Internal Assessment Test II Solution– June 2022

Sub:	Storage Area Network					Sub Code:	18CS822	Branch:	ISE		
Date:	04-06-2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	VIII A, B & C			OBE	
Answer any FIVE FULL Questions									MARKS	CO	RBT
1	Describe the Fibre Channel SAN components.								10	CO1	L2

Solution:

Components of FC SAN

1. Node (server and storage) ports
2. Cables
3. Connectors
4. Interconnecting devices such as FC switches and hubs
5. SAN management software

Node (server and storage) ports

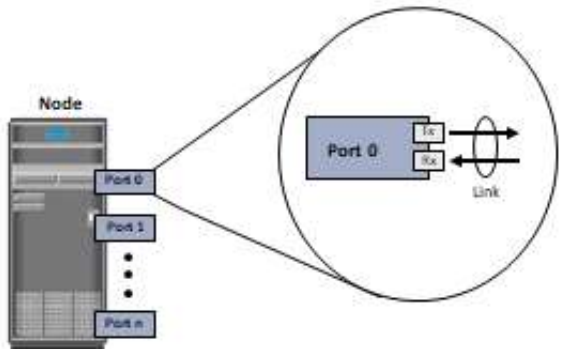
In FC network, the end devices, such as hosts, storage arrays, and tape libraries, are all referred to as *nodes*.

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.

Exist on

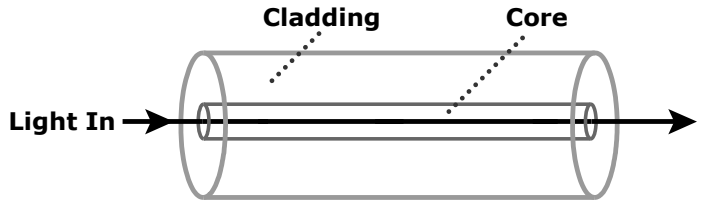
1. Host bus adapter (HBA) in server
2. Front-end adapters in storage



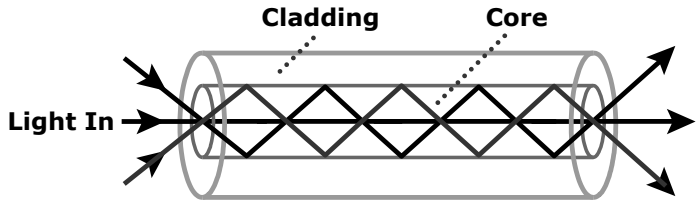
3. Cables

1. Copper cables for short distance (back-end)(acceptable signal-to-ratio for distance up to 30 meters).

2. Optical fiber cables for long distance. carry data in the form of light.
3. Two types of optical cables: single-mode and multimode



Single-mode Fiber



Multimode Fiber

3**.Connectors**

6. Attached at the end of a cable to enable swift (rapid) connection and disconnection of the cable to and from a port.
7. Commonly used connectors for fiber optic cables are:
    1. Standard Connector (SC)
        1. Duplex connectors
    2. Lucent Connector (LC)
        1. Duplex connectors
    3. Straight Tip (ST)
        1. Patch panel connectors
        2. Simplex connectors

