virtual volumes to the LUNs on the individual arrays.

➔ The hosts remain unaware of the mapping operation and access the virtual volumes as if they were accessing the physical storage attached to them.

➔ Typically, the virtualization layer is managed via a dedicated virtualization appliance to which the hosts and the storage arrays are connected.

➔ Block-level storage virtualization enables extending the storage volumes online to meet application growth requirements. It consolidates heterogeneous storage arrays and enables transparent volume access.

➔ Block-level storage virtualization also provides the advantage of non disruptive data migration With a block-level virtualization solution in place, the virtualization layer handles the back-end migration of data, which enables LUNs to remain online and accessible while data is migrating.

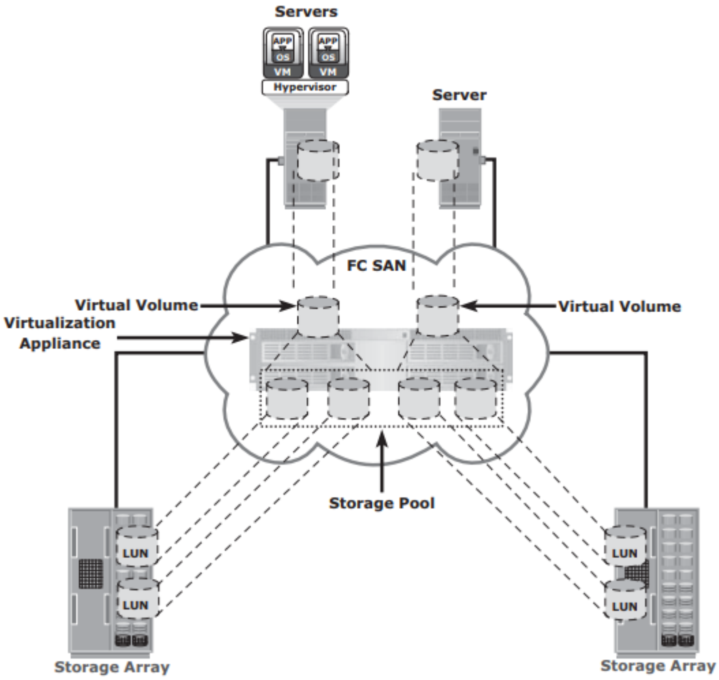


Figure 5-24: Block-level storage virtualization

21) Explain Zoning and their variants.

Zoning is an FC switch function that enables node ports within the fabric to be logically segmented into groups and to communicate with each other within the group.

Whenever a change takes place in the name server database, the fabric controller sends a Registered State Change Notifi cation (RSCN) to all the nodes impacted by the change. If zoning is not confi gured, the fabric controller sends an RSCN to all the nodes in the fabric. Involving the nodes that are not impacted by the change results in increased fabric-management traffic.

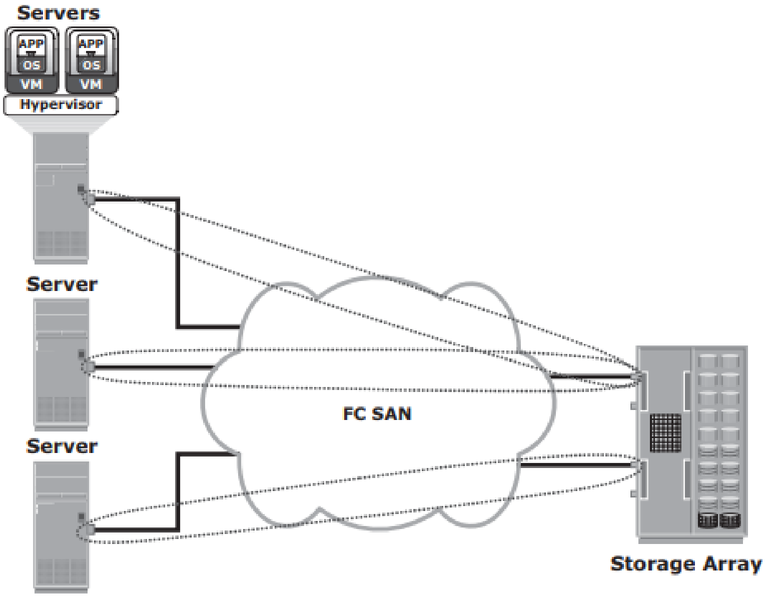


Figure 5-17: Zoning

➔ **Port zoning**: Uses the physical address of switch ports to define zones. In port zoning, access to node is determined by the physical switch port to which a node is connected. The zone members are the port identifier (switch domain ID and port number) to which HBA and its targets (storage devices) are connected. If a node is moved to another switch port in the fabric, then zoning must be modified to allow the node, in its new port, to participate in its original zone.

➔ **WWN zoning:** Uses World Wide Names to define zones. The zone members are the unique WWN addresses of the HBA and its targets (storage devices). A major advantage of WWN zoning is its flexibility. WWN zoning allows nodes to be moved to another switch port in the fabric and maintain connectivity to its zone partners without having to modify the zone configuration. This is possible because the WWN is static to the node port.

➔ **Mixed zoning:** Combines the qualities of both WWN zoning and port zoning. Using mixed zoning enables a specific node port to be tied to the WWN of another node.

