MODULE 4 QB

-PP

1) Define Business Continuity. Explain BC Terminology.

Ans) Business Continuity means having a plan inorder to keep your business running during and after unexpected events such as disasters or cyber attacks.

BC Terminology:

1) Business Continuity Planning (BCP): The process of creating and validating a comprehensive plan for ensuring that an organization can continue operating during and after disruptive events.

2) Disaster recovery:

This is the coordinated process of restoring systems, data and the infrastructure required to support ongoing business operations after a disaster occurs.

3) Disaster restart:

This is the process of restarting business operations with mirrored consistent copies of data and applications.

4) Recovery-Point Objective (RPO):

- This is the point in time in which systems and data must be recovered after an outage.
- It defines the amount of data loss that can occur in a business.

5) Recovery-Time Objective (RTO):

- The time within which systems and applications must be recovered after an outage.

6) Data vault:

- A repository at a remote site where data can be periodically or continuously copied.
- There is always a copy at another site link.
- Applications can run at both sites simultaneously.

7) Hot site:

An off-site facility which has all the necessary hardware and software to enable rapid recovery of critical business functions.

8) Cold site:

A site that does not have the necessary hardware and software to enable rapid recovery of critical business functions but is available for use in case of a disaster.

9) Warm Site:

An off-site facility that has some hardware and software pre-installed, but still requires additional configuration before it can be used for disaster recovery.

10) Server Clustering:

A group of servers and other necessary resources coupled to operate as a single system.

11) High Availability (HA):

The ability of a system or application to remain operational with minimal downtime and after a disruptive event during normal operations.

2) Explain BC planning life cycle with a neat diagram.

Ans) The BC planning life cycle includes five stages:

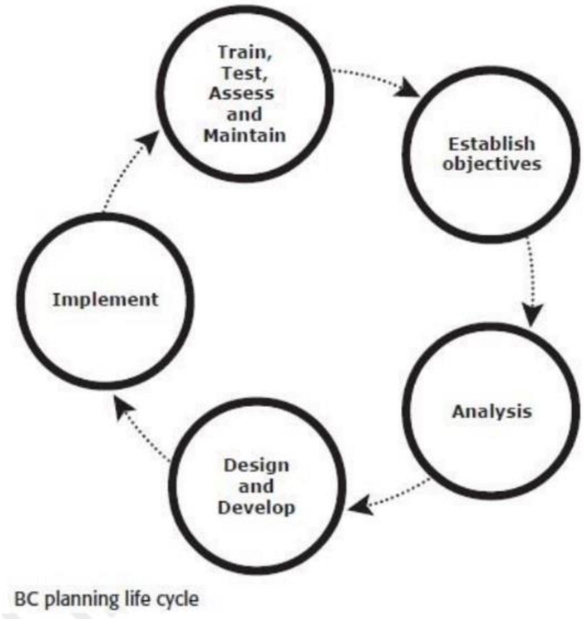
1) Establishing objectives

2) Analyzing

3) Designing and developing

4) Implementing

5) Training, testing, assessing and maintaining



BC planning life cycle

1) Establish objectives:

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

2) Analysis:

- Collect information on data profiles, business processes, infrastructure support, dependencies and frequency of using business infrastructure.
- Conduct a Business Impact Analysis (BIA).
- Identify critical business processes and assign recovery priorities.
- Perform risk analysis for critical functions.
- Perform cost benefit analysis for available solutions based on the mitigation strategy.
- Evaluate options.

3) Design and develop:

- Define the team structure and assign individual roles and responsibilities.
- Design data protection strategies and develop infrastructure.
- Develop contingency solutions.
- Develop emergency response procedures.
- Detail recovery and restart procedures.

4) Implement:

- 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) Train, test, assess and maintain:

- 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.
- 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.

3) Define Business Impact Analysis. List and explain the important BC Technology Solutions.

Ans) A business impact analysis (BIA) identifies which business units, operations and processes are essential to the survival of the business.

BC Technology Solutions:

The important BC Technology Solutions are:

1) Backup:

- Data backup is a predominant method of ensuring data availability.
- The frequency of backup is determined based on RPO, RTO and the frequency of data changes.