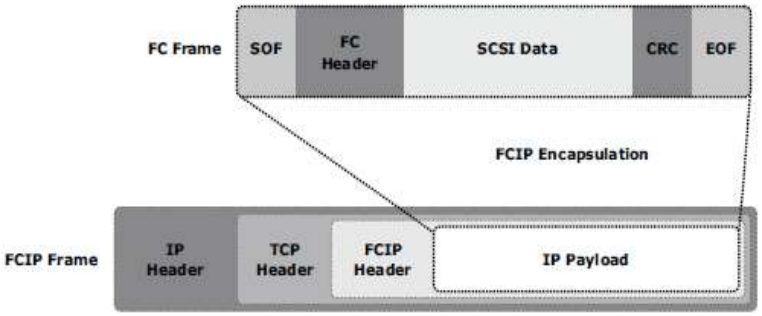
4.Interconnecting Devices

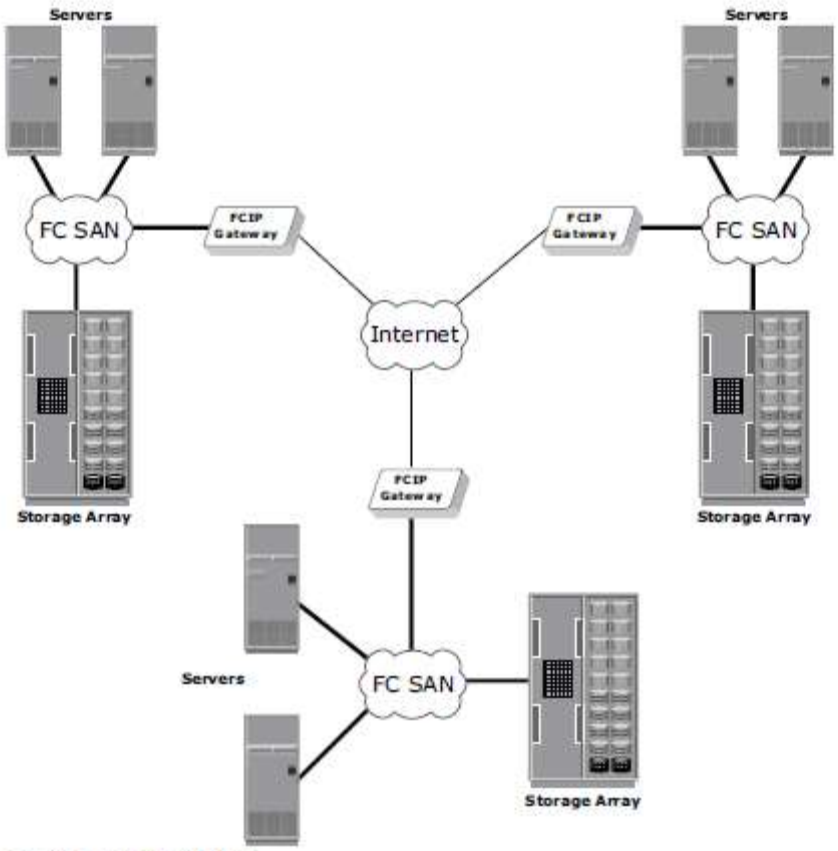
Hubs

4. **Physically** connect nodes in a logical loop or a physical star topology
5. Provide **limited** connectivity and scalability
6. All nodes must **share** the loop because data travels through all the connection points.
7. Because of the availability of low-cost and high-performance switches, hubs are no longer used in FC SANs

Switches

	8. More **intelligent** than hubs and directly route data from one physical port to another 9. Switches are available with fixed port count or modular design 10. Nodes **do not share** the bandwidth. 11. Instead, each node has a dedicated communication path **Directors** 12. **High-end switches** with a **higher port count** and better fault tolerance capabilities. 13. Always modular, and its port count can be increased by inserting additional 'line cards' or 'blades' 14. High-end switches and directors contain redundant components 5**. SAN Management Software** • A suite of tools used in a SAN to manage interfaces between host and storage arrays • Management of various resources from one central console. • Provides integrated management of SAN environment • Key management functions: 1. Mapping of storage devices, switches and servers 2. Monitoring and generating alerts for discovered devices 3. Logical partitioning of SAN (zoning) 4. Management of SAN components (HBAs, storage components and interconnecting devices)			
2	Identify and define the factors that influence NAS performance and availability of it Soultion: 1. **Number of hops**: A large number of hops can increase latency because IP processing is required at each hop, adding to the delay caused at the router. 2. **Authentication with a directory service such as LDAP, Active Directory, or NIS**: The authentication service must be available on the network, with adequate bandwidth, and must have enough resources to accommodate the authentication load. Otherwise, a large number of authentication requests are presented to the servers, increasing latency. Authentication adds to latency only when authentication occurs. 3. **Retransmission:** Link errors, buffer overflows, and flow control mechanisms can result in retransmission. This causes packets that have not reached the specified destination to be resent. Care must be taken when configuring parameters for speed and duplex settings on the network devices and the NAS heads so that they match. Improper configuration may result in errors and retransmission, adding to latency. 4. **Overutilized routers and switches**: The amount of time that an overutilized device in a network takes to respond is always more than the response time of an optimally utilized or underutilized device. Network administrators can view vendor-specific statistics to determine the utilization of switches and routers in a network. Additional devices should be added if the current devices are overutilized. 5. **File/directory lookup and metadata requests**: NAS clients access files on NAS devices. The processing required before reaching the appropriate file or directory can cause delays. Sometimes a delay is caused by deep directory structures and can be	10	CO2	L2