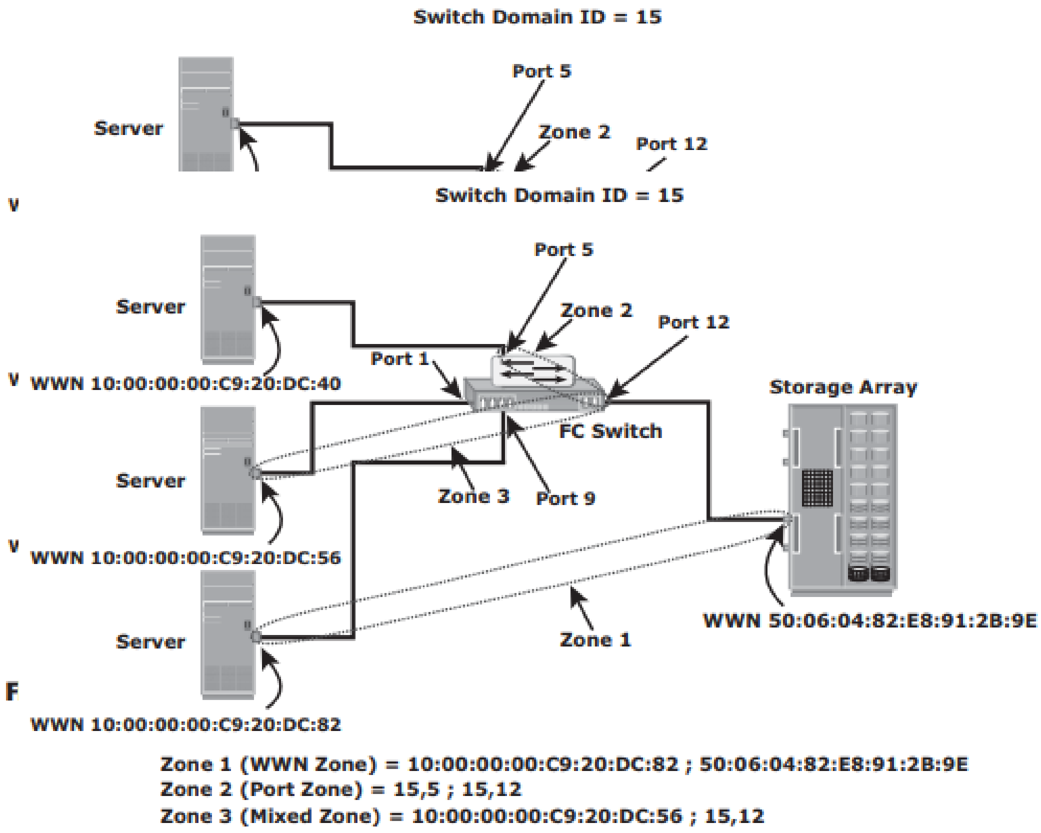
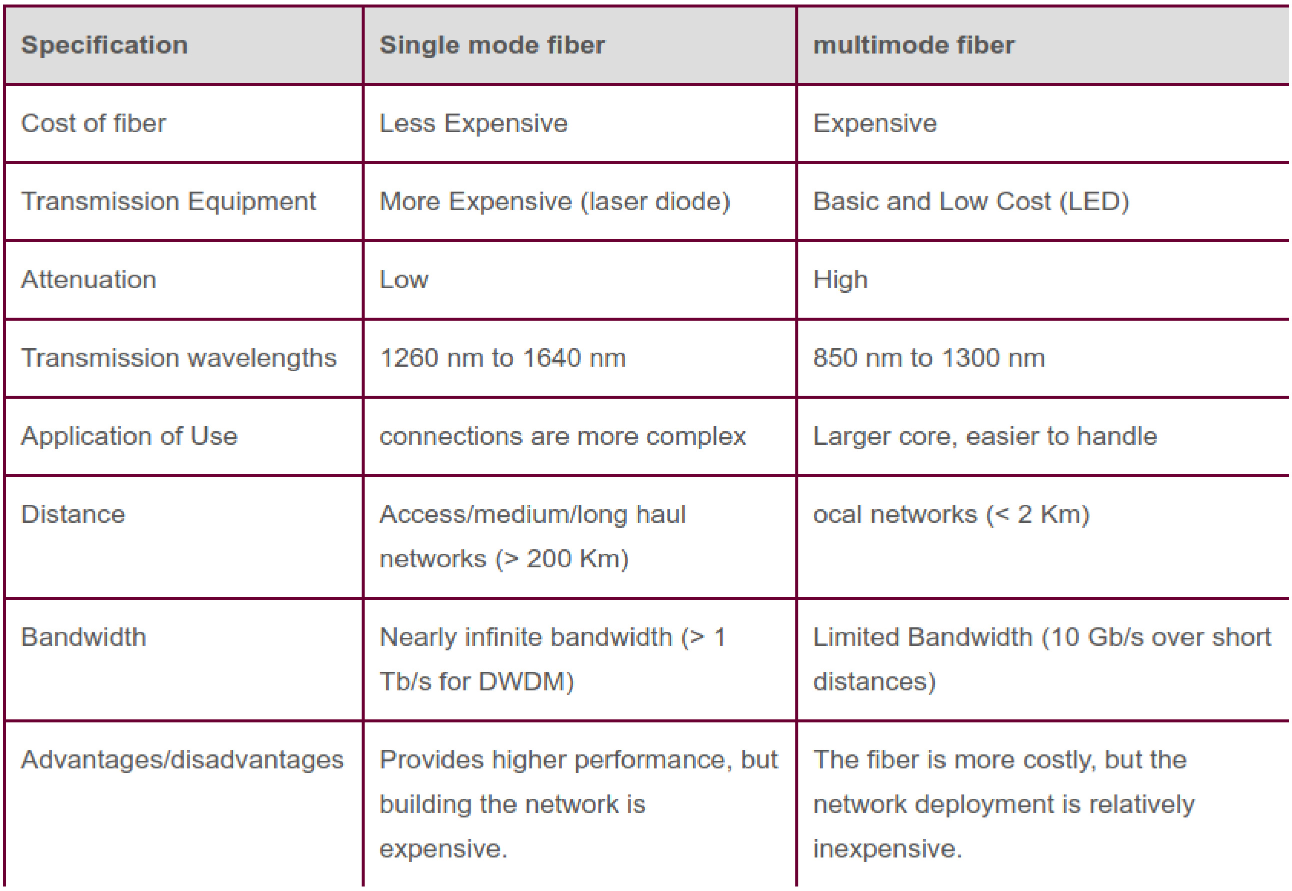
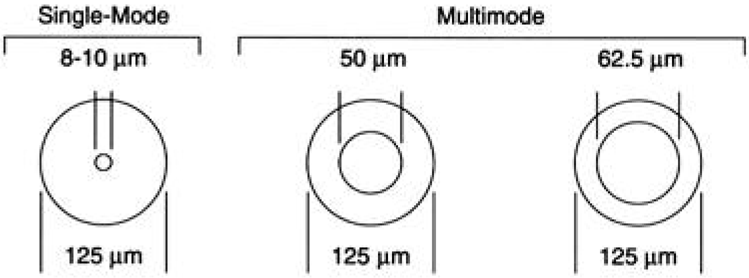

