SUBJECT CODE / NAME : **CCS367 / STORAGE TECHNOLOGIES**

YEAR / SEM: **III / V**

UNIT I
STORAGE SYSTEMS

Introduction to Information Storage: Digital data and its types, Information storage, Key characteristics of data center and Evolution of computing platforms. Information Lifecycle Management.Third Platform Technologies: Cloud computing and its essential characteristics, Cloud services and cloud deployment models, Big data analytics, Social networking and mobile computing, Characteristics of third platform infrastructure and Imperatives for third platform transformation. Data Center Environment: Building blocks of a data center, Compute systems and compute virtualization and Software-defined data center.

➔ INFORMATION STORAGE

Businesses use data to derive information that is critical to their day-to-day operations. Storage is a repository that enables users to store and retrieve this digital data.

➔ DIGITAL DATA AND ITS TYPES

DATA:

- Data is a collection of raw facts from which conclusions may be drawn.
- Handwritten letters, a printed book, a family photograph, a movie on video tape, printed and duly signed copies of mortgage papers, a bank's ledgers, and an account holder's passbooks are all examples of data.

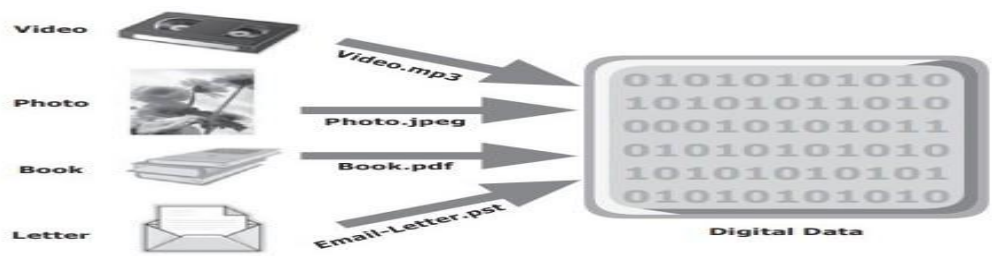


Figure 1-2: Digital data

- Before the advent of computers, the procedures and methods adopted for data creation and sharing were limited to fewer forms, such as paper and film.
- Today, the same data can be converted into more convenient forms such as an e-mail message, an e-book, a bitmapped image, or a digital movie.
- This data can be generated using a computer and stored in strings of 0s and 1s, as shown in Figure 1-2. *Data in this form is called digital data and is accessible by the user only after it is processed by a computer*

➢ With the advancement of computer and communication technologies, the rate of data generation and sharing has increased exponentially.

The following is a list of some of the factors that have contributed to the growth of digital data:

■ ***Increase in data processing capabilities***: Modern-day computers provide a significant increase in processing and storage capabilities. This enables the conversion of various types of content and media from conventional forms to digital formats.

■ ***Lower cost of digital storage***: Technological advances and decrease in the cost of storage devices have provided low-cost solutions and encouraged the development of less expensive data storage devices. This cost benefit has increased the rate at which data is being generated and stored.

■ ***Affordable and faster communication technology***: The rate of sharing digital data is now much faster than traditional approaches. A handwritten letter may take a week to reach its destination, whereas it only takes a few seconds for an e-mail message to reach its recipient.

➢ Inexpensive and easier ways to create, collect, and store all types of data, coupled with increasing individual and business needs, have led to accelerated data growth, popularly termed the data explosion.

Data has different purposes and criticality, so both individuals and businesses have contributed in varied proportions to this data explosion.

The importance and the criticality of data vary with time. Most of the data Created holds significance in the short-term but becomes less valuable over time.

This governs the type of data storage solutions used. Individuals store data on a variety of storage devices, such as hard disks, CDs, DVDs, or Universal Serial Bus (USB) flash drives.

Example of Research and Business data :

■ *Seismology*: Involves collecting data related to various sources and parameters of earthquakes, and other relevant data that needs to be processed to derive meaningful information.

■ *Product data*: Includes data related to various aspects of a product, such as inventory, description, pricing, availability, and sales.