	resolved by flattening the directory structure. Poor file system layout and an overutilized disk system can also degrade performance. 6. **Overutilized NAS devices:** Clients accessing multiple files can cause high utilization levels on a NAS device which can be determined by viewing utilization statistics. High utilization levels can be caused by a poor file system structure or insufficient resources in a storage subsystem. 7. **Overutilized clients:** The client accessing CIFS or NFS data may also be overutilized. An overutilized client requires longer time to process the responses received from the server, increasing latency. Specific performance-monitoring tools are available for various operating systems to help determine the utilization of client resources.			
3	Describe the structure of the FCIP frame Encapsulation and FCIP Topology **Solution:**  **Figure 8-9:** FCIP encapsulation	10	CO1	L2

	 Figure 8-10: FCIP topology			
4	What is Business Continuity? Explain BC Planning Life Cycle with a neat diagram **What is Business Continuity?** businesss continuity is an organization's ability to maintain essential functions during and after a disaster has occurred. Business continuity planning establishes risk management processes and procedures that aim to prevent interruptions to mission-critical services, and reestablish full function to the organization as quickly and smoothly as possible. **BC Planning Lifecycle** □ BC planning must follow a disciplined approach like any other planning process. □ Organizations today dedicate specialized resources to develop and maintain BC plans. □ From the conceptualization to the realization of the BC plan, a lifecycle of activities can be defined for the BC process. □ The BC planning lifecycle includes five stages: 1. Establishing objectives 2. Analyzing 3. Designing and developing 4. Implementing	10	CO2	L2

5. Training, testing, assessing, and maintaining

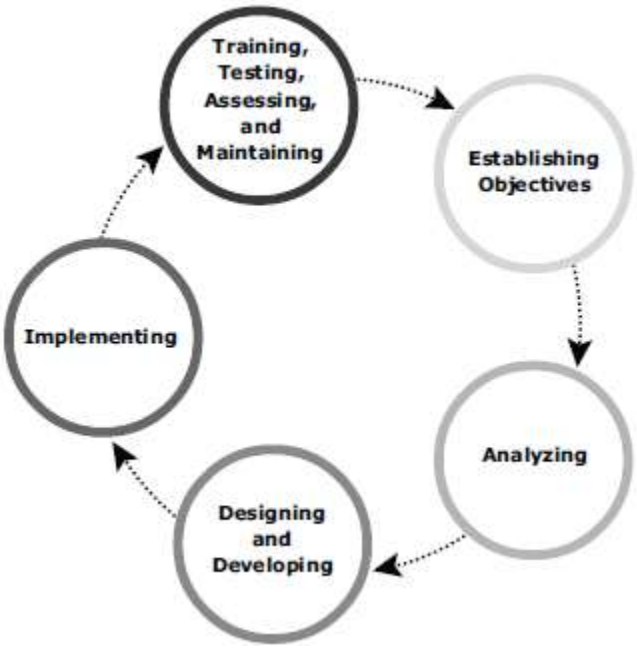


Figure: BC planning lifecycle

 Several activities are performed at each stage of the BC planning lifecycle, including the following key activities:

1. Establishing objectives

- Determine BC requirements.
- Estimate the scope and budget to achieve requirements.
- Select a BC team by considering subject matter experts from all areas of the business, whether internal or external.
- Create BC policies.

2. Analyzing

- Collect information on data profiles, business processes, infrastructure support, dependencies, and frequency of using business infrastructure.
- Identify critical business needs and assign recovery priorities.
- Create a risk analysis for critical areas and mitigation strategies.
- Conduct a Business Impact Analysis (BIA).
- Create a cost and benefit analysis based on the consequences of data unavailability.
- Evaluate options.