Switch Domain ID = 15
Port 5
Server
Zone 2
Port 12
v
Switch Domain ID = 15
Port 5
Server
Zone 2
Port 12
Port 1
v WWN 10:00:00:00:C9:20:DC:40
Storage Array
FC Switch
Server
Zone 3
Port 9
v WWN 10:00:00:00:C9:20:DC:56
WWN 50:06:04:82:E8:91:2B:9E
Server
Zone 1
F
WWN 10:00:00:00:C9:20:DC:82
Zone 1 (WWN Zone) = 10:00:00:00:C9:20:DC:82 ; 50:06:04:82:E8:91:2B:9E
Zone 2 (Port Zone) = 15,5 ; 15,12
Zone 3 (Mixed Zone) = 10:00:00:00:C9:20:DC:56 ; 15,12

Figure 5-19: Types of zoning

22) State difference between single mode fiber and multimode fiber and the advantages of using optic fiber over copper cables for SAN networks.



Specification	Single mode fiber	multimode fiber
Cost of fiber	Less Expensive	Expensive
Transmission Equipment	More Expensive (laser diode)	Basic and Low Cost (LED)
Attenuation	Low	High
Transmission wavelengths	1260 nm to 1640 nm	850 nm to 1300 nm
Application of Use	connections are more complex	Larger core, easier to handle
Distance	Access/medium/long haul networks (> 200 Km)	ocal networks (< 2 Km)
Bandwidth	Nearly infinite bandwidth (> 1 Tb/s for DWDM)	Limited Bandwidth (10 Gb/s over short distances)
Advantages/disadvantages	Provides higher performance, but building the network is expensive.	The fiber is more costly, but the network deployment is relatively inexpensive.



1. Greater Bandwidth

Copper cables were originally designed for voice transmission and have a limited bandwidth. Fiber optic cables provide more bandwidth for carrying more data than copper cables of the same diameter. Within the fiber cable family, singlemode fiber delivers up to twice the throughput of multimode fiber.

2. Faster Speeds

Fiber optic cables have a core that carries light to transmit data. This allows fiber optic cables to carry signals at speeds that are only about 31 percent slower than the speed of light—faster than Cat5 or Cat6 copper cables. There is also less signal degradation with fiber cables.

3. Longer Distances

Fiber optic cables can carry signals much farther than the typical 328-foot limitation for copper cables. For example, some 10 Gbps singlemode fiber cables can carry signals almost 25 miles. The actual distance depends on the type of cable, the wavelength and the network.

4. Better Reliability

Fiber is immune to temperature changes, severe weather and moisture, all of which can hamper the connectivity of copper cable. Plus, fiber does not carry electric current, so it's not bothered by electromagnetic interference (EMI) that can interrupt data transmission. It also does not present a fire hazard like old or worn copper cables can.

5. Thinner and Sturdier

Compared to copper cables, fiber optic cables are thinner and lighter in weight. Fiber can withstand more pull pressure than copper and is less prone to damage and breakage.

6. More Flexibility for the Future

Media converters make it possible to incorporate fiber into existing networks. The converters extend UTP Ethernet connections over fiber optic cable. Modular patch panel solutionsintegrate equipment with 10 Gb, 40 Gb and 100/120 Gb speeds to meet current needs and provide flexibility for future needs. The panels in these solutions accommodate a variety of cassettes for different types of fiber patch cables.