2) Local replication:

- Data can be replicated to a separate location within the same storage array.
- Replicas can also be used for restoring operations if data corruption occurs.

3) Remote replication:

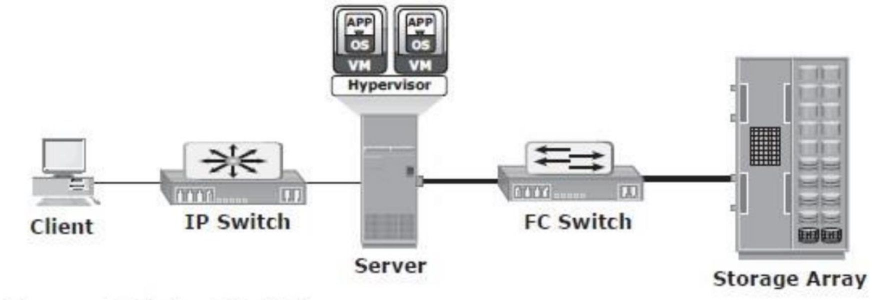
- Data in a storage array can be replicated to another storage array located at a remote site.
- If the storage array is lost due to a disaster, business operations can be started from the remote storage array.

4) Explain Failure Analysis in BC.

Ans) Failure analysis involves analyzing both the physical and virtual infrastructure components to identify systems that are susceptible to a single point of failure and implementing fault-tolerance mechanisms.

1) Single Point of Failure:

- A single point of failure refers to the failure of a component that can terminate the availability of the entire system or IT service.
- The client is connected to the server through an IP network, and the server is connected to the storage array through an FC connection.
- In a setup in which each component must function as required to ensure data availability, the failure of a single physical or virtual component causes the unavailability of an application.



Single point of failure

Resolving Single Points of Failure:

- To mitigate single points of failure, systems are designed with redundancy, such that the system fails only if all the components in the redundancy group fail.
- Setting up redundant HBAs or NIC teaming on a server can prevent a single HBA or NIC failure from causing downtime.
- Configuration of redundant switches to account for a switch failure.
- Configuration of multiple storage array ports to mitigate a port failure .
- RAID and hot spare configuration to ensure continuous operation in the event of disk failure.
- Implementation of a redundant storage array at a remote site to mitigate local site failure.
- Implementing server (or compute) clustering, a fault-tolerance mechanism whereby two or more servers in a cluster access the same set of data volumes.

- Implementing a VM Fault Tolerance mechanism ensures BC in the event of a server failure.

2) Multipathing Software:

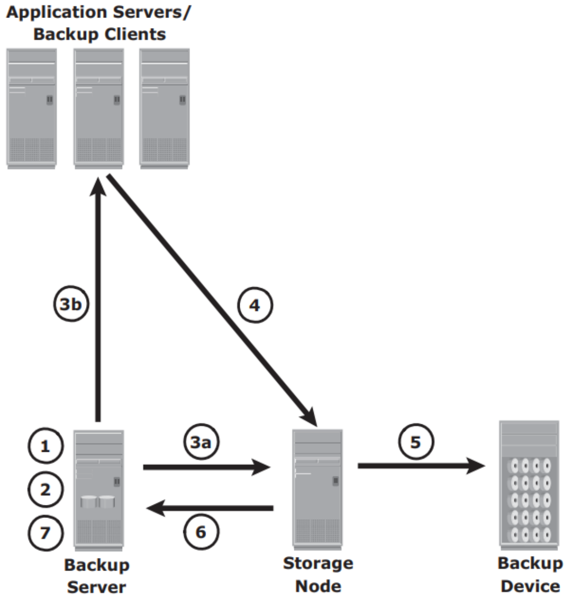
- Configuration of multiple paths increases the data availability through path failover.
- Redundant paths to the data eliminate the possibility of the path becoming a single point of failure.
- Multiple paths to data also improve I/O performance through load balancing among the paths.
- It also maximizes server, storage and data path utilization.
- Multipathing software provides the functionality to recognize and utilize alternative I/O paths to data.
- Multipathing software also manages the load balancing by distributing I/Os to all available, active paths.

5) Explain Backup and Restore Operaion.

