UNIT-3

INTRODUCTION TO BUSINESS CONTINUITY

Introduction

Upon completion of this module, you should be able to:

- Define business continuity (BC) and information availability (IA)
- Explain the impact of information unavailability
- Describe BC planning process
- Explain business impact analysis (BIA)
- Explain BC technology solutions

Why Business Continuity (BC)?

- Information is an organization's most important asset
- Continuous access to information ensures smooth functioning of business operations
- Cost of unavailability of information to an organization is greater than ever

Threats to information availability

Natural disasters	Unplanned occurrences	Planned occurrences
• flood, fire, earthquake	• cybercrime, human error, network and computer failure	• upgrades, backup, restore • result in the inaccessibility of information

What is Business Continuity?

Business Continuity

It is a process that prepares for, responds to, and recovers from a system outage that can adversely affects business operations.

An integrated and enterprise-wide process that includes set of activities to ensure "**information availability**"

BC involves **proactive measures** (data protection, and security) and **reactive countermeasures** (disaster recovery and restart) to be invoked in the event of a failure.

In a virtualized environment, BC solutions need to protect **both** physical and virtualized resources.

The goal of a BC solution is to ensure the "**information availability**" required to conduct vital business operations.

Information Availability

Information Availability

It is the ability of an IT infrastructure to function according to business expectations, during its specified time of operation.

- Information availability can be defined with the help of:

Accessibility

- Information should be accessible to the right user when required

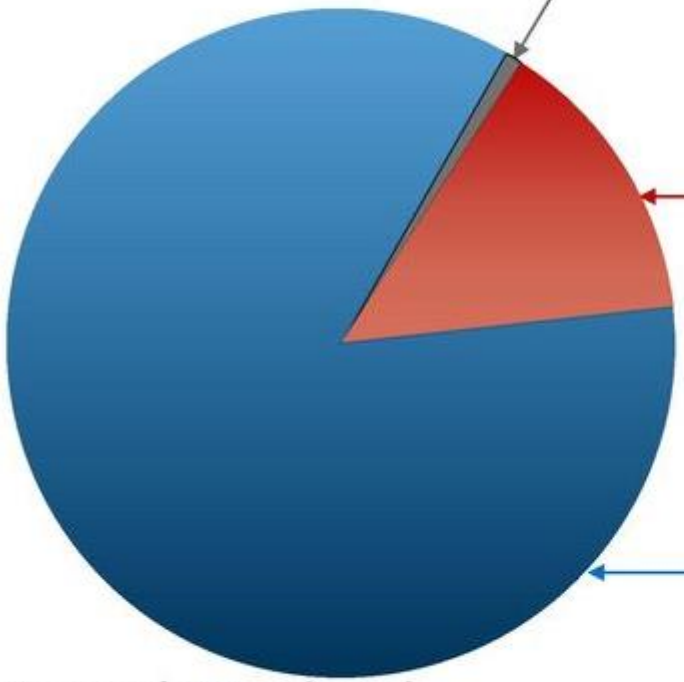
Reliability

- Information should be reliable and correct in all aspects

Timeliness

- Defines the time window during which information must be accessible

Causes of Information Unavailability



Disaster (<1% of Occurrences)

Natural or man made disaster

- Flood
- Fire
- Earthquake
- Contamination

Unplanned Outages (20%)

Failure

- Database corruption
- Component (physical and/or virtual) failure
- Human error

Planned Outages (80%)-expected and scheduled but still cause data to be unavailable

Competing workloads

- Backup, reporting
- Data warehouse extracts
- Application and data restore

- Various planned and unplanned incidents result in data unavailability

Impact of Downtime

Know the downtime costs (per hour, day, two days, and so on.)

Lost Productivity

- Number of employees impacted x hours out x hourly rate

Lost Revenue

- Direct loss
- Compensatory payments
- Lost future revenue
- Billing losses
- Investment losses

Damaged Reputation

- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Financial Performance

- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Other Expenses

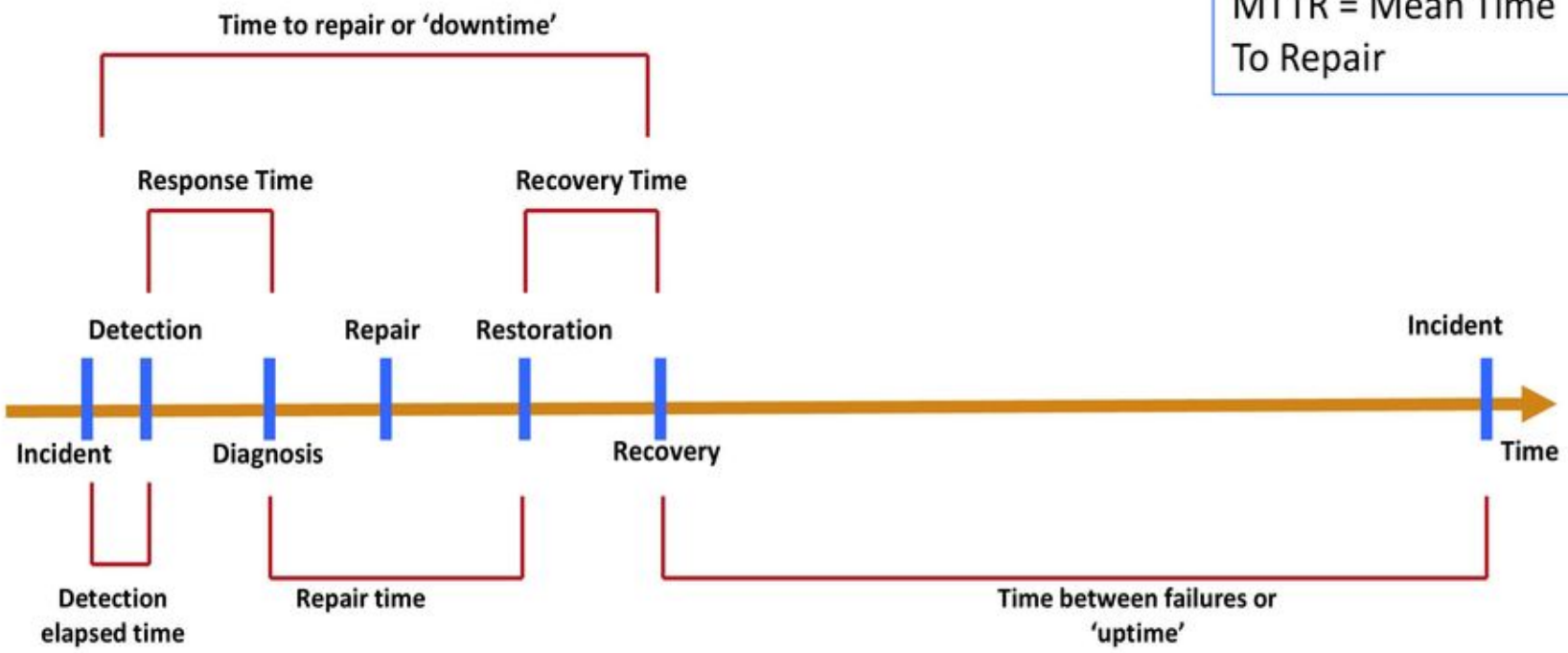
- Temporary employees, equipment rental, overtime costs, extra shipping costs, travel expenses, and so on.

Measuring Information Availability

- Information availability relies on the **availability** of **both** physical and virtual components of a data center.
- **Failure** of these components might **disrupt** information availability.
  - A failure is the termination of a component's ability to perform a required function.
- The component's ability can be restored by performing an external **corrective actions**, such as a manual reboot, a repair, or replacement of the failed component(s).
- Proactive risk analysis, performed as part of the BC planning process, considers the component failure rate and average repair time, which are measured by **MTBF (Mean Time Between Failure)** and **MTTR (Mean Time To Repair)**

Measuring Information Availability (contd.)

MTBF = Mean Time Between Failure
MTTR = Mean Time To Repair



- MTBF: Average time available for a system or component to perform its normal operations between failures

  MTBF = Total uptime/Number of failures

- MTTR: Average time required to repair a failed component

  MTTR = Total downtime/Number of failures

Measuring Information Availability (contd.)