7. Lower Total Cost of Ownership

Although some fiber optic cables may have a higher initial cost than copper, the durability and reliability of fiber can make the total cost of ownership (TCO) lower. And, costs continue to decrease for fiber optic cables and related components as technology advances.

23) Compare the different fabric services available and their individual functionality? Examine the different service classes.

The **Fabric Login Server** is located at the predefined address of FFFFFE and is used during the initial part of the node's fabric login process.

The **Name Server** (formally known as Distributed Name Server) is located at the predefined address FFFFFC and is responsible for name registration and management of node ports. Each switch exchanges its Name Server information with other switches in the fabric to maintain a synchronized, distributed name service.

Each switch has a **Fabric Controller** located at the predefined address FFFFFD. The Fabric Controller provides services to both node ports and other switches. The Fabric Controller is responsible for managing and distributing Registered State Change Notifications (RSCNs) to the node ports registered with the Fabric Controller

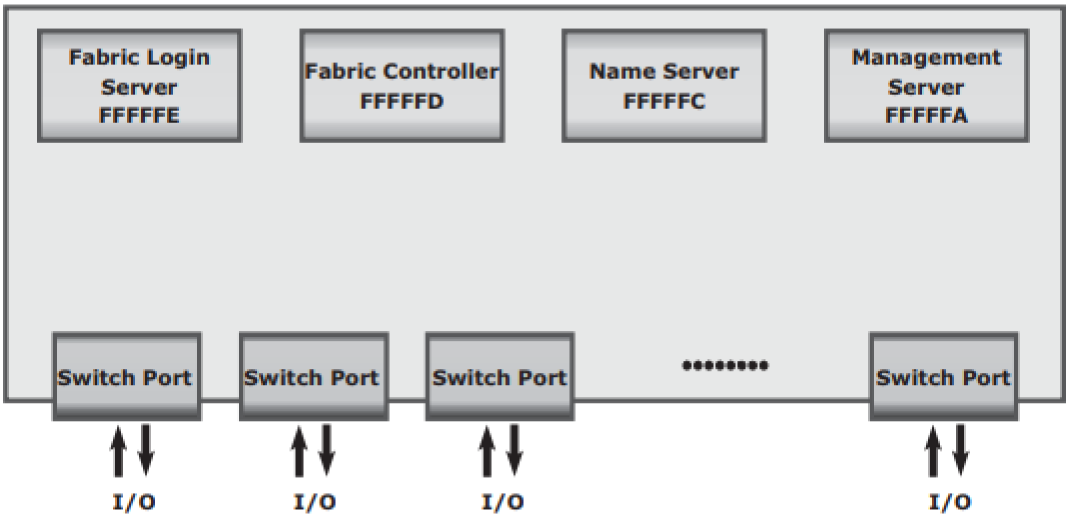
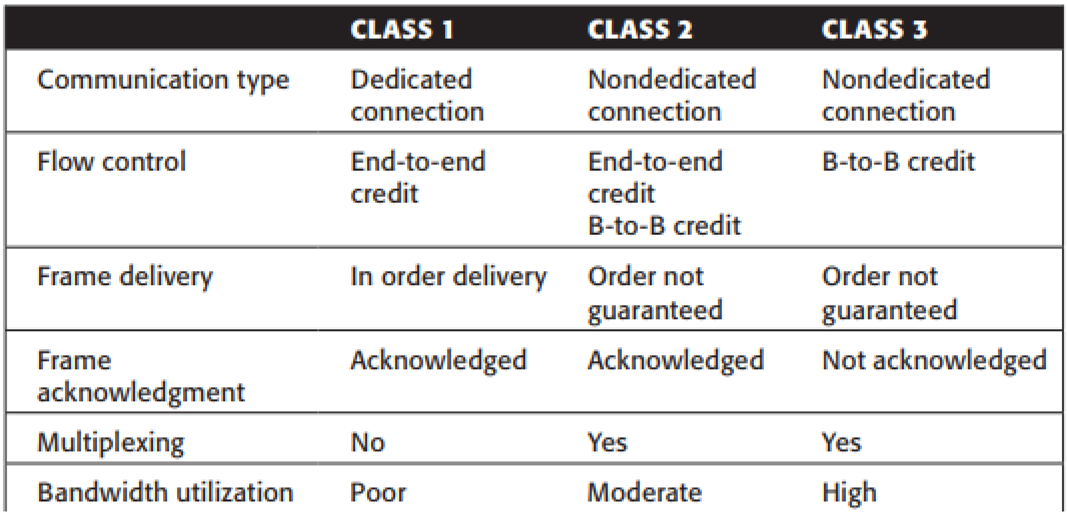


Figure 5-16: Fabric services provided by FC switches



	CLASS 1	CLASS 2	CLASS 3
Communication type	Dedicated connection	Nondedicated connection	Nondedicated connection
Flow control	End-to-end credit	End-to-end credit B-to-B credit	B-to-B credit
Frame delivery	In order delivery	Order not guaranteed	Order not guaranteed
Frame acknowledgment	Acknowledged	Acknowledged	Not acknowledged
Multiplexing	No	Yes	Yes
Bandwidth utilization	Poor	Moderate	High

24) Elaborate the need for using ip SAN? Explain the different variants of ip storage protocols and topologies and their different application.