Ans)

Backup Operation:

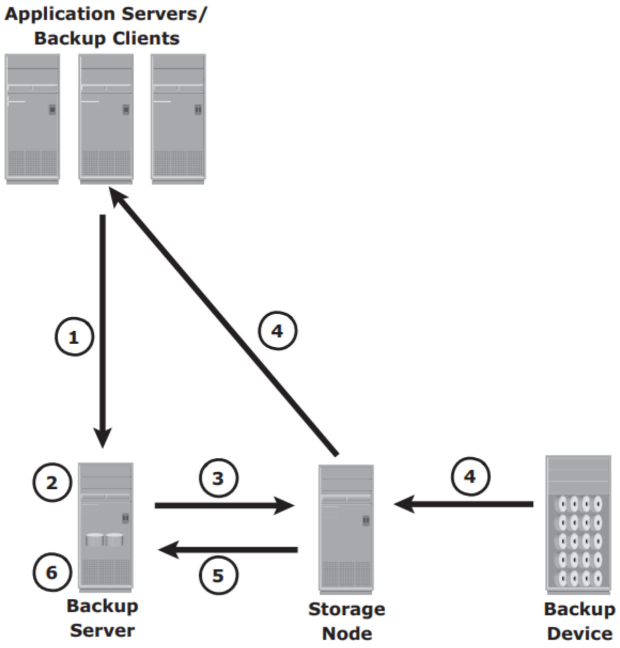
- When a backup operation is initiated, significant network communication takes place between the different components of a backup infrastructure.
- The backup server initiates the backup process for different clients based on the backup schedule configured for them.
- For example, the backup for a group of clients may be scheduled to start at 11:00 p.m. everyday.
- The backup server maintains the information about backup clients to be backed up and storage nodes to be used in a backup operation.
- The backup server instructs storage node to load backup media in backup device.
- Simultaneously, it instructs the backup clients to gather the data to be backed up and send it over the network to the assigned storage node
- After the backup data is sent to the storage node, the client sends some backup metadata (number of files, name of the files, storage node details and so on) to the backup server.
- The storage node receives the client data, organizes it and sends it to the backup device.
- The storage node then sends additional backup metadata (location of the data on the backup device, time of backup, and so on) to the backup server.
- The backup server updates the backup catalog with this information.



Backup operation

Restore Operation:

- Upon receiving a restore request, an administrator opens the restore application to view the list of clients that have been backed up.
- While selecting the client for which a restore request has been made, the administrator also needs to identify the client that will receive the restored data.
- Data can be restored on the same client for whom the restore request has been made or on any other client.
- The administrator then selects the data to be restored and the specified point in time to which the data has to be restored based on the RPO.
- The backup server instructs the appropriate storage node to mount the specific backup media onto the backup device.
- Data is then read and sent to the client that has been identified to receive the restored data.



Restore operation

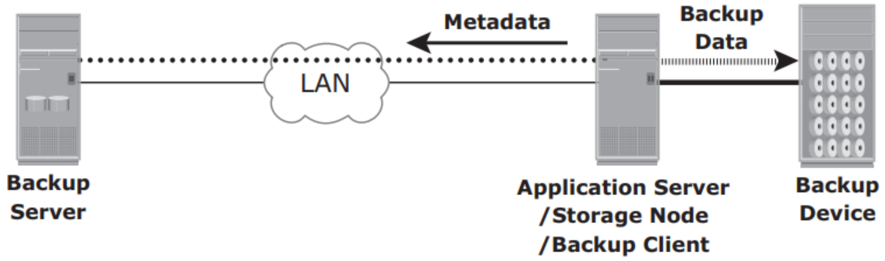
6) Explain Backup Topologies.

Ans) Three basic topologies are used in a backup environment: direct-attached backup, LAN-based backup, and SAN-based backup.

A mixed topology is also used by combining LAN-based and SAN-based topologies.