MTBF = Mean Time Between Failure
MTTR = Mean Time To Repair

- IA can be expressed in terms of system uptime and downtime and measured as the amount or percentage of system uptime:

  IA = MTBF/(MTBF + MTTR) or IA = uptime/(uptime + downtime)

  - System uptime is the period of time during which the system is in an accessible state
  - System downtime is the period of time during which the system is not accessible state

BC Terminologies – 1

Disaster recovery

Coordinated process of restoring systems, data, and infrastructure required to support business operations after a disaster occurs

Restoring previous copy of data and applying logs to that copy to bring it to a known point of consistency

Generally implies use of **backup** technology

Disaster restart

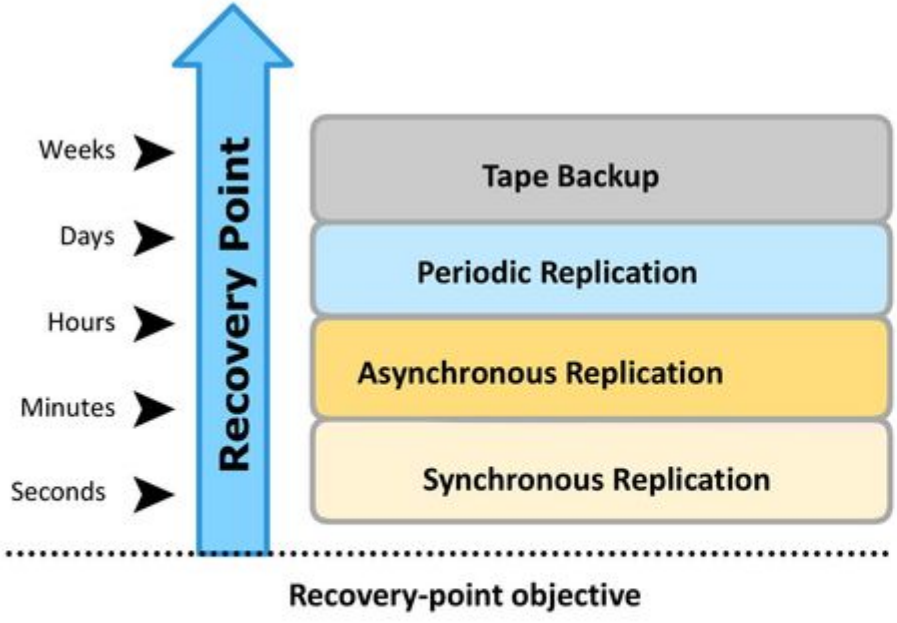
Process of restarting business operations with mirrored consistent copies of data and applications

Generally implies use of **replication** technologies

BC Terminologies – 2

Recovery-Point Objective (RPO)

- Point-in-time to which systems and data must be recovered after an outage
- Amount of data loss that a business can endure



- Based on the RPO, organizations plan for the frequency with which a backup or replica must be made

RPO of 24 hours: Backups are created at an offsite tape library every midnight. Recovery strategy: to restore data from the set of last backup tapes.

RPO of 6 hours: Backups must be made at least once in 6 hours

RPO of 1 hour: Backup to the remote sit every hour. Recovery strategy is to recover the database to the point of the last log shipment.

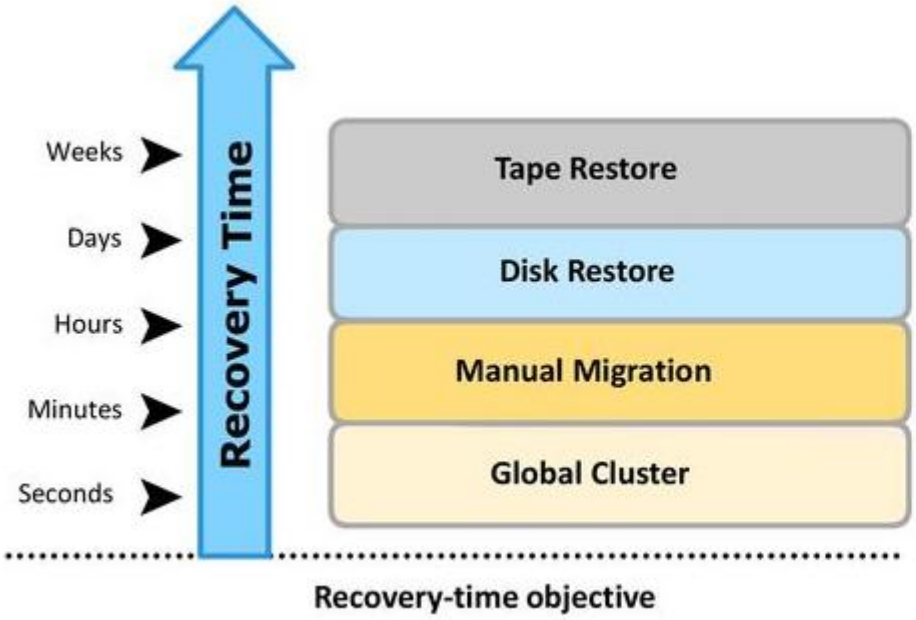
RPO in the order of minutes: Mirroring data asynchronously to a remote site.

RPO of zero: Mirroring data synchronously to a remote site.

BC Terminologies – 2

Recovery-Time Objective (RTO)

- Time within which systems and applications must be recovered after an outage
- Amount of downtime that a business can endure and survive



- Based on the RTO, organizations plan for recovery strategies to ensure data availability

RTO of 72 hours: Restore from tapes available at a cold site

RTO of 12 hours: Restore from tapes available at a hot site.

RTO of few hours: Use disk-based backup technology, which gives faster restore than a tape backup.

RTO of a few seconds: Cluster production servers with bidirectional mirroring, enabling the applications to run at both sites simultaneously.

Cold site: a site when operations can be moved in the event of disaster, with minimum IT infrastructure in place, but not activated

Hot site: a site when operations can be moved in the event of disaster. All equipment is available and running at all times

BC Planning Lifecycle

- 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.

- Collect information on data profiles, business processes, infrastructure support
- Conduct a business impact analysis.
- Identify critical business processes and assign recovery priorities.
- Perform risk analysis for critical functions and create mitigation strategies.
- Perform cost benefit analysis.
- Evaluate options.

- Define the team structure and assign individual roles and responsibilities
- Design data protection strategies and develop infrastructure
- Develop contingency solution

- Implement risk management and mitigation procedures
- Prepare the DR 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

- Train the employees who are responsible for backup and replication
- Train employees on emergency response procedures
- Perform damage-assessment processes and review recovery plans
- Test the BC plan regularly to evaluate its performance and identify its limitations

Failure Analysis

- Involves analyzing both physical and virtual infrastructure components
  - To identify systems that are susceptible to a single point of failure and implementing fault-tolerance mechanisms.