IP SAN is a dedicated storage area network (SAN) that allows multiple servers to access pools of shared block storage devices using storage protocols that depend on the Internet Engineering Taskforce standard Internet Protocol suite.

Two primary protocols that leverage IP as the transport mechanism are InternetSCSI (iSCSI) and Fibre Channel over IP (FCIP).

iSCSI is encapsulation of SCSI I/Oover IP. FCIP is a protocol in which an FCIP entity such as an FCIP gateway is used to tunnel FC fabrics through an IP network

iSCSI is an IP based protocol that establishes and manages connections between host and storage over IP

iSCSI encapsulates SCSI commands and data into an IP packet and transports them using TCP/IP.

In **FCIP**, FC frames are encapsulated onto the IP payload. An FCIP implementation is capable of merging interconnected fabrics into a single fabriFibre Channel over

FC SAN provides a high-performance infrastructure for localized data movement.

Organizations are now looking for ways to transport data over a long distance between their disparate SANs at multiple geographic locations

25) Discuss Fiber channel protocol Stack and eloborate their functions.

It is easier to understand a communication protocol by viewing it as a structure of independent layers. 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.

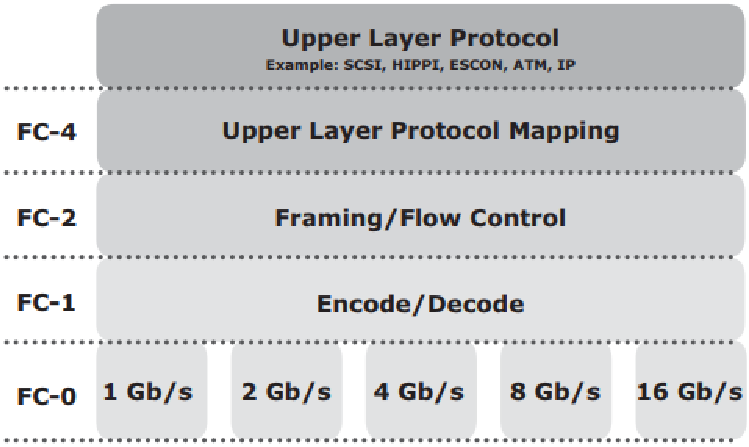


Figure 5-12: Fibre Channel protocol stack

FC-4

Layer FC-4 is the uppermost layer in the FCP stack. This layer defines the application interfaces and the way Upper Layer Protocols (ULPs) are mapped to the lower FC layers.

FC-2

Layer The FC-2 layer provides Fibre Channel addressing, structure, and organization of data (frames, sequences, and exchanges). It also defi nes fabric services, classes of service, fl ow control, and routing.

FC-1

Layer The FC-1 layer defi nes how data is encoded prior to transmission and decoded upon receipt. At the transmitter node, an 8-bit character is encoded into a 10-bit transmissions character. This character is then transmitted to the receiver node.

FC-0

Layer FC-0 is the lowest layer in the FCP stack. This layer defi nes the physical interface, media, and transmission of bits. The FC-0 specifi cation includes cables, connectors, and optical and electrical parameters for a variety of data rates. The FC transmission can use both electrical and optical media.

UNIT 4

26)Examine the difference between the NAS storage and Content managed storage? What are the components of object based storage.

The OSD system is typically composed of three key components: nodes, private network, and storage.

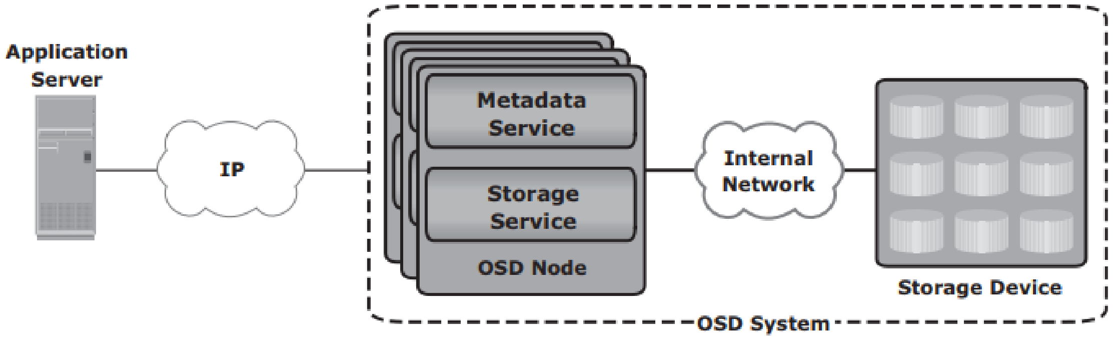


Figure 8-4: OSD components

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 and storage service. The metadata service is responsible for generating the object ID from the contents of a file. It also maintains the mapping of the object IDs and the file system namespace.
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.

27)What is data deduplication? Elaborate on the various methods of data deduplication and their advantages.

Data deduplication (*intelligent compression* or *single-instance storage)* is a process that eliminates redundant copies of data and reduces storage overhead.

There are two methods of deduplication: **file level and subfile level**.

File-level deduplication (also called single-instance storage) detects and removes redundant copies of identical files. It enables storing only one copy of the file; the subsequent copies are replaced with a pointer that points to the original file. File-level deduplication is simple and fast but does not address the problem of duplicate content inside the files. For example, two 10-MB PowerPoint presentations with a difference in just the title page are not considered as duplicate files, and each file will be stored separately.