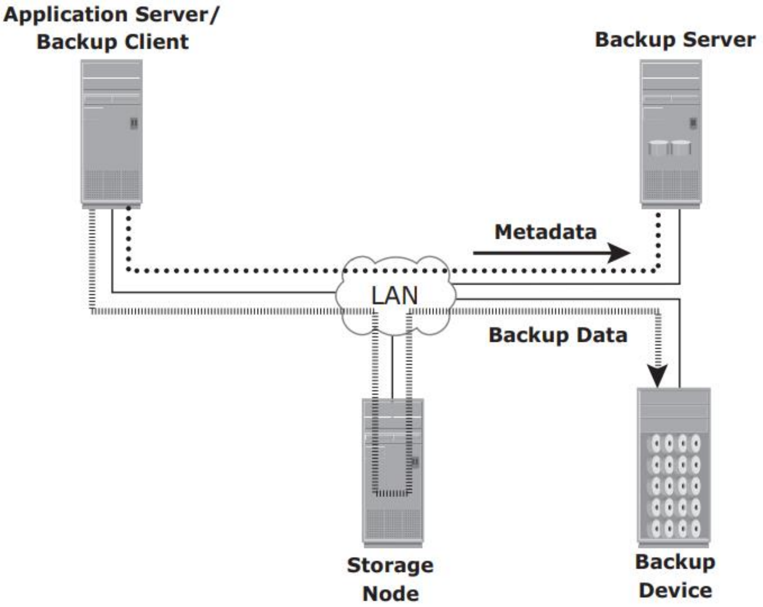
1) Direct-attached backup topology:

- In a direct-attached backup, the storage node is configured on a backup client and the backup device is attached directly to the client.
- Only the metadata is sent to the backup server through the LAN.
- This configuration frees the LAN from backup traffic.
- As the environment grows, there will be a need for centralized management and sharing of backup devices to optimize costs.
- An appropriate solution is required to share the backup devices among multiple servers.



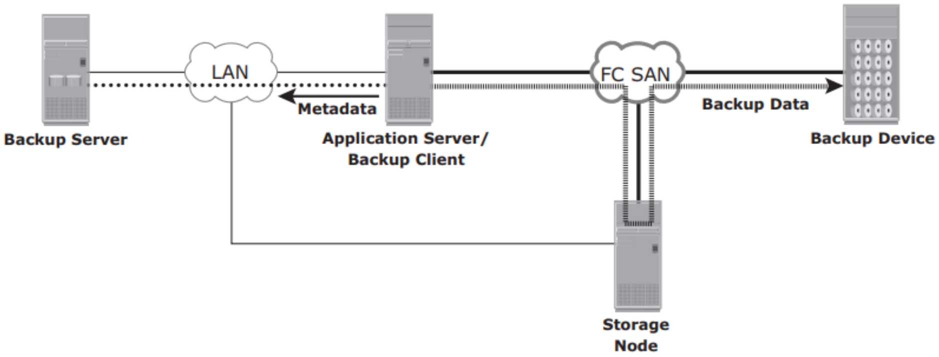
2) LAN-based backup topology:

- In a LAN-based backup, the clients, backup server, storage node and backup device are connected to the LAN.
- The data to be backed up is transferred from the backup client (source) to the backup device (destination) over the LAN, which might affect network performance.



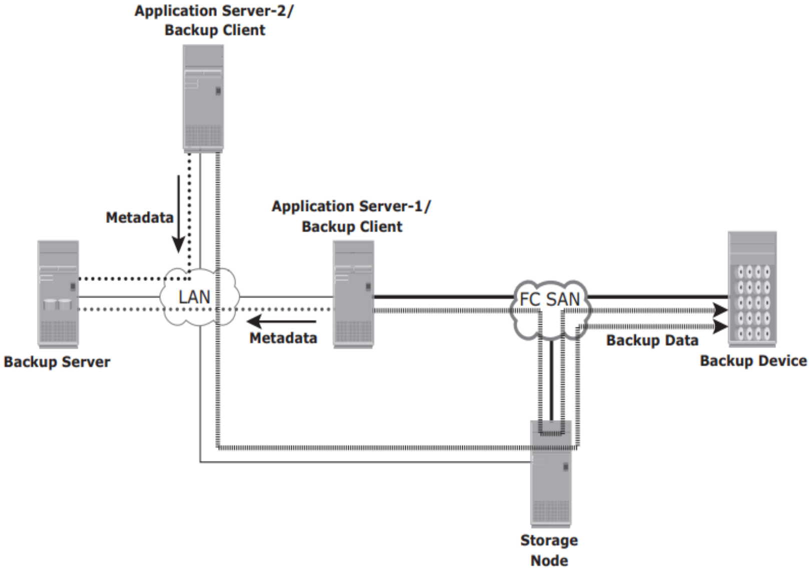
3) SAN-based backup topology:

- In SAN-based backup topology, the backup device and clients are attached to the SAN.
- In this example, a client sends the data to be backed up to the backup device over the SAN.
- Therefore, the backup data traffic is restricted to the SAN, and only the backup metadata is transported over the LAN.