Single Point of Failure

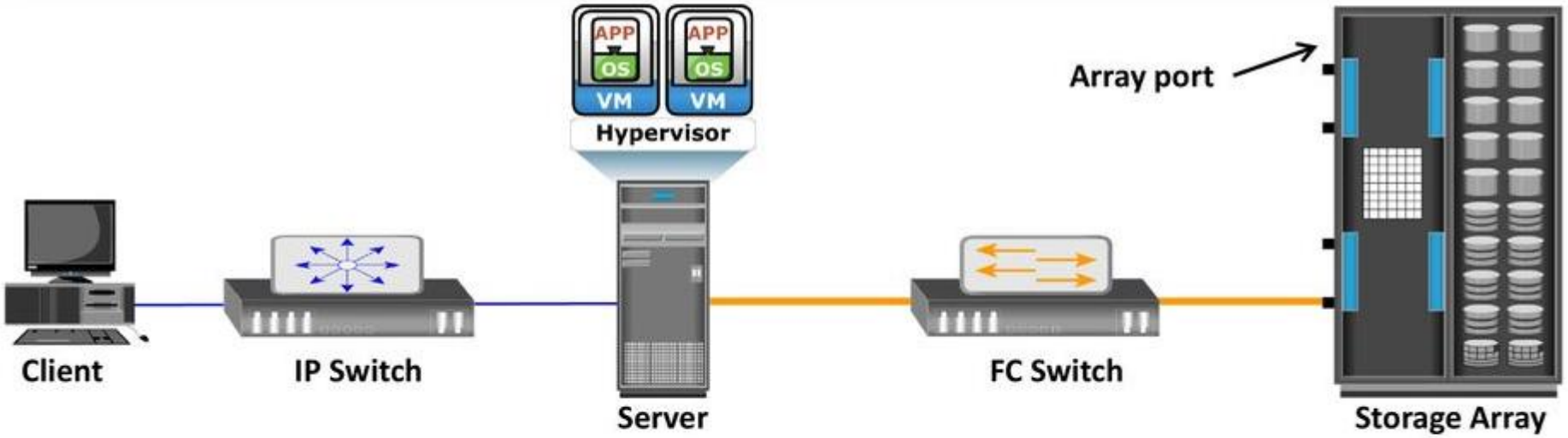
Resolving Single Points of Failure

Multipathing Software

Failure Analysis: (1) Single Points of Failure

Single Points of Failure

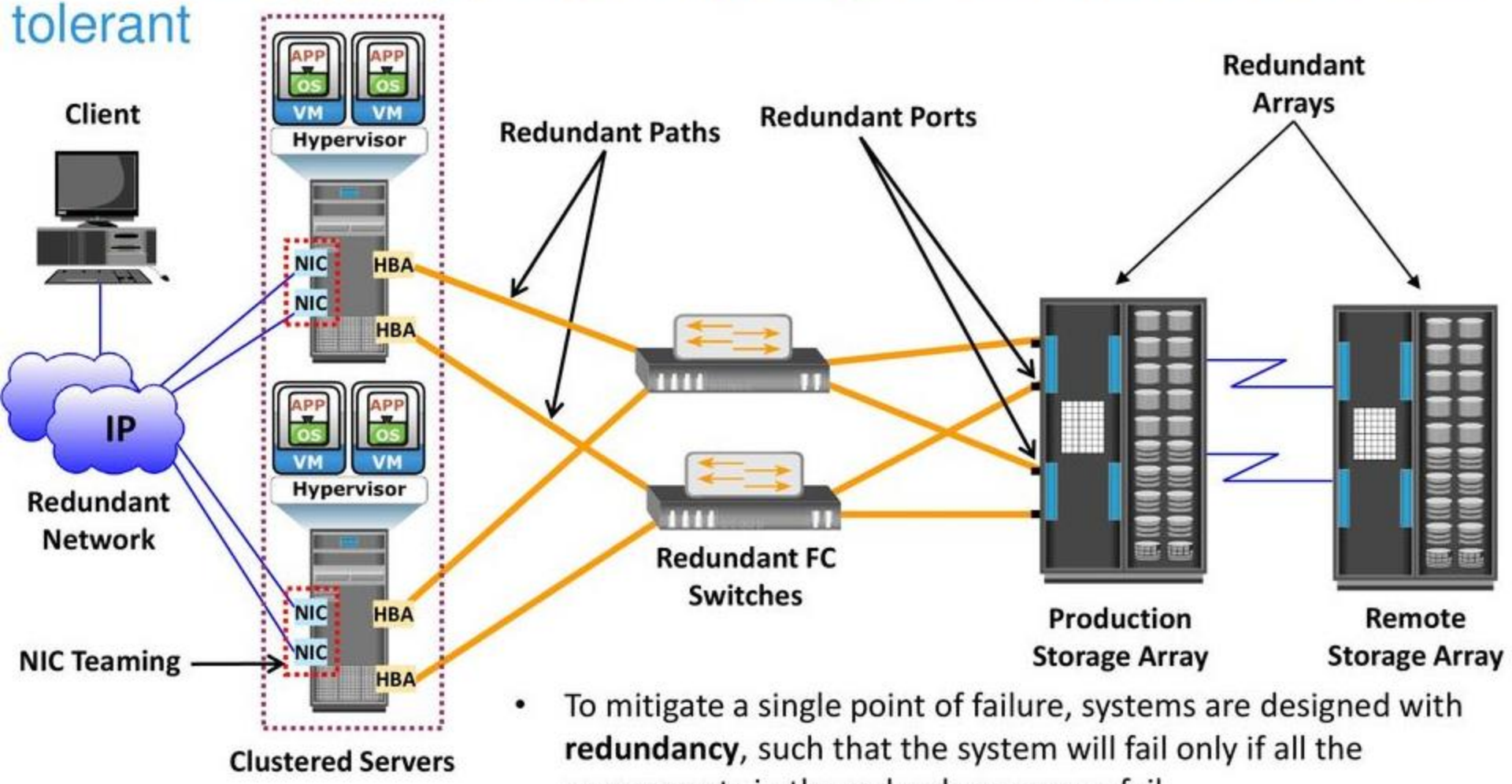
It refers to the failure of a component of a system that can terminate the availability of the entire system or IT service.



A VM, a hypervisor, or an HBA/NIC on the server, the physical server itself, the IP network, the FC switch, the storage array port, or even the storage array could be a potential single point of failure

E.g.: For example, failure of a hypervisor can affect all the running VMs and virtual network, which are hosted on it

Failure Analysis: (2) Resolving Single Points of Failure / Fault tolerant



- To mitigate a single point of failure, systems are designed with **redundancy**, such that the system will fail only if all the components in the redundancy group fail.
- This ensures that the failure of a single component **does not affect data availability**.
- **Careful analysis** is performed to eliminate every single point of failure

Failure Analysis: (2) Resolving Single Points of Failure / Fault tolerant

- Based on the figure, implementation to resolve single points of failure includes:
  - Configuration of multiple HBAs to mitigate single HBA failure.
  - Configuration of multiple fabrics to account for a switch failure.
  - Configuration of multiple storage array ports to enhance the storage array's availability.
  - RAID configuration to ensure continuous operation in the event of disk failure.
  - Implementing a storage array at a remote site to mitigate local site failure.
  - Implementing server (host) clustering, a fault-tolerance mechanism whereby two or more servers in a cluster access the same set of volumes.
    - Clustered servers exchange *heartbeats* to inform each other about their health.
    - If one of the servers fails, the other server takes up the complete workload.

Failure Analysis: (3) Multipathing Software

- Configuration of multiple paths **increases** the **data availability** through path failover
- Multipathing software provides the functionality to **recognize** and **utilize alternative** I/O paths to data

Provides **load balancing** by distributing I/Os to all available, active paths:	**Intelligently** manages the paths to a device by sending I/O down the optimal path:
• Improves I/O performance and data path utilization	• Based on the load balancing and failover policy setting for the device

- E.g.: Microsoft Multipath I/O (MPIO) is a Microsoft-provided framework that allows storage providers to develop multipath solutions that contain the hardware-specific information needed to optimize connectivity with their storage arrays

Business Impact Analysis

- Identifies which business units and processes are **essential** to the survival of the business
- BIA includes the following set of tasks:
  - Determine the **business areas**
  - Identify **key** business processes critical to its operation
  - Determine **attributes** of the business process: applications, databases, h/w, s/w
  - Estimates the **cost of failure** for each business process
  - Calculates the **maximum tolerable outage** and defines **RTO** for each business process
  - Businesses can prioritize and implement **countermeasures** to mitigate the likelihood of such disruptions

BC Technology Solutions

- After analyzing the business impact of an outage, designing the appropriate solutions to recover from a failure is the next important activity
- Solutions that enable BC are:
  - Fault tolerant configuration
    - Done by implementing redundancies
    - Resolving single points of failure
  - Multipathing software
  - Backup and replication
    - Backup and recovery
    - Local replication
    - Remote replication

Backup and Replication

Note: Backup and Replication will be discussed in forthcoming modules.

Backup and Recovery

- Backup to tape has been a predominant method to ensure BC
- Frequency of backup is determined based on RPO, RTO, and the frequency of data changes

Local Replication

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

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, BC operations start from the remote storage array.

Backup and Recovery

Upon completion of this module, you will be able to:

- Describe best practices for planning Backup and Recovery.
- Describe the common media and types of data that are part of a Backup and Recovery strategy.
- Describe the common Backup and Recovery topologies.
- Describe the Backup and Recovery Process.
- Describe Management considerations for Backup and Recovery.