Subfile deduplication breaks the file into smaller chunks and then uses a specialized algorithm to detect redundant data within and across the file. As a result, subfile deduplication eliminates duplicate data across files. There are two forms of subfile deduplication: f**ixed-length block and variable-length segment.**

> The **fixed-length block deduplication** divides the files into fixed length blocks and uses a hash algorithm to find the duplicate data. Although simple in design, fixed-length blocks might miss many opportunities to discover redundant data because the block boundary of similar data might be different.
>
> In **variable-length segment deduplication**, if there is a change in the segment, the boundary for only that segment is adjusted, leaving the remaining segments unchanged. This method vastly improves the ability to find duplicate data segments compared to fixed-block.

28) List the recovery considerations? Examine the backup methods.

➔ amount of data loss and downtime that a business can endure in terms of RPO and RTO are the primary considerations in selecting and implementing a specific backup strategy.

➔ RPO refers to the point in time to which data must be recovered, and the point in time from which to restart businessoperations. This specifies the time interval between two backups.

➔ RPO determines backup frequency

➔ if an application requires an RPO of 1 day, it would need the data to be backed up at least once every day

➔ Another consideration is the retention period, which defines the duration for which a business needs to retain the backup copies.

➔ example, data backed up for archival is retained for a longer period than data backed up for operational recovery.

➔ backup media type or backup target is another consideration, that is driven by RTO and impacts the data recovery time. The time-consuming operation of starting and stopping in a tape-based

➔ system affects the backup performance, especially while backing up a large number of small files.

- ➔ most appropriate time for performing a backup tominimize any disruption to production operations.
- ➔ Organizations must also consider the granularity of backups

Backup Methods

Hot backup and cold backup are the two methods deployed for a backup based on the state of the application when the backup is performed

In a hot backup, the application is up-and-running, with users accessing their data during the backup process. This method of backup is also referred to as an online backup.

cold backup requires the application to be shut down during the backup process. Hence, this method is also referred to as an offline backup.

hot backup of online production data is challenging because data is actively used and changed. If a file is open, it is normally not backed up duringthe backup process. In such situations, an open file agent is required to back up the open file.

A point-in-time (PIT) copy method is deployed in environments in which The impact of downtime from a cold backup or the performance impact resulting from a hot backup is unacceptable The PIT copy is created from the production volume and used as the source for the backup. This reduces the impact on the Pro duction volume Attributes are as important as the data itself and must be backed up for consistency.

29)Compare Fabric SAN network and NAS and enumerate circumstances which are conducive for implementation of NAS and SAN.

30)Discuss the NAS protocols NFS and CIFS variants.

NFS and CIFS are the common protocols for file sharing.

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

NFS creates a connection between the client and the remote system to transfer data. NFS (NFSv3 and earlier) is a stateless protocol, which means that it does not maintain any kind of table to store information about open files and associated pointers.

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. The CIFS protocol enables remote clients to gain access to files on a server. CIFS enables file sharing with other clients by using special locks. Filenames in CIFS are encoded using unicode characters. 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. The fault tolerance features of CIFS depend on whether an application is written to take advantage of these features. Moreover, CIFS is a stateful protocol because the CIFS server maintains connection information regarding every connected client. If a network failure or CIFS server failure occurs, the client receives a disconnection notification.

UNIT 5

31) Discuss Storage Tiering and its implementation variants.

Storage tiering is a technique of establishing a hierarchy of different storage types (tiers). This enables storing the right data to the right tier, based on service level requirements, at a minimal cost. Each tier has different levels of protection, performance, and cost. For example, high performance solidstate drives (SSDs) or FC drives can be configured as tier 1 storage to keep frequently accessed data, and low cost SATA drives as tier 2 storage to keep the less frequently accessed data. Keeping frequently used data in SSD or FC improves application performance. Moving less-frequently accessed data to SATA can free up storage capacity in high performance drives and reduce the cost of storage.

Storage tiering can be implemented as a manual or an automated process. Manual storage tiering is the traditional method where the storage administrator monitors the storage workloads periodically and moves the data between the tiers. Manual storage tiering is complex and time-consuming. Automated storage tiering automates the storage tiering process, in which data movement between the tiers is performed nondisruptively.

Intra-Array Storage Tiering

The process of storage tiering within a storage array is called intra-array storage tiering. It enables the efficient use of SSD, FC, and SATA drives within an array and provides performance and cost optimization. The goal is to keep the SSDs busy by storing the most frequently accessed data on them, while moving out the less frequently accessed data to the SATA drives. Data movements executed between tiers can be performed at the LUN level or at the sub-LUN level. The performance can be further improved by implementing tiered cache. LUN tiering, sub-LUN tiering, and cache tiering are detailed next.