■ *Customer data*: A combination of data related to a company's customers, such as order details, shipping addresses, and purchase history.

■ *Medical data*: Data related to the health care industry, such as patient history, radiological images, details of medication and other treatment, and insurance information

- Businesses generate vast amounts of data and then extract meaningful information from this data to derive economic benefits. Therefore, businesses need to maintain data and ensure its availability over a longer period.

Furthermore, the data can vary in criticality and may require special handling.

For example, legal and regulatory requirements mandate that banks maintain account information for their customers accurately and securely. Some businesses handle data for millions of customers, and ensures the security and integrity of data over a long period of time. This requires highcapacity storage devices with enhanced security features that can retain data for a long period.

TYPES OF DATA :

Data can be classified as *structured or unstructured* (see Figure 1-3) based on how it is stored and managed.

- Structured data is organized in rows and columns in a rigidly defined format so that applications can retrieve and process it efficiently. Structured data is typically stored using a database management system (DBMS).
- Data is unstructured if its elements cannot be stored in rows and columns, and is therefore difficult to query and retrieve by business applications.

For example, customer contacts may be stored in various forms such as sticky notes, e-mail messages, business cards, or even digital format files such as .doc, .txt, and .pdf. Due its unstructured nature, it is difficult to retrieve using a customer relationship management application.

Unstructured data may not have the required components to identify itself uniquely for any type of processing or interpretation. Businesses are primarily concerned with managing unstructured data because over 80 percent of enterprise data is unstructured and requires significant storage space and effort to manage

➔ INFORMATION STORAGE :

INFORMATION:

- Data, whether structured or unstructured, does not fulfill any purpose for individuals or businesses unless it is presented in a meaningful form. Businesses need to analyze data for it to be of value.
- *Information is the intelligence and knowledge derived from data.*
- Businesses analyze raw data in order to identify meaningful trends. On the basis of these trends, a company can plan or modify its strategy. For example, a retailer identifies customers' preferred products and brand names by analyzing their purchase patterns and maintaining an inventory of those products.
- Effective data analysis not only extends its benefits to existing businesses, but also creates the potential for new business opportunities by using the information in creative ways. *Job portal is an example.*
- In order to reach a wider set of prospective employers, job seekers post their résumés on various websites offering job search facilities.

- These websites collect the résumés and post them on centrally accessible locations for prospective employers.
- In addition, companies post available positions on job search sites. Job-matching software matches keywords from résumés to keywords in job postings. In this manner, the job search engine uses data and turns it into information for employers and job seekers.

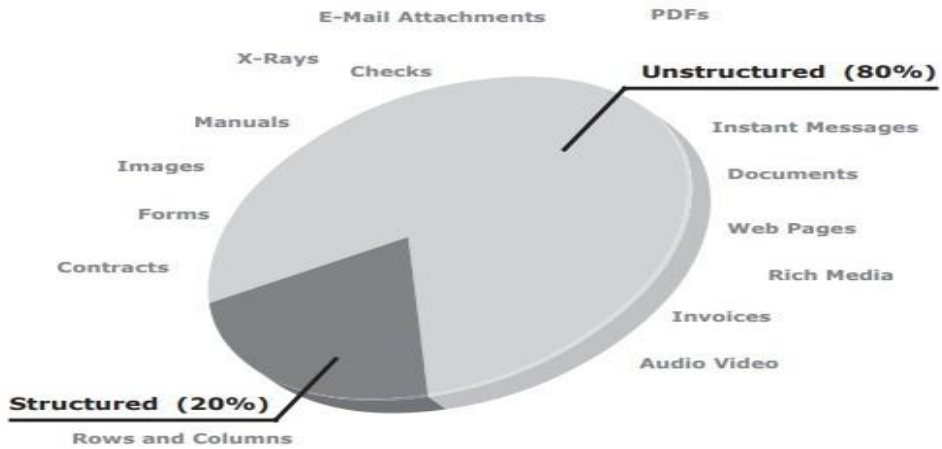


Figure 1-3: Types of data

STORAGE:

- Data created by individuals or businesses must be stored so that it is easily accessible for further processing.
- In a computing environment, devices designed for storing data are termed storage devices or simply storage.
- The type of storage used varies based on the type of data and the rate at which it is created and used.
- Devices such as memory in a cell phone or digital camera, DVDs, CD-ROMs, and hard disks in personal computers are examples of storage devices.
- Businesses have several options available for storing data including internal hard disks, external disk arrays and tape

➔ DATA CENTER INFRASTRUCTURE:

- Organizations maintain data centers to provide centralized data processing capabilities across the enterprise. Data centers store and manage large amounts of mission-critical data.
- The data center infrastructure includes computers, storage systems, network devices, dedicated power backups, and environmental controls (such as air conditioning and fire suppression).
- Large organizations often maintain more than one data center to distribute data processing workloads and provide backups in the event of a disaster. The storage requirements of a data center are met by a combination of various stor- age architectures.

CORE ELEMENTS:

- *Five core elements are essential for the basic functionality of a data center:*

Application: An application is a computer program that provides the logic for computing operations. Applications, such as an order processing system, can be layered on a database, which in turn uses operating system services to perform read/write operations to storage devices.

Database: More commonly, a database management system (DBMS) provides a structured way to store data in logically organized tables that are interrelated. A DBMS optimizes the storage and retrieval of data.

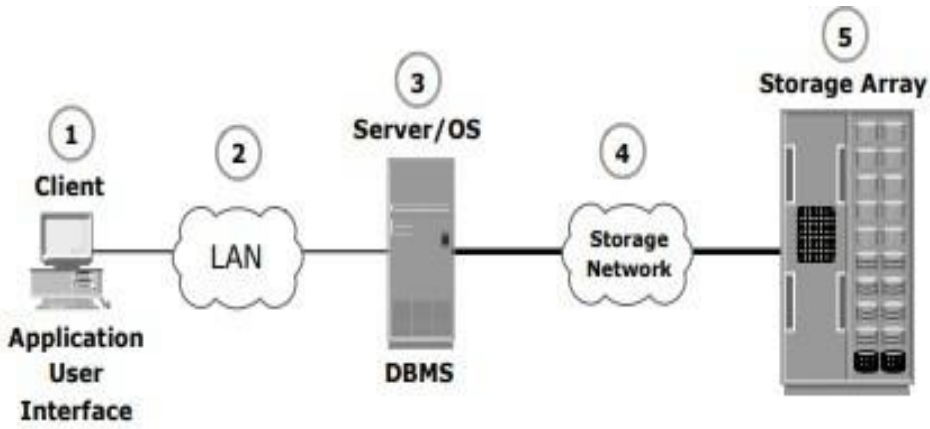
Server and operating system: A computing platform that runs applica tions and databases.

Network: A data path that facilitates communication between clients and servers or between servers and storage.

Storage array: A device that stores data persistently for subsequent use.

These core elements are typically viewed and managed as separate entities, but all the elements must work together to address data processing requirements.

Figure 1-5 shows an example of an order processing system that involves the five core elements of a data center and illustrates their functionality in a business process.