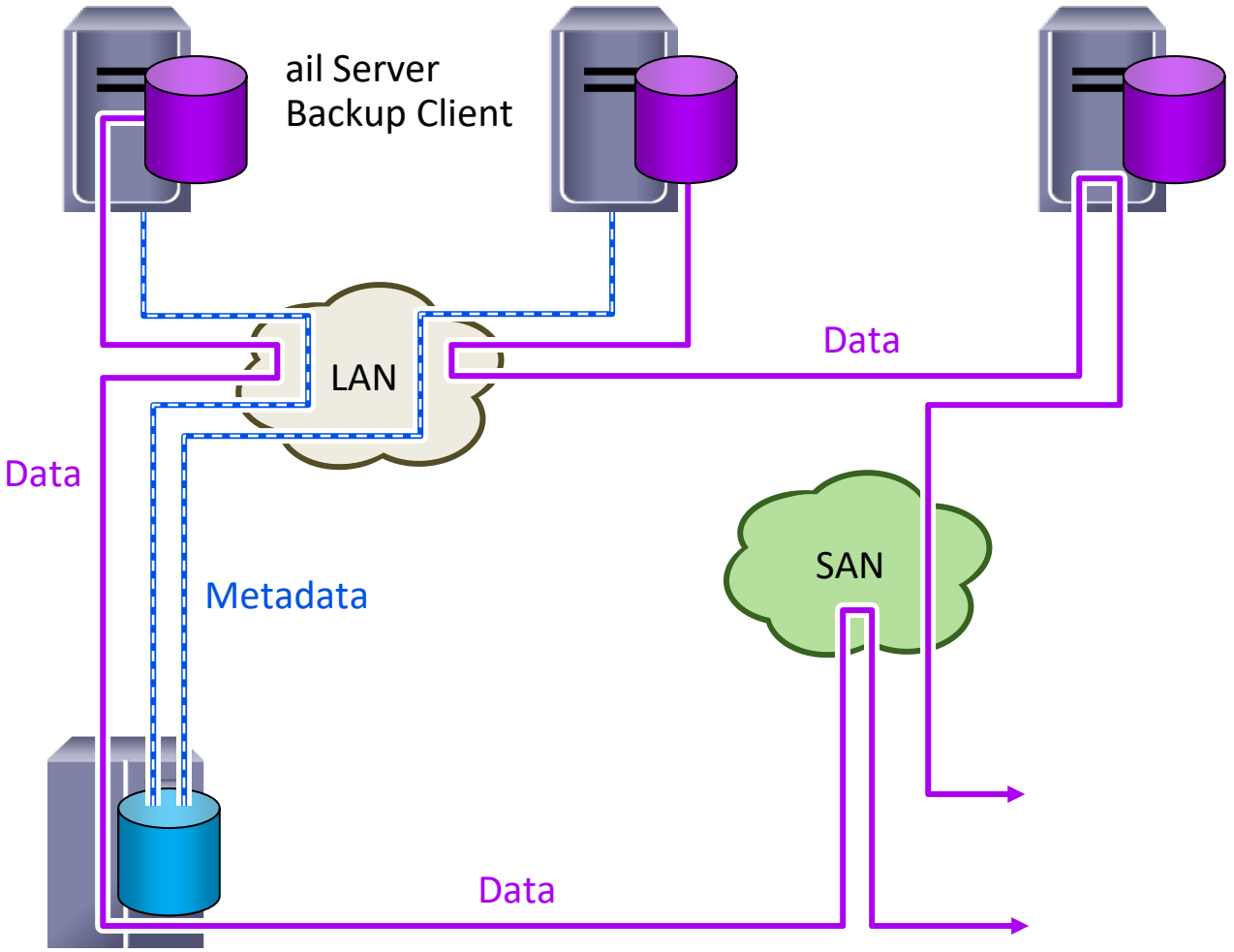
Business Considerations

- Customer business needs determine:
  - What are the restore requirements – RPO & RTO?
  - Where and when will the restores occur?
  - What are the most frequent restore requests?
  - Which data needs to be backed up?
  - How frequently should data be backed up?
    - hourly, daily, weekly, monthly
  - How long will it take to backup?
  - How many copies to create?
  - How long to retain backup copies?

Backup Architecture Topologies

- There are 3 basic backup topologies:
  - Direct Attached Based Backup
  - LAN Based Backup
  - SAN Based Backup
- These topologies can be integrated, forming a “mixed” topology

SAN/LAN Mixed Based Backups



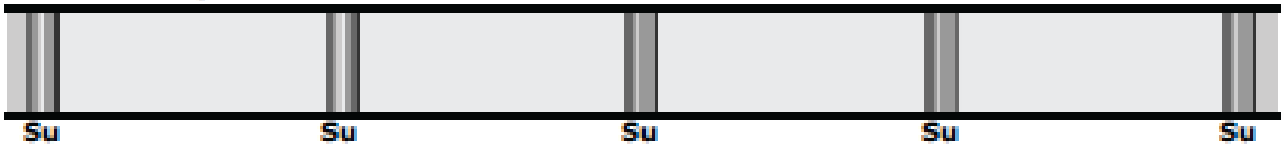
Backup Purpose

- Disaster recovery
- Operational backup
- Archival

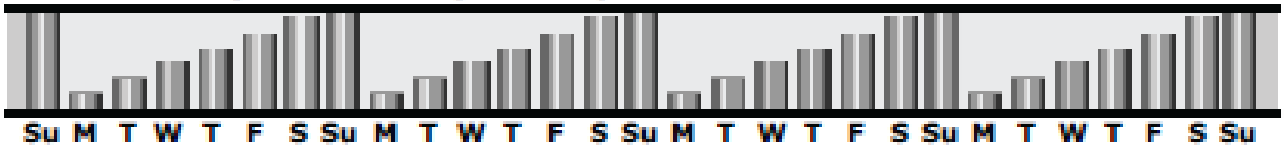
Backup Granularity

- Backup granularity depends on business needs and required RTO/RPO.
- Based on granularity, backups can be categorized as full, cumulative, and incremental.
- *Full backup* is a backup of the complete data on the production volumes at a certain point in time.
- *Incremental backup* copies the data that has changed since the last full or incremental backup, whichever has occurred more recently.
- *Cumulative* (or *differential*) *backup* copies the data that has changed since the last full backup. This method takes longer than incremental backup but is faster to restore.

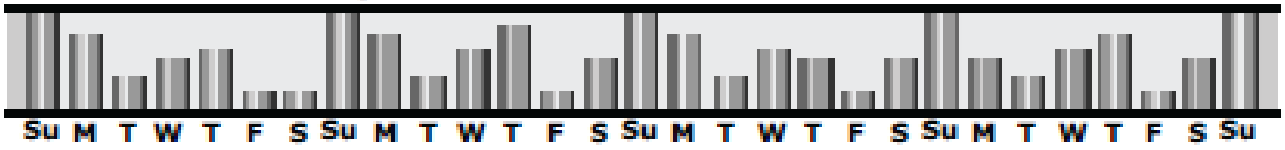
Full Backup

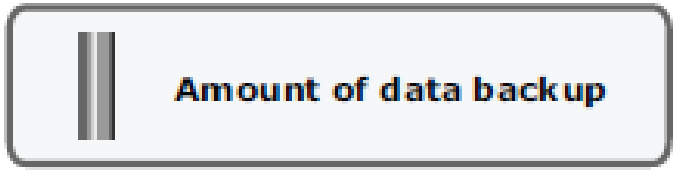


Cumulative (Differential) Backup

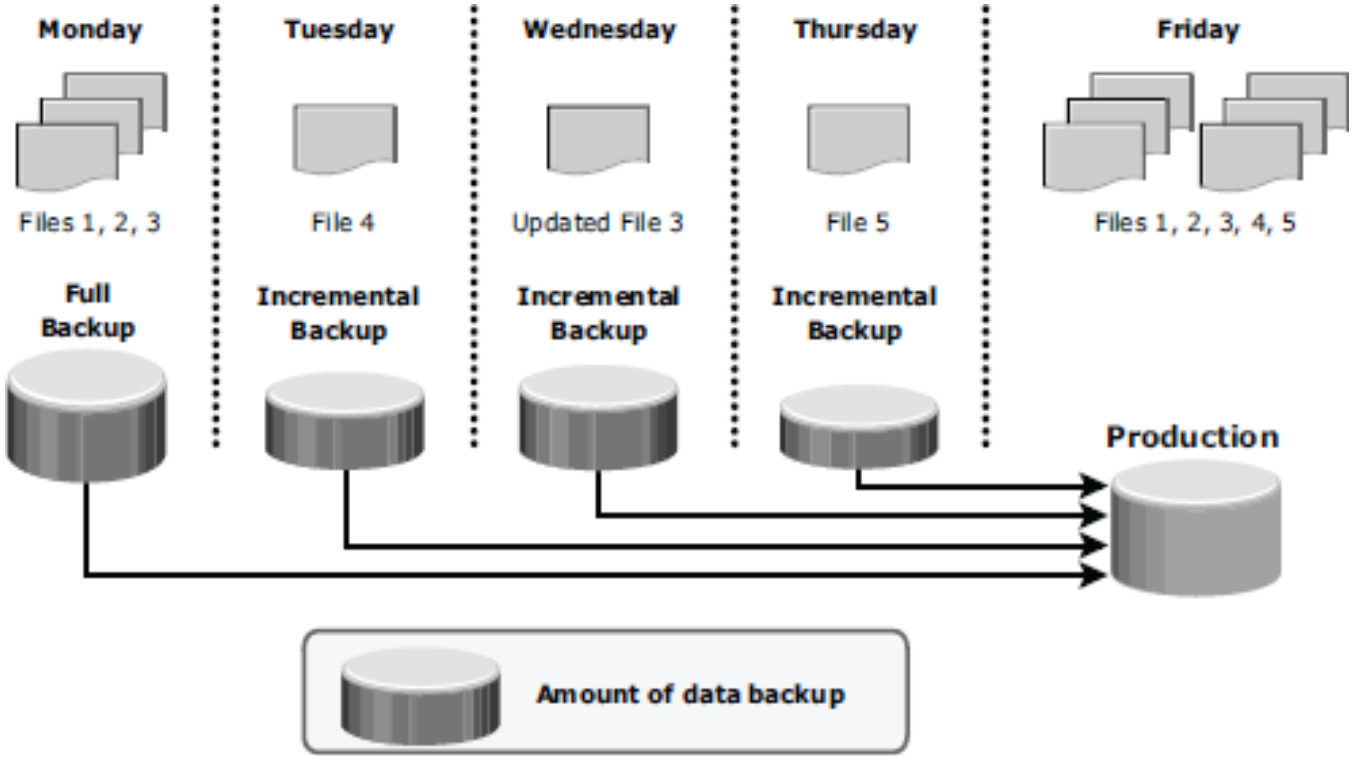


Incremental Backup





Restoring from an incremental backup



Recovery Considerations

- RPO and RTO are major considerations when planning a backup strategy.
- RPO defines the tolerable limit of data loss for a business and specifies the time interval between two backups.