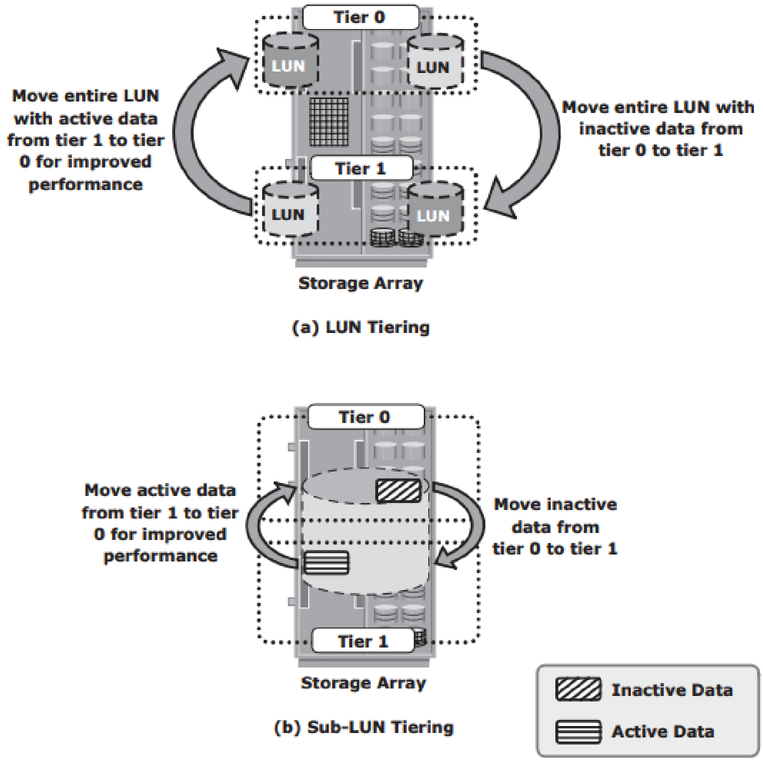

Tier 0
LUN
LUN
Move entire LUN with active data from tier 1 to tier 0 for improved performance
Move entire LUN with inactive data from tier 0 to tier 1
Tier 1
LUN
LUN
Storage Array
(a) LUN Tiering
Tier 0
Move active data from tier 1 to tier 0 for improved performance
Move inactive data from tier 0 to tier 1
Tier 1
Storage Array
(b) Sub-LUN Tiering
▨ Inactive Data
☰ Active Data

Figure 15-12: Implementation of intra-array storage tiering

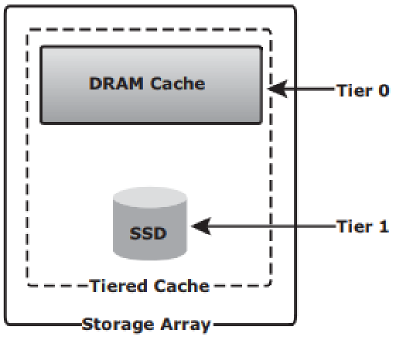


Figure 15-13: Cache tiering

Inter-Array Storage Tiering

The process of storage tiering between storage arrays is called inter-array storage tiering. Inter-array storage tiering automates the identification of active or inactive data to relocate them to different performance or capacity tiers between the arrays.

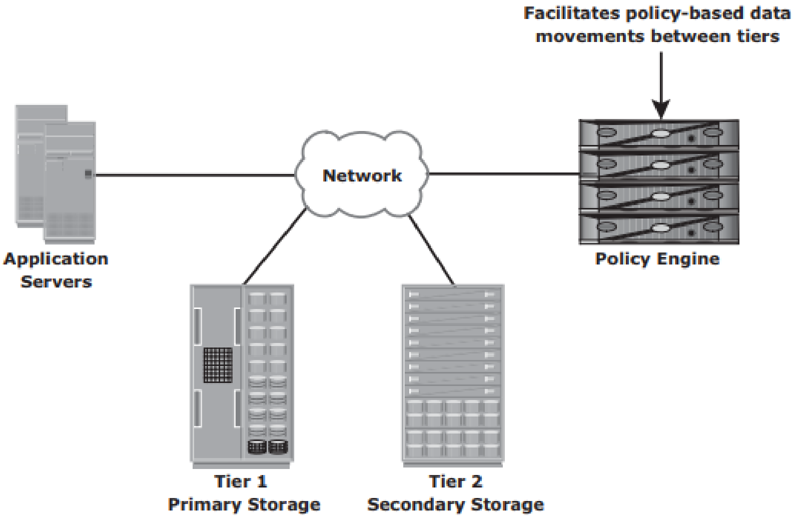


Figure 15-14: Implementation of inter-array storage tiering

31) Explain Information Life Cycle Management with a neat diagram.

In both traditional data center and virtualized environments, managing information can be expensive if not managed appropriately.

- ➔ Exploding digital universe: The rate of information growth is increasing exponentially. Creating copies of data to ensure high availability and repurposing has contributed to the multifold increase of information growth.
- ➔ Increasing dependency on information: The strategic use of information plays an important role in determining the success of a business and provides competitive advantages in the marketplace.
- ➔ Changing value of information: Information that is valuable today might become less important tomorrow. The value of information often changes over time.