4) A mixed topology:

- The mixed topology uses both the LAN-based and SAN-based topologies.
- This topology might be implemented for several reasons including cost, server location, reduction in administrative overhead and performance considerations.



7) Explain the Backup involved in NAS Environments.

Ans) In the NAS environment, backups can be implemented in different ways:

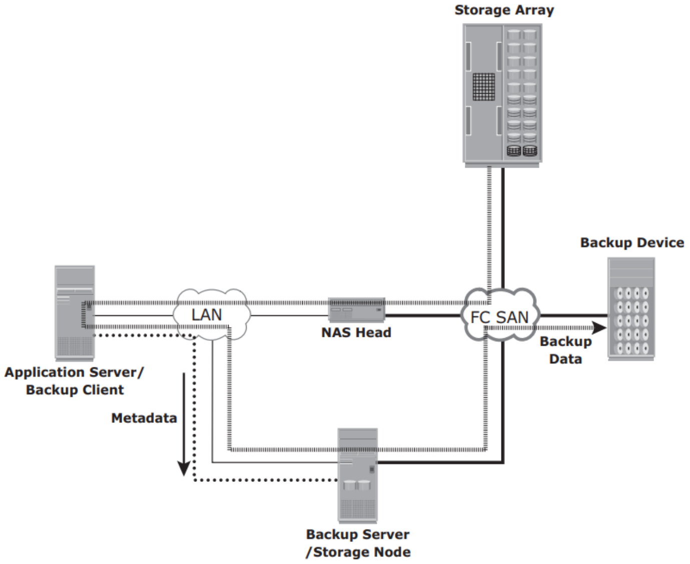
1) Server based

2) Serverless

3) Network Data Management Protocol (NDMP)

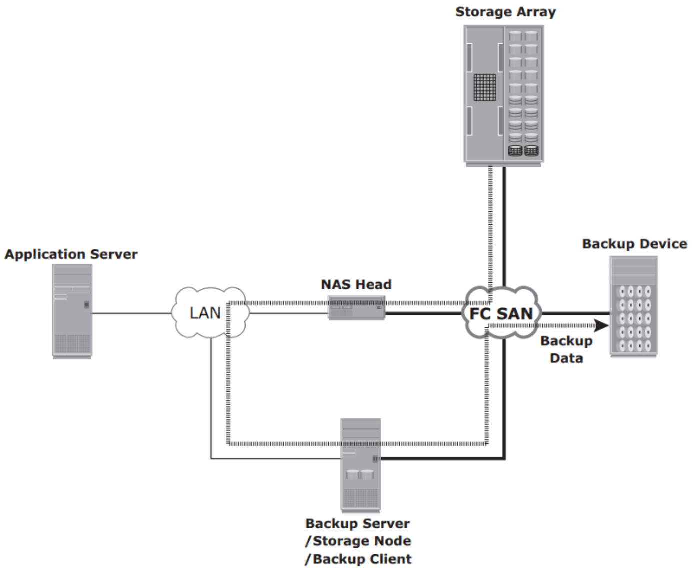
1) Server based:

- Here, the NAS head retrieves data from a storage array over the network and transfers it to the backup client running on the application server.
- The backup client sends this data to the storage node, which in turn writes the data to the backup device.
- This results in overloading the network with the backup data and using application server resources to move the backup data.



2) Serverless:

- In a serverless backup, the network share is mounted directly on the storage node.
- This avoids overloading the network during the backup process and eliminates the need of using application server resources.
- Here, the storage node, which is also a backup client, reads the data from the NAS head and writes it to the backup device without involving the application server.
- Compared to the previous solution, this eliminates one network hop.

