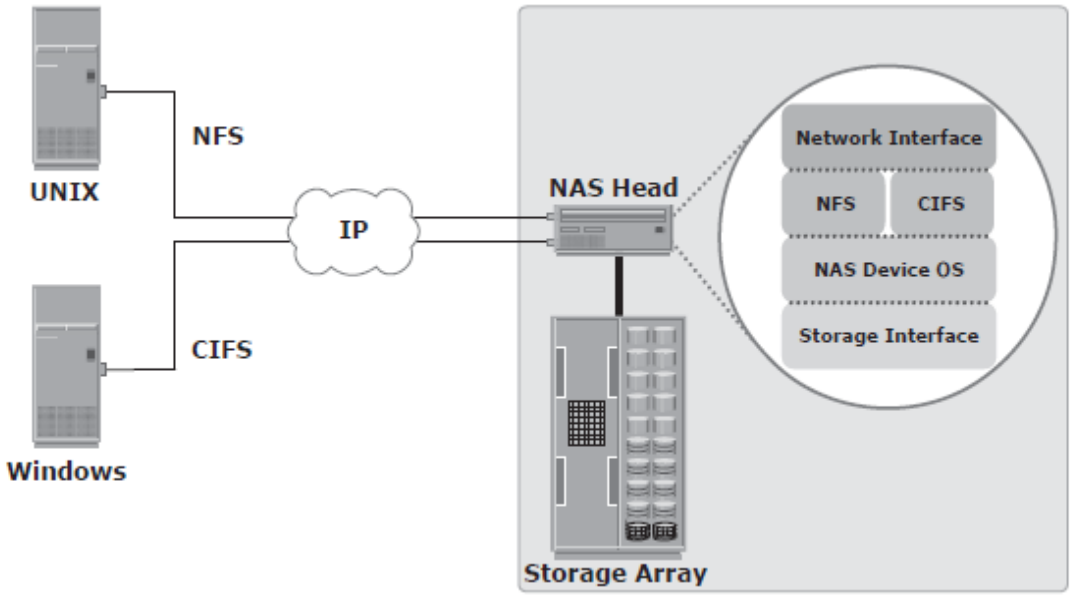
Components of NAS

- ➔ A NAS device has two key components: NAS head and storage.
- ➔ CPU and memory
- ➔ One or more network interface cards (NICs), which provide connectivity to the client network. Examples of network protocols supported by NIC include Gigabit Ethernet, Fast Ethernet, ATM, and Fiber Distributed Data Interface (FDDI).
- ➔ An optimized operating system for managing the NAS functionality.
- ➔ It translates fi le-level requests into block-storage requests and further converts the data supplied at the block level to fi le data.
- ➔ NFS, CIFS, and other protocols for fi le sharing Industry-standard storage protocols and ports to connect and manage physical disk resources.



Factors Affecting NAS Performance

- ➔ 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.
- ➔ Authentication with a directory service such as Active Directory or NIS:
  The authentication service must be available on the network with enough resources to accommodate the authentication load. Otherwise, a large number of authentication requests can increase latency.
- ➔ Retransmission: Link errors and buffer overfl ows can result in retransmission. This causes packets that have not reached the specifi ed destination to be re-sent. Care must be taken to match both speed and duplex settings on the network devices and the NAS heads. Improper configuration might result in errors and retransmission, adding to latency.
- ➔ Overutilized routers and switches: The amount of time that anoverutilized 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 utilization statistics to determine the optimum

- ➔ File system lookup and metadata requests: NAS clients access files on NAS devices. The processing required to reach the appropriate fi le or directory can cause delays
- ➔ Over utilized NAS devices: Clients accessing multiple fi les can cause high utilization levels on a NAS device, which can be determined by viewing utilization statistics.

BC Planning Life Cycle

- ➔ Establishing objectives
- ➔ Analyzing
- ➔ Desig.ning and developing
- ➔ Implementing
- ➔ Training, testing, assessing, and maintaining

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 profi les, 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 and create Perform cost benefi t 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.
   - ➢ 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 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.
   - ➢ 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 refl ect regular changes within the data center

Business continuity RPO RTO

Recovery-Point Objective (RPO):

- 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.
- A large RPO signifies high toleranceto information loss in a business.
- **RPO of 24 hours:** Backups are created at an offsite tape library every midnight. The corresponding recovery strategy is to restore data from the set of last backup tapes.
- **RPO of 1 hour:** Shipping database logs to the remote site every hour. The corresponding recovery strategy is to recover the database to the point of the last log shipment.
- **RPO in the order of minutes:** Mirroring data asynchronously to a remote site.
- **Near zero RPO:** Mirroring data synchronously to a remote site.

Recovery-Time Objective (RTO):

- The time within which systems and applications must be recovered after an outage. It defines the amount of downtime that a business can endure and survive.
- Businesses can optimize disaster recovery plans after defining the RTO for a given system.

Measuring Information MTTF and MTTR

- **Mean Time Between Failure (MTBF):**

  It is the average time available for a system or component to perform its normal operations between failures. It is the measure of system or component reliability and is usually expressed in hours.