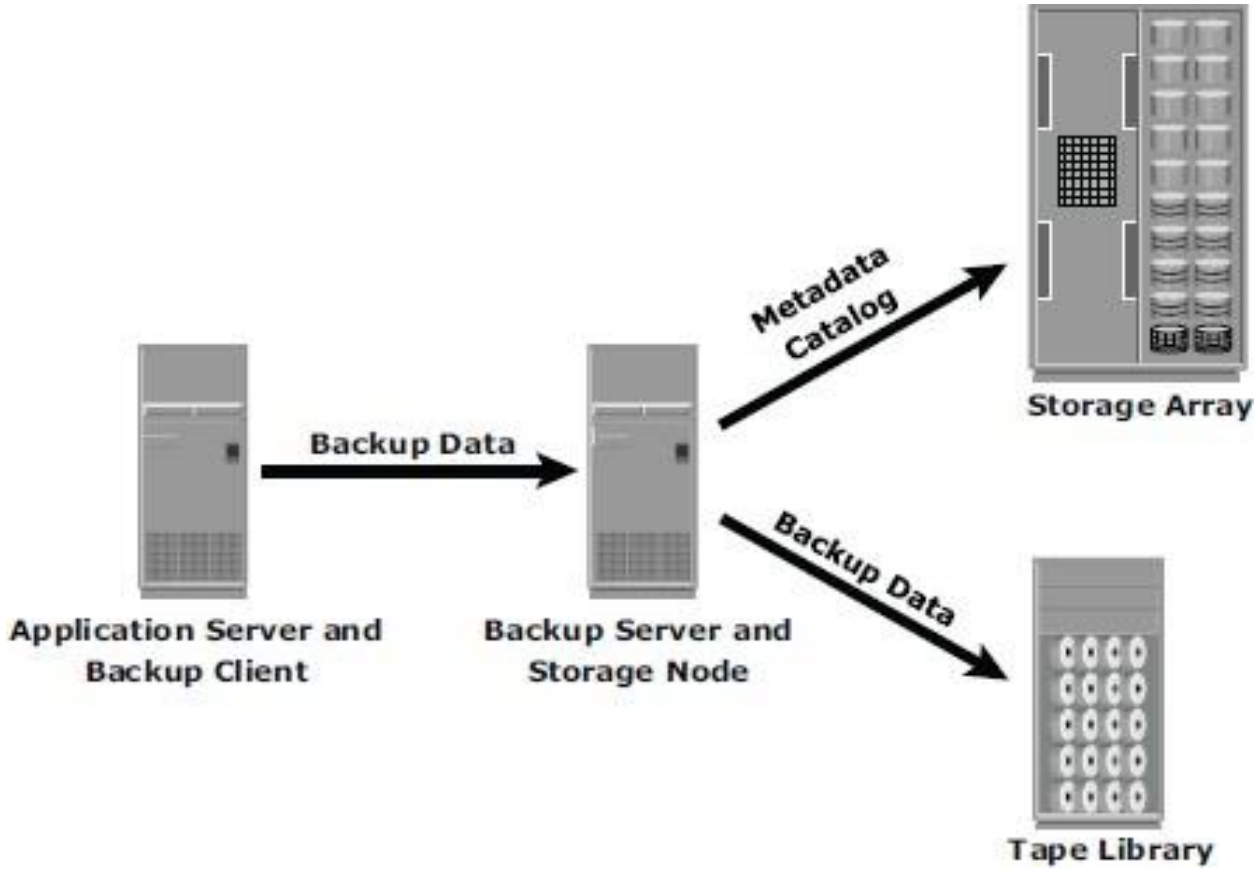
Backup Methods

- Hot backup and cold backup are the two methods deployed for backup.
- They are 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. In a *cold backup*, the application is not active during the backup process.
- A *point-in-time (PIT)* copy method is deployed in environments where the impact of downtime from a cold backup or the performance resulting from a hot backup is unacceptable.

Backup Architecture

- A backup system uses client/server architecture with a backup server and multiple backup clients.
- The backup server depends on backup clients to gather the data to be backed up.
- Some backup architecture refers to the storage node as the *media server* because it connects to the storage device. Storage nodes play an important role in backup planning because they can be used to consolidate backup servers

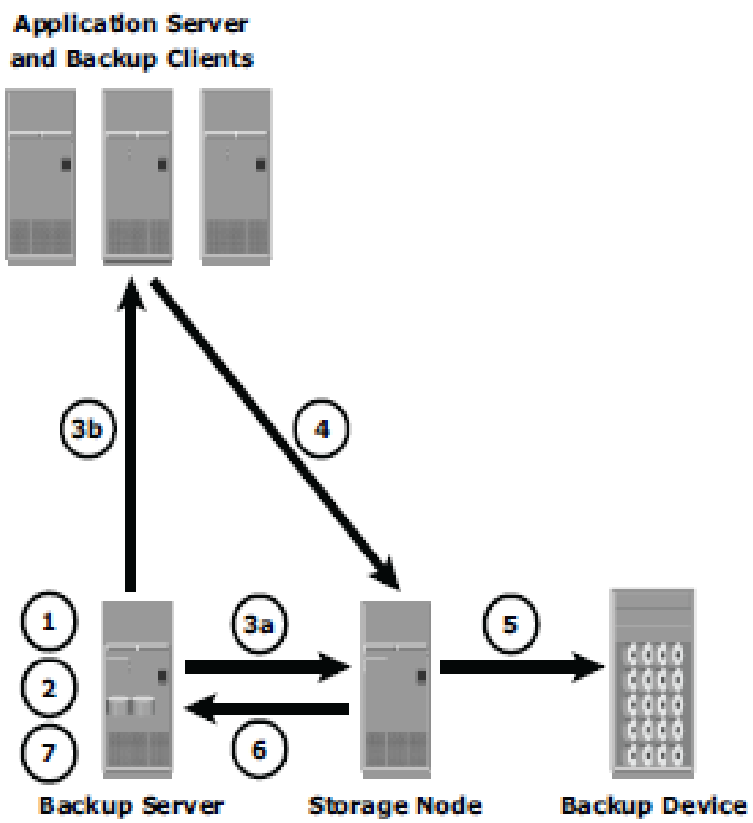
Backup architecture and process



Backup and Restore Operations

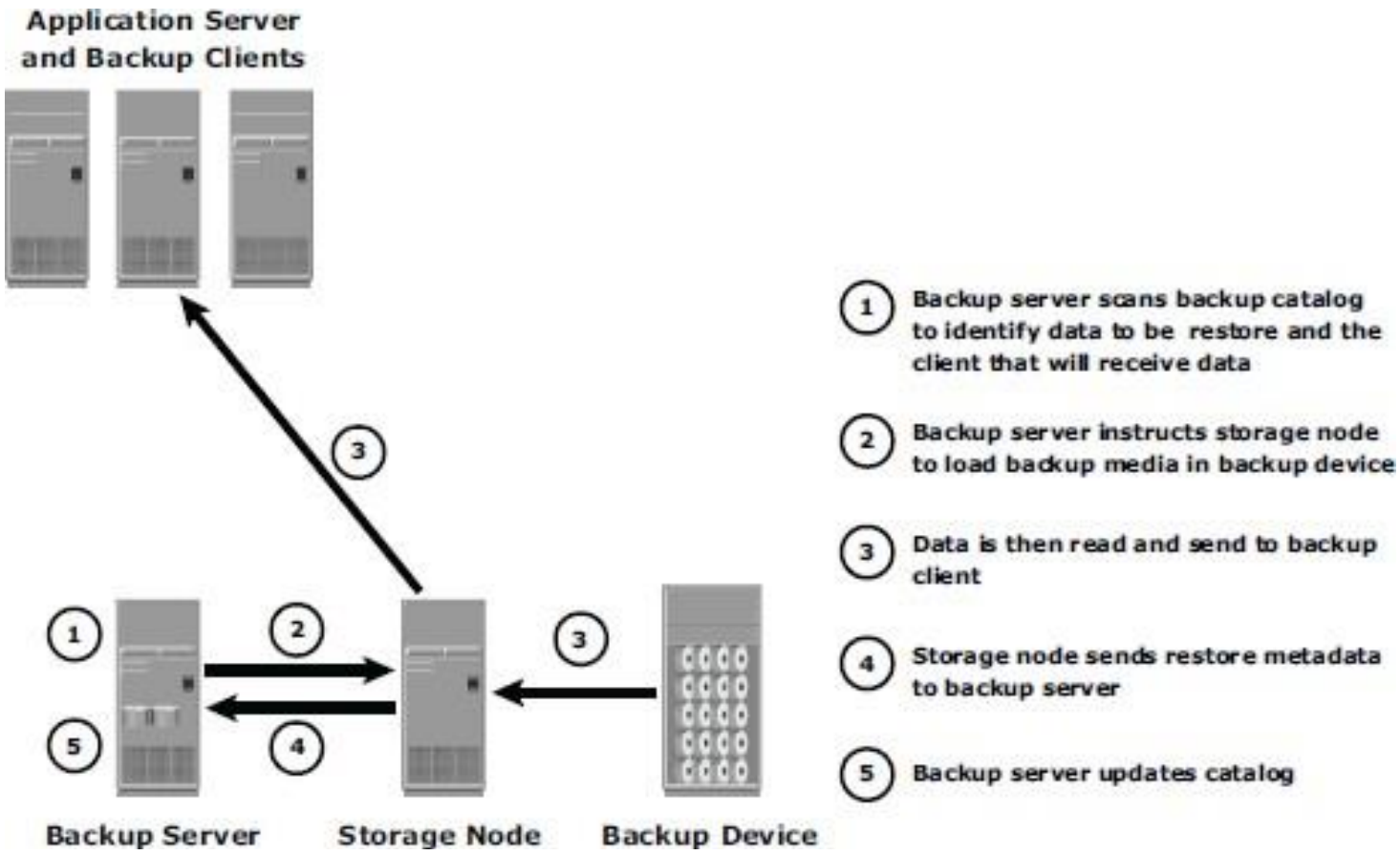
- When a backup process is initiated, significant network communication takes place between the different components of a backup infrastructure.
- The backup server initiates the backup process for different clients based on the backup schedule configured for them.