3. Designing and developing

	➢ Define the team structure and assign individual roles and responsibilities. For example, different teams are formed for activities such as emergency response, damage assessment, and infrastructure and application recovery. ➢ Design data protection strategies and develop infrastructure. ➢ Develop contingency scenarios. ➢ Develop emergency response procedures. ➢ Detail recovery and restart procedures. **4. Implementing** ➢ Implement risk management and mitigation procedures that include backup, replication, and management of resources. ➢ Prepare the disaster recovery sites that can be utilized if a disaster affects the primary data center. ➢ Implement redundancy for every resource in a data center to avoid single points of failure. **5. Training, testing, assessing, and maintaining** ➢ Train the employees who are responsible for backup and replication of business-critical data on a regular basis or whenever there is a modification in the BC plan. ➢ Train employees on emergency response procedures when disasters are declared. ➢ Train the recovery team on recovery procedures based on contingency scenarios. ➢ Perform damage assessment processes and review recovery plans. ➢ Test the BC plan regularly to evaluate its performance and identify its limitations. ➢ Assess the performance reports and identify limitations. ➢ Update the BC plans and recovery/restart procedures to reflect regular changes within the data center.			
5	Demonstrate the various ways of implementing NAS and its benefits with a neat diagram. There are two types of NAS implementations: integrated and gateway. □ The *integrated NAS* device has all of its components and storage system in a single enclosure. □ In *gateway* implementation, NAS head shares its storage with SAN environment. **1. Integrated NAS**	10	CO2	L3

	□ An integrated NAS device has all the components of NAS, such as the NAS head and storage, in a single enclosure, or frame. □ This makes the integrated NAS a self-contained environment. □ The NAS head connects to the IP network to provide connectivity to the clients and service the file I/O requests. □ The storage consists of a number of disks that can range from low-cost ATA to high throughput FC disk drives. □ Management software manages the NAS head and storage configurations. □ An integrated NAS solution ranges from a low-end device, which is a single enclosure, to a high-end solution that can have an externally connected storage array. □ A low-end appliance-type NAS solution is suitable for applications that a small department may use, where the primary need is consolidation of storage, rather than high performance or advanced features such as disaster recovery and business continuity. □ This solution is fixed in capacity and might not be upgradable beyond its original configuration. □ To expand the capacity, the solution must be scaled by deploying additional units, a task that increases management overhead because multiple devices have to be administered. □ In a high-end NAS solution, external and dedicated storage can be used. □ This enables independent scaling of the capacity in terms of NAS heads or storage. □ However, there is a limit to scalability of this solution. **2. Gateway NAS** □ A gateway NAS device consists of an independent NAS head and one or more storage arrays. □ The NAS head performs the same functions that it does in the integrated solution; while the storage is shared with other applications that require block-level I/O. □ Management functions in this type of solution are more complex than those in an integrated environment because there are separate administrative tasks for the NAS head and the storage. □ In addition to the components that are explicitly tied to the NAS solution, a gateway solution can also utilize the FC infrastructure, such as switches, directors, or direct-attached storage arrays. □ The gateway NAS is the most scalable because NAS heads and storage arrays can be independently scaled up when required.			

 Adding processing capacity to the NAS gateway is an example of scaling.

 When the storage limit is reached, it can scale up, adding capacity on the SAN independently of the NAS head.

 Administrators can increase performance and I/O processing capabilities for their environments without purchasing additional interconnect devices and storage.

 Gateway NAS enables high utilization of storage capacity by sharing it with SAN environment.

3.Integrated NAS Connectivity

 An integrated solution is self-contained and can connect into a standard IP network.

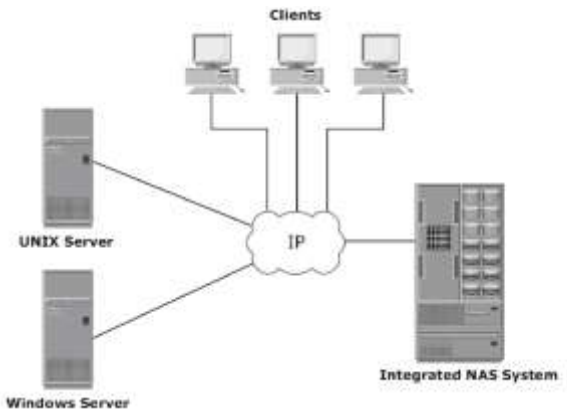
 Although the specifics of how devices are connected within a NAS implementation vary by vendor and model.

 In some cases, storage is embedded within a NAS device and is connected to the NAS head through internal connections, such as ATA or SCSI controllers.

 In others, the storage may be external but connected by using SCSI controllers.

 In a high-end integrated NAS model, external storage can be directly connected by FC HBAs or by dedicated FC switches.