- **Mean Time To Repair (MTTR):**

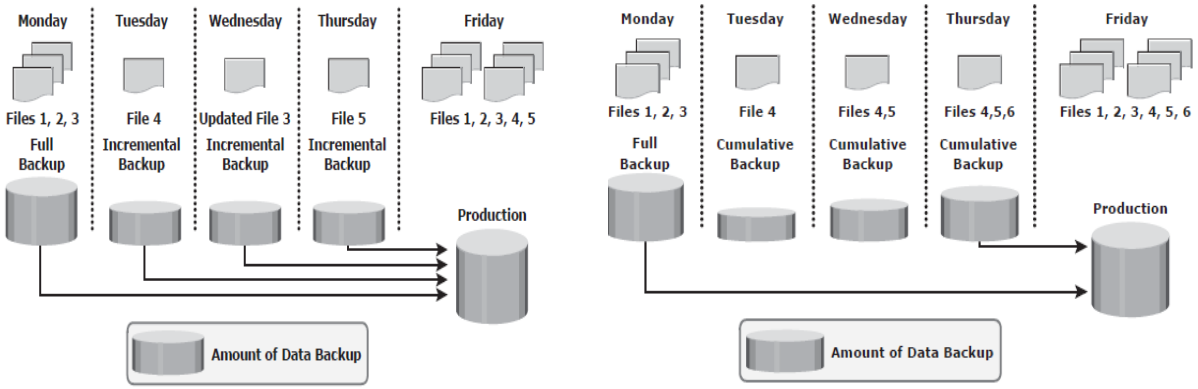
  It is the average time required to repair a failed component. While calculating MTTR, it is assumed that the fault responsible for the failure is correctly identifi ed and the required spares and personnel are available.

  IA = system uptime/(system uptime + system downtime)

  IA = MTBF/(MTBF + MTTR)

Backup Granularity

- 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 is a backup of the complete data on the production volumes. A full backup copy is created by copying the data in the prIt provides a faster recovery but requires more storage
- ***Full backup space*** and also takes more time to back up.oduction volumes to a backup storage device
- ***Incremental backup*** copies the data that has changed since the last fullor incremental backup, whichever has occurred more recently. This is much faster than a full backup (because the volume of data backed up is restricted to the changed data only) but takes longer to restore.
- ***Cumulative backup*** copies the data that has changed since the last full backup. This method takes longer than an incremental backup but is faster to restore.



Incremental and cumulative backup

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 fi le is open, it is normally not backed up duringthe backup process. In such situations, an open fi le agent is required to back up the open file.
- These agents interact directly with the operating system or application and enable the creation of consistent copies of open files.
- disadvantage associated with a hot backup is that the agents usually affect the overall application performance.
- Consistent backups of databases can also be done by using a cold backup.This requires the database to remain inactive during the backup.
- 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 Production volume.
- Attributes are as important as the data itself and must be backed up for consistency.
- In a disaster recovery environment, bare-metal recovery (BMR) refers to a backupin which all metadata, system information, and application configurations are appropriately backed up for a full system recovery.
- BMR builds the base system,which includes partitioning, the file system layout, the operating system, the applications,and all the relevant configurations.
- BMR recovers the base system fi rst before starting the recovery of data files. Some BMR technologies — for example server confi guration backup (SCB) can recover a server even onto dissimilar hardware.

IP San protocol

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

InternetSCSI (iSCSI)

- iSCSI is encapsulation of SCSI I/O over IP.,
- 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.
- iSCSI is widely adopted for connecting servers to storage because it is relatively inexpensive and easy to implement.

Fibre Channel over IP (FCIP).

- FCIP is a protocol in which an FCIP entity such as an FCIP gateway is used to tunnel FC fabrics through an IP network.,
- 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 Ethernet (FcoE).

Compare Object Oriented Storage Device, NAS, Content Oriented Storage Device

NAS	OOSD	COSD
NAS,or Network Attached Storage, is the main and primary shared storage architecture for file storage, which has been the ubiquitous and familiar way to store data for a long time, based on	Object Storage was developed to address the scalability requirements, geographic reach, and economics of massive data storage, data is stored in objects that carry a unique ID and	

a traditional file system comprising files organized in hierarchical directories.	embed an extensible set of metadata.	
ADV		
File storage has been around for so long that it is ingrained in IT and consumer domains. Devices and applications out there leverage such an interface when it comes to storing or retrieving data.	->Unlimited scalability ->Geographic reach (access anywhere) ->Single namespace ->Built-in data resilience ->Extensible and flexible metadata tagging	
DISADV		
While NAS performs well at small to medium scale, it breaks down at large scale due to the overhead of the underlying file system that must be maintained, as well as limitations of related data protection schemes that must be implemented to safeguard data (RAID).	One typical challenge is dealing with the native REST interface used by Object Storage solutions. Another consideration for Object Storage is that objects can’t be updated partially, meaning the entire object must be stored at once This makes Object Storage mostly suitable for nearly static or infrequently changed data sets.	