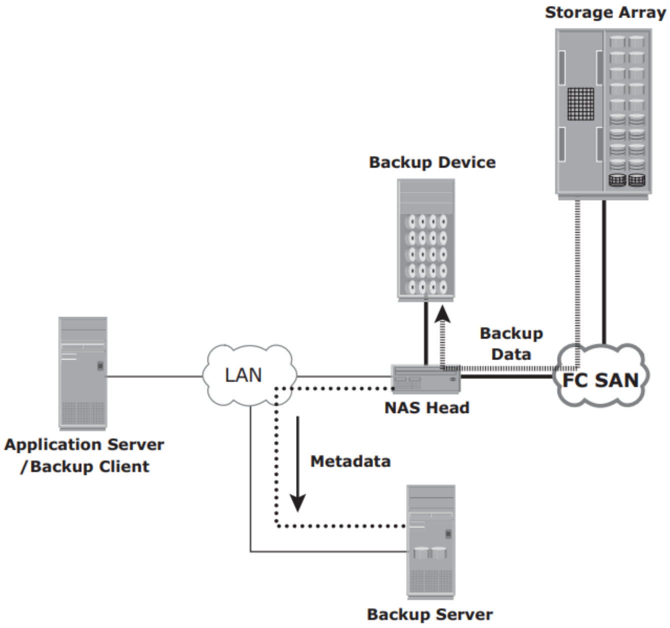


3) NDMP-Based Backup:

- NDMP is an industry-standard TCP/IP-based protocol specifically designed for a backup in a NAS environment.
- It communicates with several elements in the backup environment such as NAS head, backup devices, backup server for data transfer.
- It enables vendors to use a common protocol for the backup architecture.
- Data can be backed up using NDMP regardless of the operating system or platform.
- NDMP optimizes backup and restore by using the high-speed connection between the backup devices and the NAS head.
- In NDMP, backup data is sent directly from the NAS head to the Backup device.

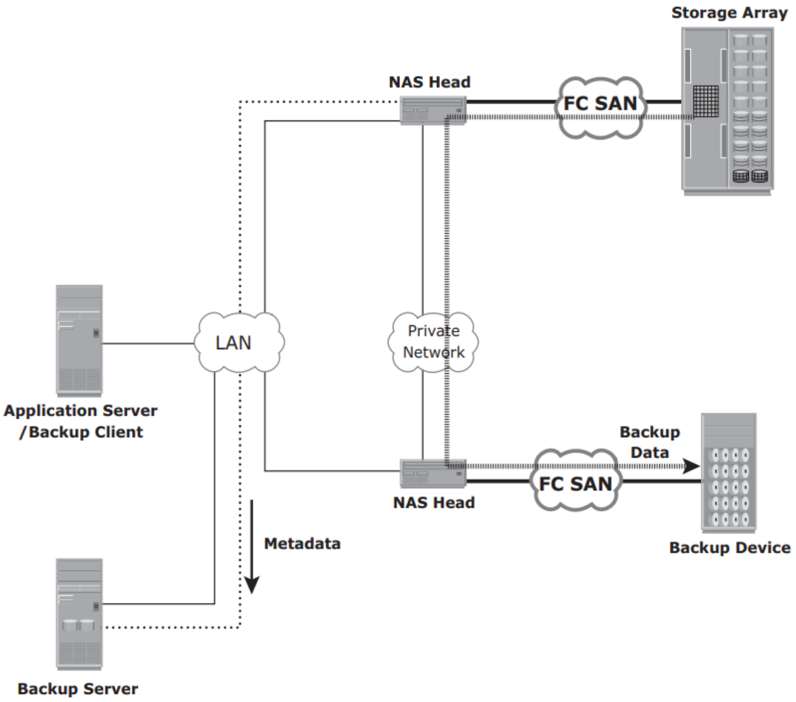
i) NDMP 2-way in a NAS environment:

- In this model, network traffic is minimized by isolating data movement from the NAS head to the locally attached backup device.
- Only metadata is transported on the network.



ii) NDMP 3-way in a NAS environment:

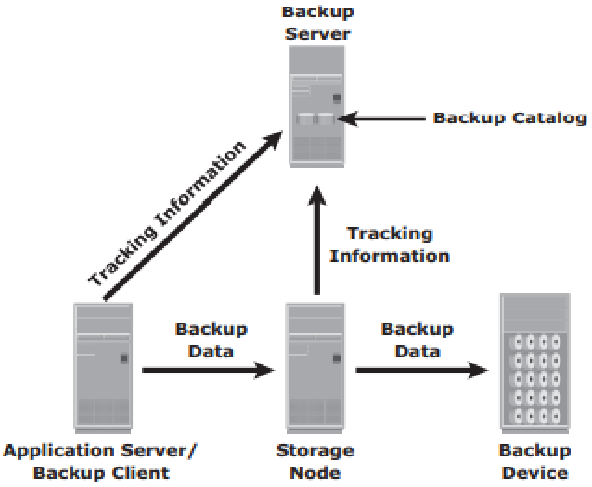
- In this model, a separate private backup network must be established between all NAS heads and the NAS head connected to the backup device.
- Metadata and NDMP control data are still transferred across the public network.



8) Write a short note on

i) Backup Architecture

Ans) A backup system commonly uses the client-server architecture with a backup server and multiple backup clients.



- The backup server manages the backup operations and maintains the backup catalog, which contains information about the backup configuration and backup metadata.
- Backup configuration contains information about when to run backups, which client data to be backed up.
- The backup metadata contains information about the backed up data.
- The role of a backup client is to gather the data that is to be backed up and send it to the storage node.
- It also sends the tracking information to the backup server.
- The storage node is responsible for writing the data to the backup device.
- The storage node also sends tracking information to the backup server.
- In many cases, the storage node is integrated with the backup server and both are hosted on the same physical platform.
- A backup device is attached directly or through a network to the storage node’s host platform.
- Backup software provides reporting capabilities based on the backup catalog and the log files.
- These reports include information, such as the amount of data backed up, the number of completed and incomplete backups and the types of errors that might have occurred.

ii) Backup purpose

Ans) Backups are performed to serve three purposes:

1) Disaster recovery

2) Operational recovery
3) Archival

1) Disaster Recovery:

- The backup copies are used for restoring data at an alternate site when the primary site is incapacitated due to a disaster.
- Based on recovery-point objective (RPO) and recovery-time objective (RTO) requirements, organizations use different data protection strategies for disaster recovery.
- The tape-based backup can be used for data restoration at the disaster recovery site.
- Organizations with stringent RPO and RTO requirements use remote replication technology to replicate data to a disaster recovery site.
- This allows organizations to bring production systems online in a relatively short period of time if a disaster occurs.

2) Operational recovery:

- Data in the production environment changes with every business transaction and operation.
- Backups are used to restore data if data loss or logical corruption occurs during routine processing.
- For example, it is common for a user to accidentally delete an important e-mail or for a file to become corrupted, which can be restored using backup data.

3) Archival:

- Backups are also performed to address archival requirements.
- Traditional backups are still used by small and medium enterprises for long-term preservation of transaction records, e-mail messages and other business records required for regulatory compliance.

9) Explain the following in 2-3 points.

i) MTBF

Ans)

- MTBF - Mean Time Between Failure
- It is the average time available for a system or component to perform its normal operations between failures.

ii) RPO

Ans)

- RPO - Recovery-Point Objective
- This is the point in time to which systems and data must be recovered after an outage.
- It defines the amount of data loss that a business can endure.

iii) MTTR

Ans)

- MTTR - Mean Time To Repair
- It is the average time required to repair a failed component.
- While calculating MTTR, it is assumed that the fault responsible for the failure is correctly identified and the required spares and personnel are available.

iv) RTO

Ans)

- RTO - Recovery-Time Objective
- Time within which systems, applications or functions must be recovered after an outage.
- It defines the amount of downtime that a business can endure and survive.

10) Explain BackUp Granularity.