 In the case of a low-end integrated NAS model, backup traffic is shared on the same public IP network along with the regular client access traffic.



 In the case of a high-end integrated NAS model, an isolated backup network can be used to segment the traffic from impeding client access.

 More complex solutions may include an intelligent storage subsystem, enabling faster backup and larger capacities while simultaneously enhancing performance.
Figure: Integrated NAS connectivity

4. Gateway NAS Connectivity

 In a gateway solution, front-end connectivity is similar to that in an integrated solution.

 An integrated environment has a fixed number of NAS heads, making it relatively easy to determine IP networking requirements.

 In contrast, networking requirements in a gateway environment are complex to determine due to scalability options.

 Adding more NAS heads may require additional networking connectivity and bandwidth.

 Communication between the NAS gateway and the storage system in a gateway solution is achieved through a traditional FC SAN.

 To deploy a stable NAS solution, factors such as multiple paths for data, redundant fabrics, and load distribution must be considered.

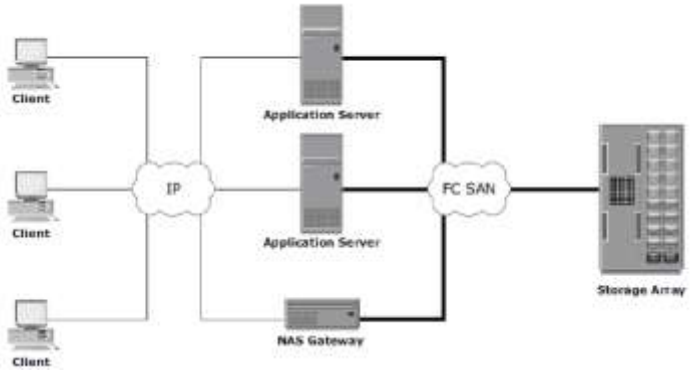


Figure: Gateway NAS connectivity

 Implementation of a NAS gateway solution requires analysis of current SAN environment.

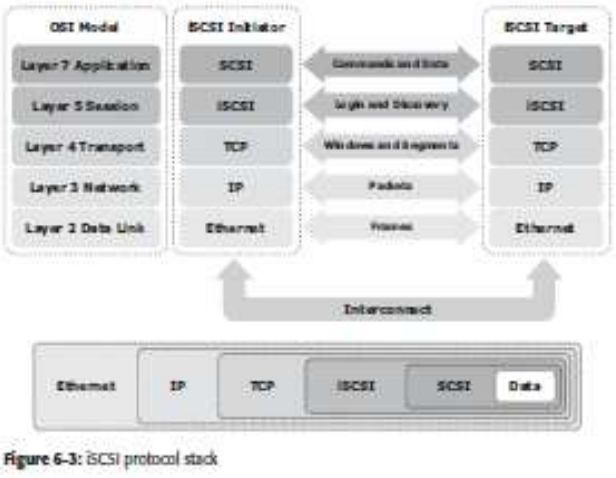
 This analysis is required to determine the feasibility of introducing a NAS workload to the existing SAN.

 Analyze the SAN to determine whether the workload is primarily read or write, or random or sequential. Determine the predominant I/O size in use.

 In general, sequential workloads have large I/Os.

 Typically, NAS workloads are random with small I/O size.

 Introducing sequential workload with random workloads can be disruptive to the sequential workload. Therefore, it is recommended to separate the NAS and SAN disks.

	□ Also, determine whether the NAS workload performs adequately with the configured cache in the storage subsystem.			
6	Draw the structure iSCSI Protocol Stack and iSCSI Discovery **Solution:** **SCSI Protocol Stack** Figure 6-3 displays a model of the iSCSI protocol layers and depicts the encapsulation order of the SCSI commands for their delivery through a physical carrier.  **Figure 6-3:** iSCSI protocol stack 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. 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. **iSCSI Discovery** • For iSCSI communication, initiator must discover location and name of target on a network • iSCSI discovery takes place in two ways:	10	CO1	L2

	•	**SendTargets discovery** • Initiator is **manually configured** with the target's network portal • Initiator issues SendTargets command; target responds with required parameters	**Internet Storage Name Service (iSNS)** • Initiators and targets **register** themselves with iSNS server • Initiator can query iSNS server for a list of available targets		