Backup operation



1. Start of scheduled backup process
2. Backup server retrieves backup related information from backup catalog
3a. Backup server instructs storage node to load backup media in backup device
3b. Backup server instructs backup clients to sends it's metadata to backup server and data to be backed up to storage node
4. Backup clients send data to storage node
5. Storage node sends data to backup device
6. Storage node sends metadata and media information to Backup server
7. Backup server update catalog and records the status

Restore operation

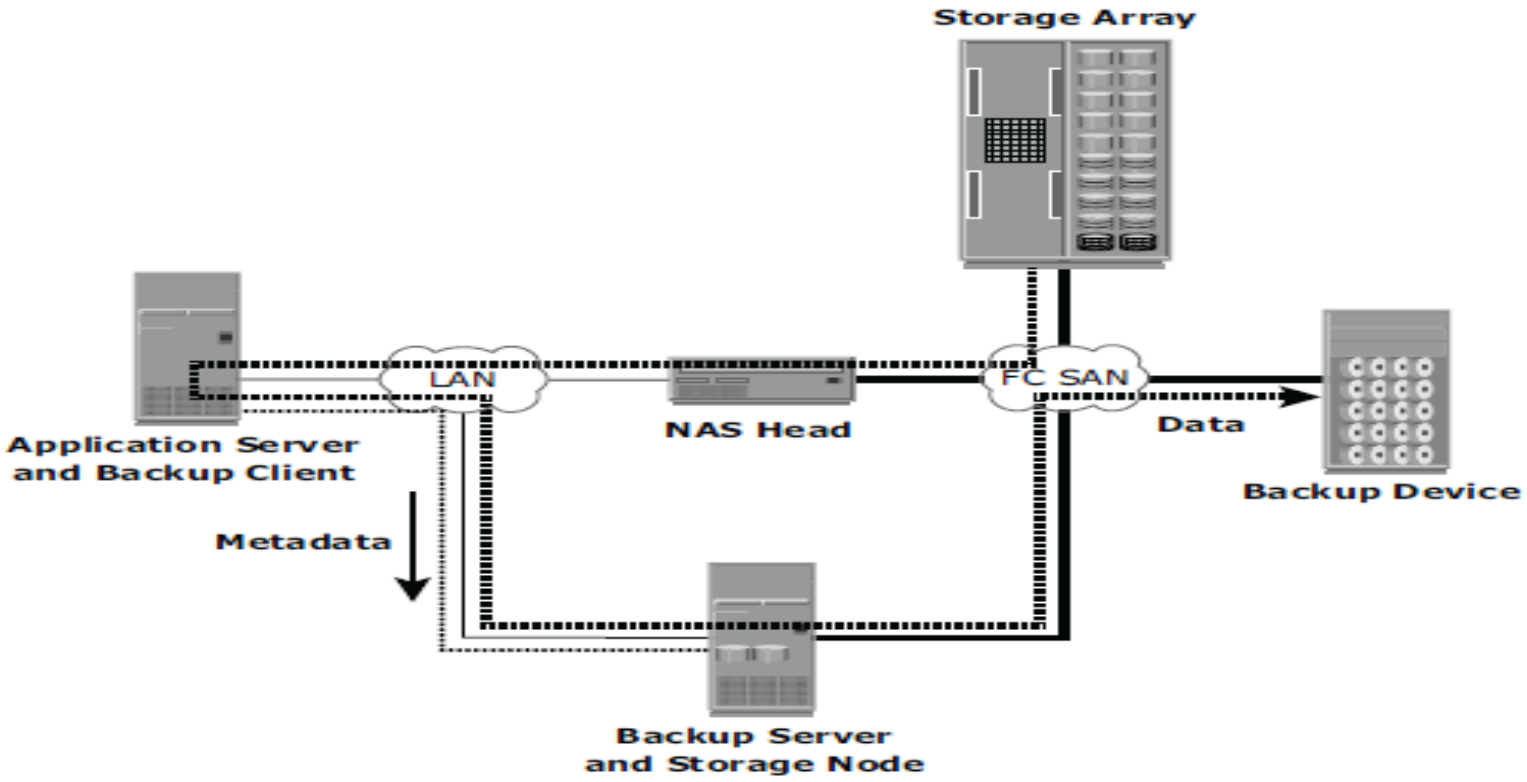


Backup in NAS Environments

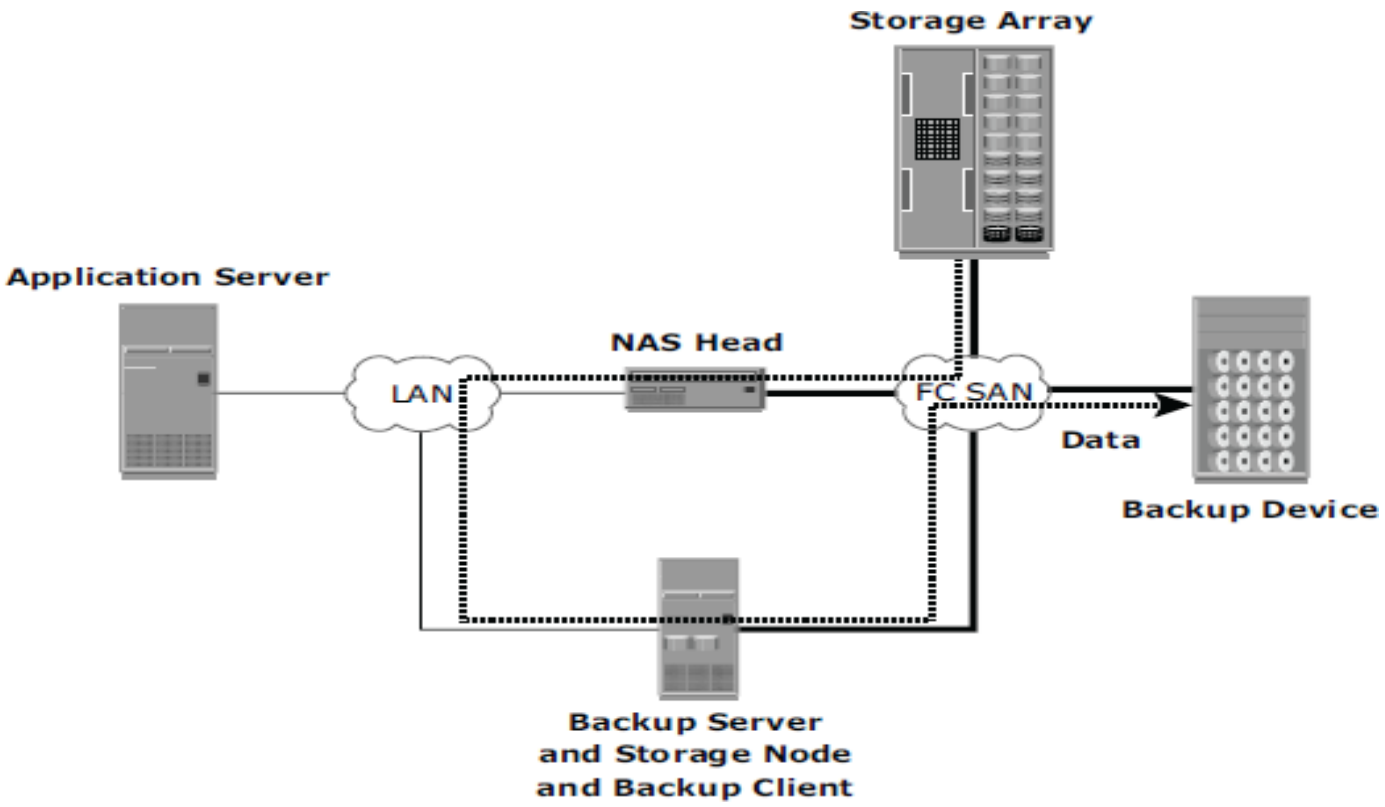
- In the NAS environment, backups can be implemented in four different ways:

1. Server based
2. Server less
3. Network Data Management Protocol (NDMP) in either NDMP 2-way
4. NDMP 3-way

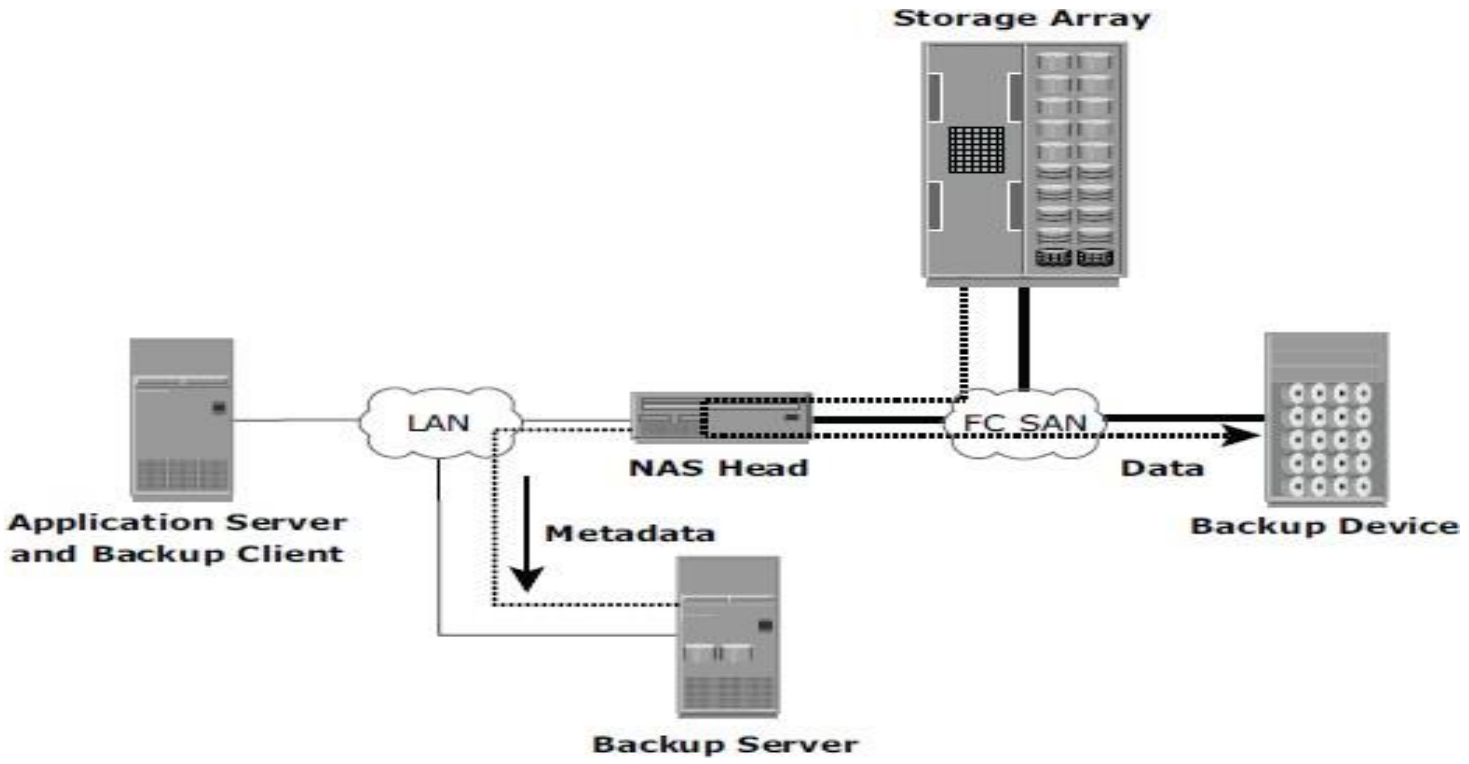
Server-based backup in NAS environment



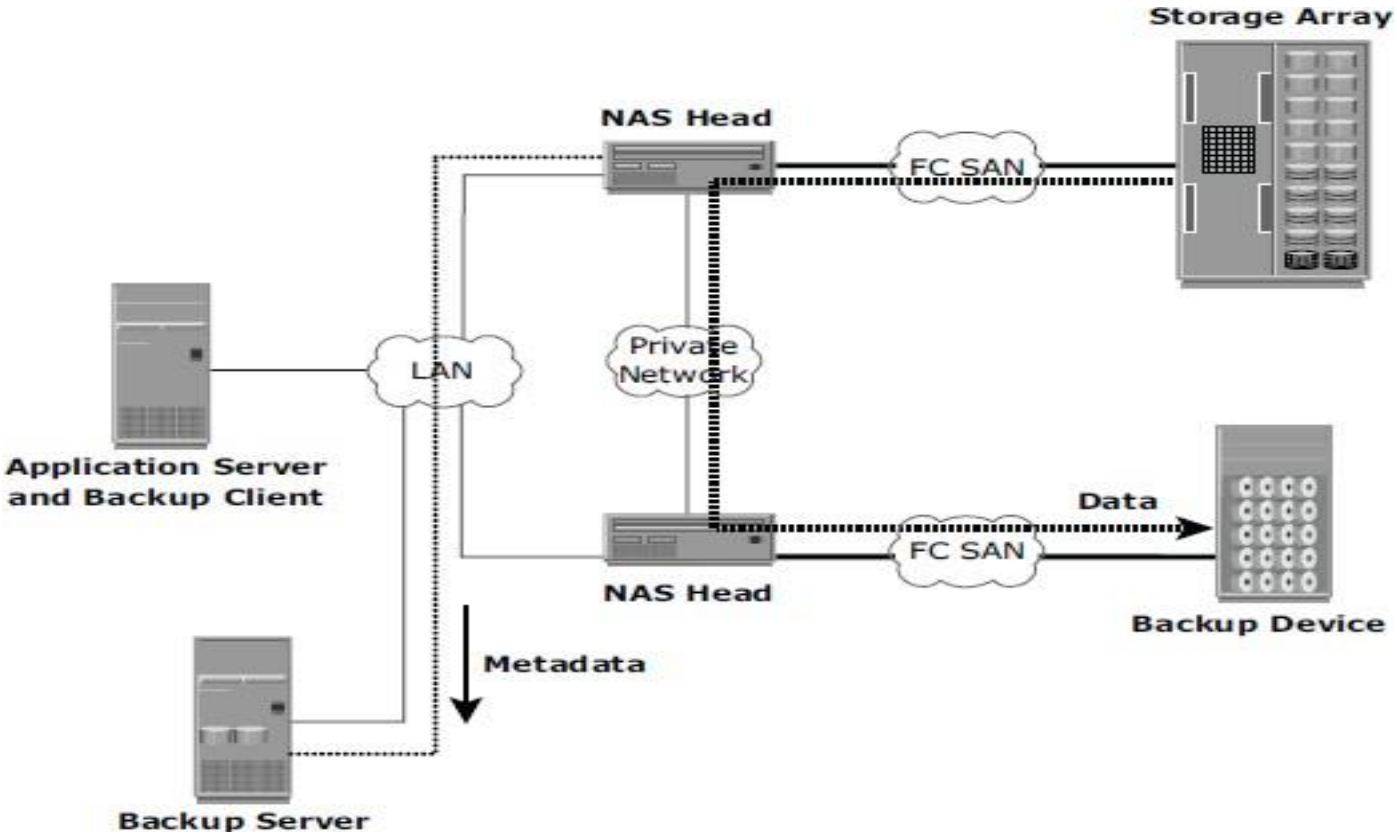
Server less backup in NAS environment



NDMP 2-way in NAS environment



NDMP 3-way in NAS environment

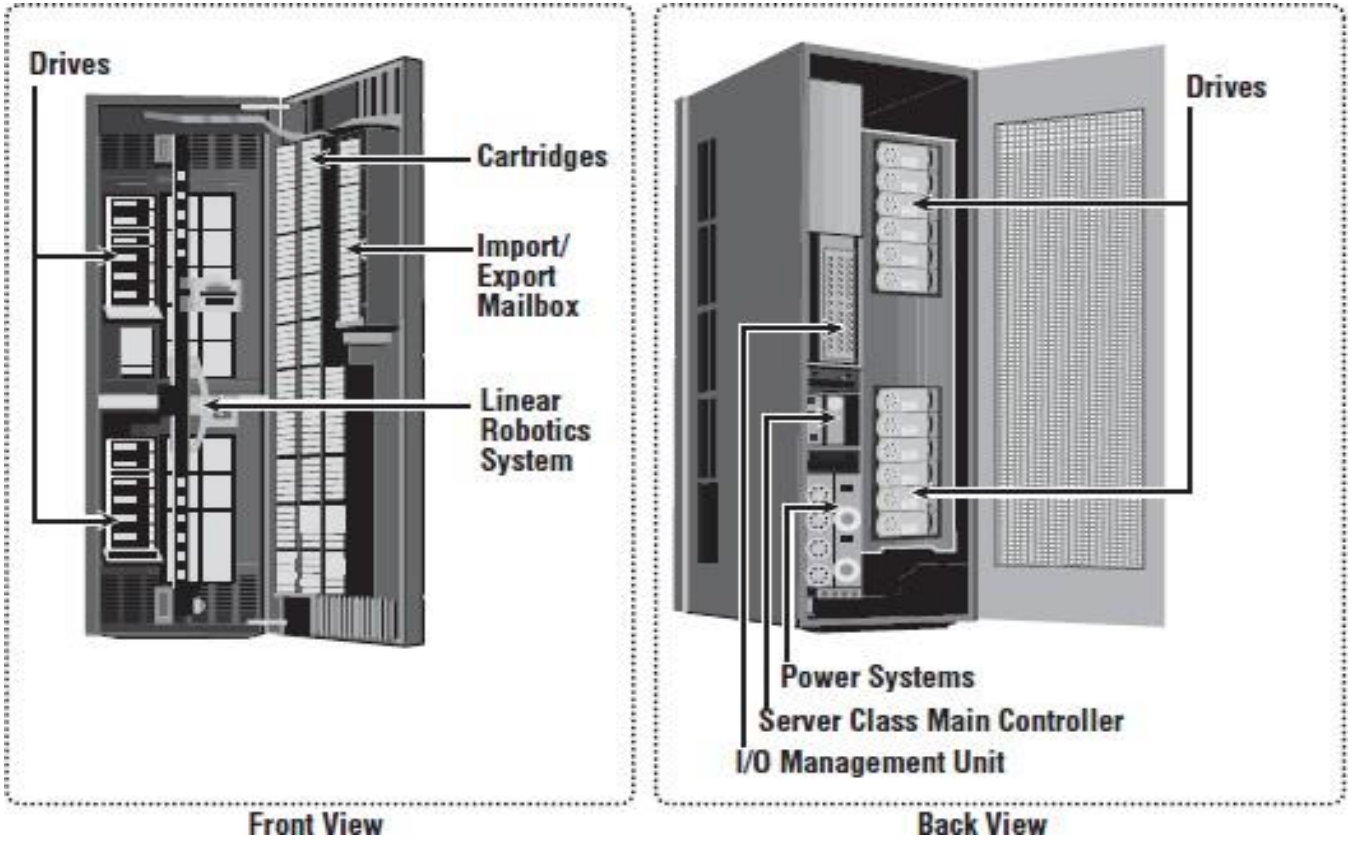


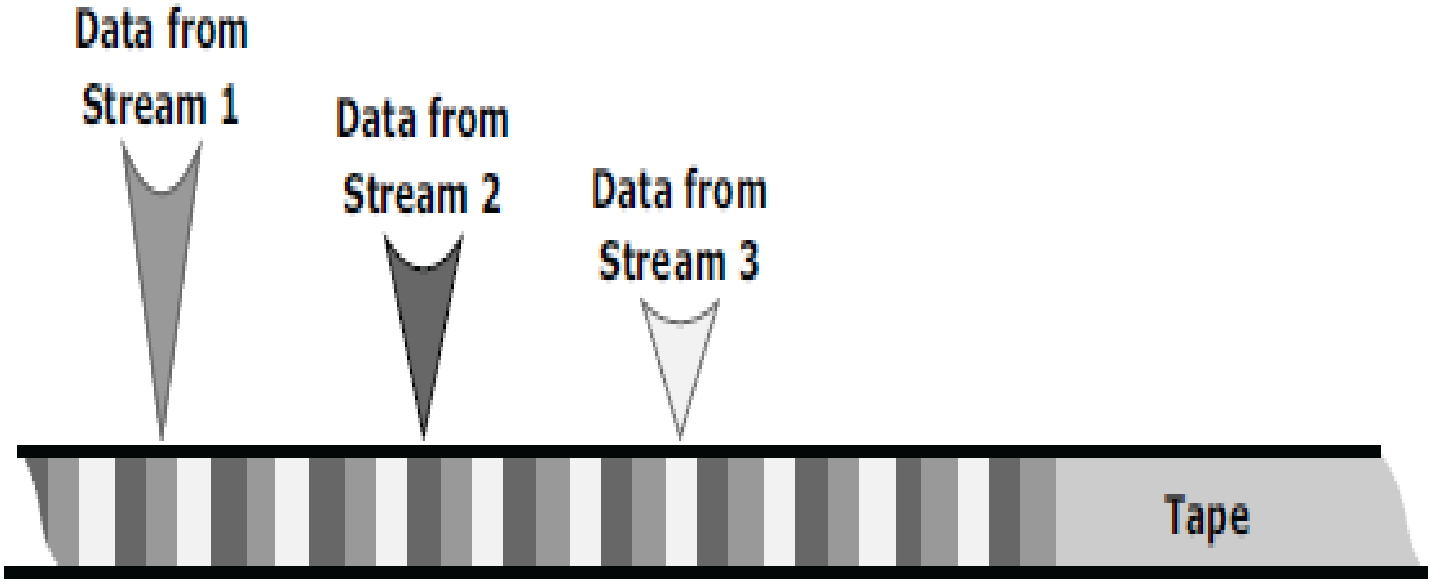
Backup Targets

- Tapes and disks are the two most commonly used backup media

1. Backup to Tape
   - Tapes, a low-cost technology, are used extensively for backup.
   - Tape drives are used to read/write data from/to a tape cartridge.
2. Physical Tape Library
   - The physical tape library provides housing and power for a number of tape drives and tape cartridges, along with a robotic arm or picker mechanism.

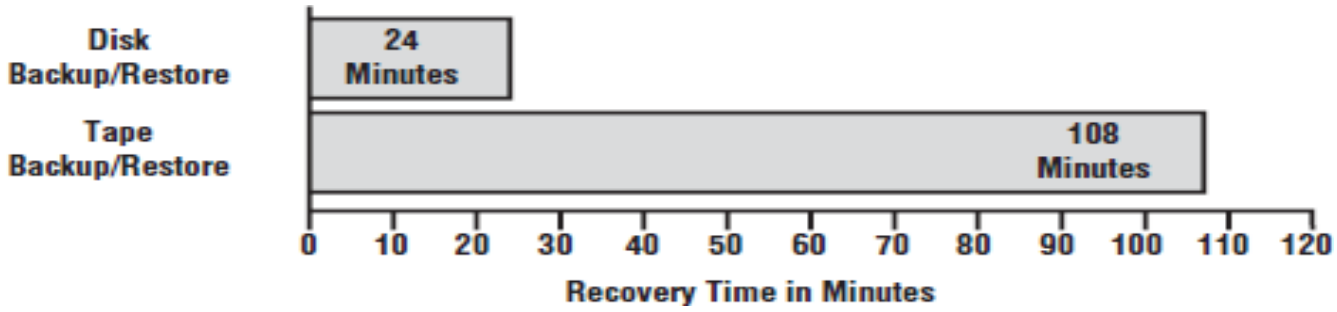