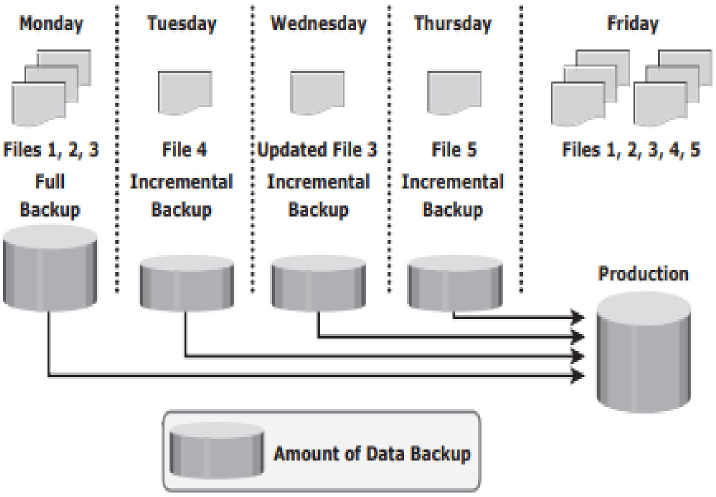
Ans) Backup granularity depends on business needs and the required RTO/RPO.
Based on the granularity, backups can be categorized as full, incremental and cumulative.

Full Backup:

Full Backup is a backup of the complete data on the production volumes.
It provides a faster recovery but requires more storage space and also takes more time to back up.

Incremental Backup:

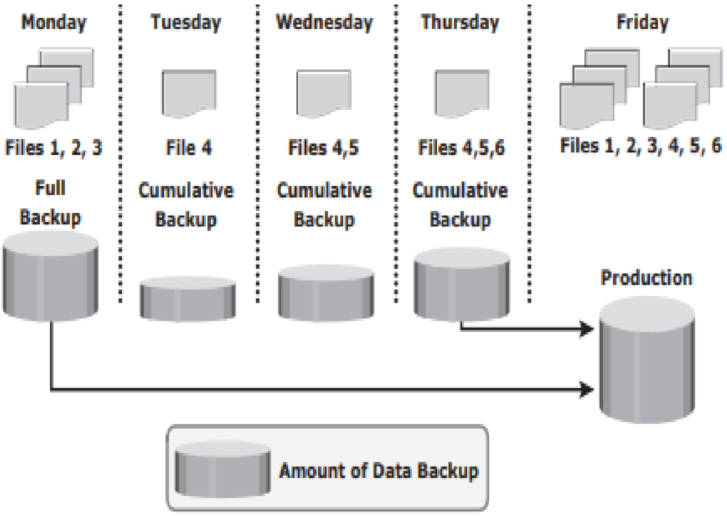
Incremental backup copies the data that has changed since the last full or incremental backup, whichever has occurred more recently.



- In this example, a full backup is performed on Monday evening.
- Each day after that, an incremental backup is performed.
- On Tuesday, a new file (File 4 in the figure) is added, and no other files have changed.
- Consequently, only file 4 is copied during the incremental backup performed on Tuesday evening.
- On Wednesday, no new files are added, but file 3 has been modified.
- Therefore, only the modified File 3 is copied during the incremental backup on Wednesday evening.
- Similarly, the incremental backup on Thursday copies only File 5.
- On Friday morning, there is data corruption, which requires data restoration from the backup.
- First step toward data restoration is restoring all data from the full backup of Monday evening.
- The next step is applying the incremental backups of Tuesday, Wednesday and Thursday.
- In this manner, data can be successfully recovered to its previous state, as it existed on Thursday evening.

Cumulative Backup:

Cumulative backup copies the data that has changed since the last full backup.
A restore from a cumulative backup requires the last full backup and the most recent cumulative backup



- In this example, a full backup of the business data is taken on Monday evening.
- Each day after that, a cumulative backup is taken.
- On Tuesday, File 4 is added and no other data is modified since the previous full backup of Monday evening.
- Consequently, the cumulative backup on Tuesday evening copies only File 4.
- On Wednesday, File 5 is added.
- The cumulative backup taking place on Wednesday evening copies both File 4 and File 5 because these files have been added or modified since the last full backup.
- Similarly, on Thursday, File 6 is added.
- Therefore, the cumulative backup on Thursday evening copies all three files: File 4, File 5 and File 6.
- On Friday morning, data corruption occurs that requires data restoration using backup copies.
- The first step in restoring data is to restore all the data from the full backup of Monday evening.
- The next step is to apply only the latest cumulative backup, which is taken on Thursday evening.
- In this way, the production data can be recovered faster because its needs only two copies of data — the last full backup and the latest cumulative backup.