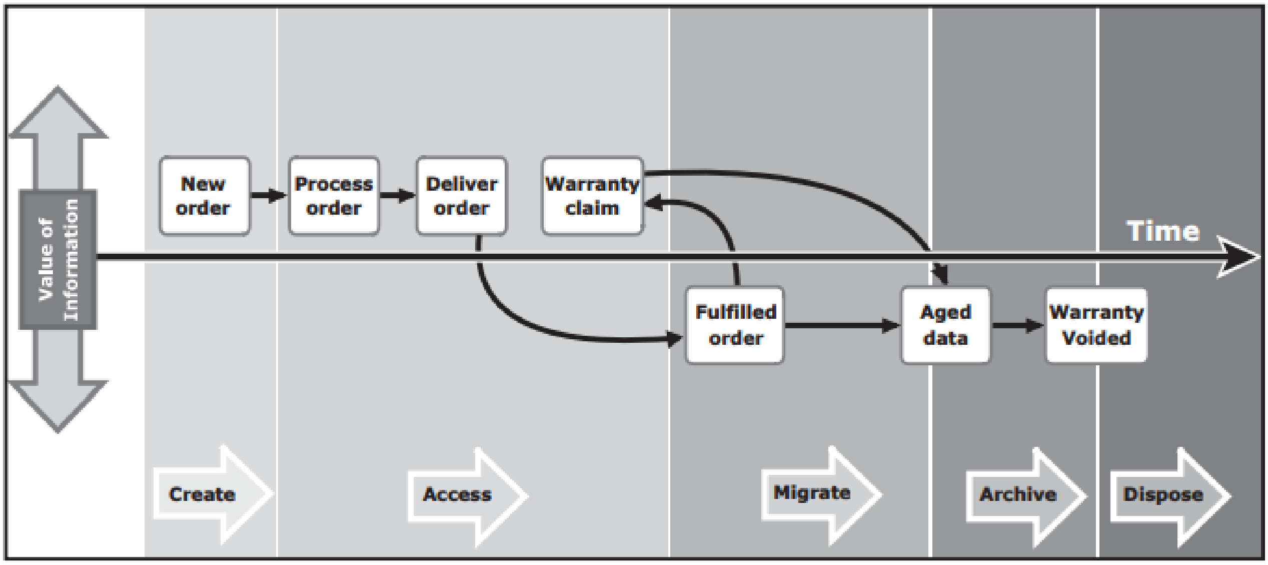


Figure 15-11: Changing value of sales order information

Information Lifecycle Management (ILM) is a proactive strategy that enables an IT organization to effectively manage information throughout its life cycle based on predefined business policies. From data creation to data deletion, ILM aligns the business requirements and processes with service levels in an automated fashion. This allows an IT organization to optimize the storage infrastructure for maximum return on investment. Implementing an ILM strategy has the following key benefits that directly address the challenges of information management:

- ➔ Lower Total Cost of Ownership (TCO): By aligning the infrastructure and management costs with information value. As a result, resources are not wasted, and complexity is not introduced by managing low-value data at the expense of high-value data.
- ➔ Simplified management: By integrating process steps and interfaces with individual tools and by increasing automation.
- ➔ Maintaining compliance: By knowing what data needs to be protected for what length of time.
- ➔ Optimized utilization: By deploying storage tiering

32) List and explain the key storage infrastructure management activities.

The pace of information growth, proliferation of applications, heterogeneous infrastructure, and stringent service-level requirements have resulted in increased complexity of managing storage infrastructures.

The key storage infrastructure management activities performed in a data center can be broadly categorized into

- ➔ availability management
- ➔ capacity management
- ➔ performance management
- ➔ security management
- ➔ Reporting.

availability management

A critical task in availability management is establishing a proper guideline based on defined service levels to ensure availability.

Availability management involves all availability-related issues for components or services to ensure that service levels are met.

A key activity in availability management is to provision redundancy at all levels, including components, data, or even sites. For example, when a server is deployed to support a critical business function, it requires high availability

capacity management

The goal of capacity management is to ensure adequate availability of resources based on their service level requirements. Capacity management also involves optimization of capacity based on the cost and future needs. Capacity management provides capacity analysis that compares allocated storage to forecasted storage on a regular basis.

performance management

Performance management ensures the optimal operational efficiency of all components. Performance analysis is an important activity that helps to identify the performance of storage infrastructure components. This analysis provides information on whether a component meets expected performance levels.

security management

The key objective of the security management activity is to ensure confidentiality, integrity, and availability of information in both virtualized and nonvirtualized environments. Security management prevents unauthorized access and configuration of storage infrastructure components.

Reporting.

Reporting on a storage infrastructure involves keeping track and gathering information from various components and processes. This information is compiled to generate reports for trend analysis, capacity planning, chargeback, and performance.

33)Define the following: i. Threats ii. Vulnerability.

Threats are the potential attacks that can be carried out on an IT infrastructure. These attacks can be classified as active or passive. Passive attacks are attempts to gain unauthorized access into the system. They pose threats to confidentiality of information. Active attacks include data modification, denial of service (DoS), and repudiation attacks. **Denial of service (DoS)** attacks prevent legitimate users from accessing resources and services. **Repudiation** is an attack against the accountability of information.

Implementing security controls at each access point of every access path is known as defense in depth. Defense in depth recommends using multiple security measures to reduce the risk of security threats if one component of the protection is compromised. It is also known as a “layered approach to security.” **Attack surface, attack vector, and work factor** are the three factors to consider when assessing the extent to which an environment is vulnerable to security threats.

- Attack surface refers to the various entry points that an attacker can use to launch an attack.
- attack vector is a step or a series of steps necessary to complete an attack.
- Work factor refers to the amount of time and effort required to exploit an attack vector.