Physical tape library




Data from
Stream 1
Data from
Stream 2
Data from
Stream 3
Tape

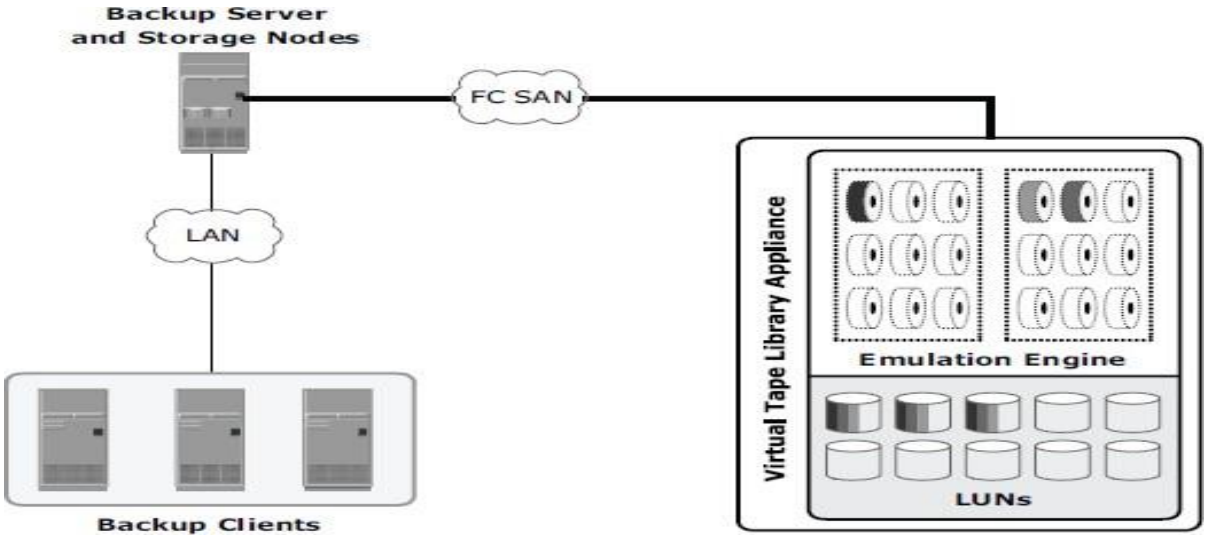
3.Backup to Disk

- Disks have now replaced tapes as the primary device for storing backup data because of their performance advantages.
- Backup-to-disk systems offer ease of implementation, reduced cost, and improved quality of service.



4.Virtual Tape Library

– A *virtual tape library (VTL)* has the same components as that of a physical tape library except that the majority of the components are presented as virtual resources.



Data Deduplication for Backup

- Data deduplication is the process of identifying and eliminating redundant data

1.Data Deduplication Methods

There are two methods of deduplication:

1.File level

2.Subfile level

2.Data Deduplication Implementation

->Source-Based Data Deduplication

->Target-Based Data Deduplication