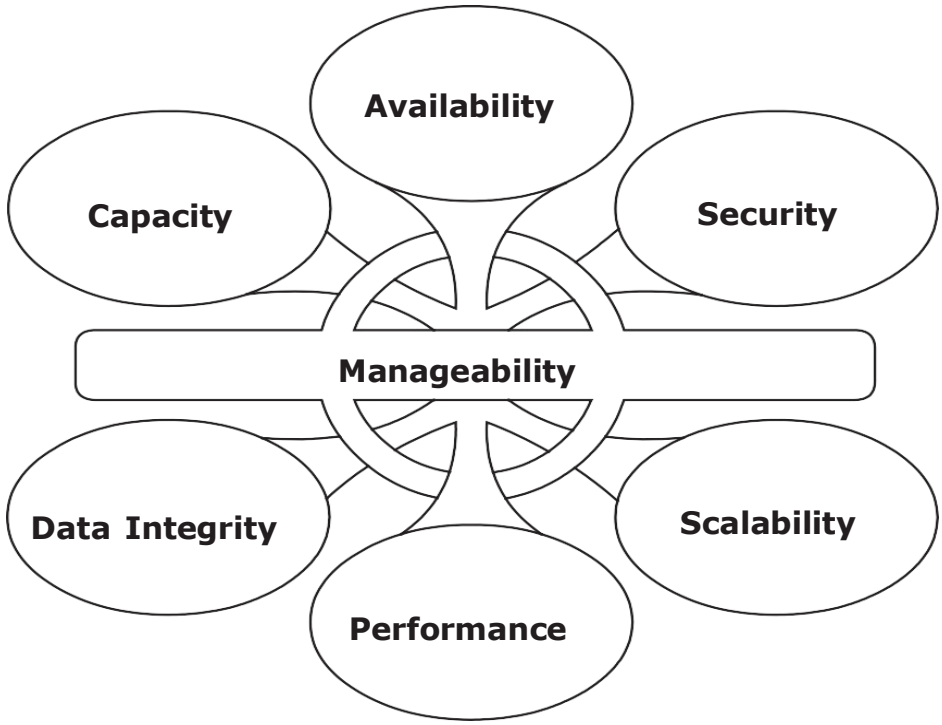


1. A customer places an order through the AUI of the order processing application software located on the client computer.
2. The client connects to the server over the LAN and accesses the DBMS located on the server to update the relevant information such as the customer name, address, payment method, products ordered, and quantity ordered.
3. The DBMS uses the server operating system to read and write this data to the database located on physical disks in the storage array.
4. The Storage Network provides the communication link between the server and the storage array and transports the read or write commands between them.
5. The storage array, after receiving the read or write commands from the server, performs the necessary operations to store the data on physical disks.

Figure 1-5: Example of an order processing system

KEY REQUIREMENTS FOR DATA CENTER ELEMENTS (OR) KEY CHARACTERISTICS OF DATA CENTER ELEMENTS :

- Uninterrupted operation of data centers is critical to the survival and success of a business. It is necessary to have a reliable infrastructure that ensures data is accessible at all times. While the requirements, shown in Figure 1-6, are appli cable to all elements of the data center infrastructure, our focus here is on storage systems.



Key Characteristics of Data Center Elements

Availability:

All data center elements should be designed to ensure acces- sibility. The inability of users to access data can have a significant negative impact on a business.

Security:

Polices, procedures, and proper integration of the data cen- ter core elements that will prevent unauthorized access to information must be established.

In addition to the security measures for client access, specific mechanisms must enable servers to access only their allocated resources on storage arrays.

Scalability:

Data center operations should be able to allocate additional processing capabilities or storage on demand, without interrupting busi- ness operations.

Business growth often requires deploying more servers, new applications, and additional databases. The storage solution should be able to grow with the business.

Performance:

All the core elements of the data center should be able to provide optimal performance and service all processing requests at high speed.

The infrastructure should be able to support performance requirements.

Data integrity:

Data integrity refers to mechanisms such as error correc- tion codes or parity bits which ensure that data is written to disk exactly as it was received.

Any variation in data during its retrieval implies cor- ruption, which may affect the operations of the organization.

Capacity:

Data center operations require adequate resources to store and process large amounts of data efficiently.

When capacity requirements increase, the data center must be able to provide additional capacity with- out interrupting availability, or, at the very least, with minimal disruption. Capacity may be managed by reallocation of existing resources, rather than by adding new resources.

Manageability:

A data center should perform all operations and activi- ties in the most efficient manner.

Manageability can be achieved through automation and the reduction of human (manual) intervention in com- mon tasks.

MANAGING STORAGE INFRASTRUCTURE:

- Managing a modern, complex data center involves many tasks. Key manage- ment activities include:

✓ ***Monitoring*** is the continuous collection of information and the review of the entire data center infrastructure. The aspects of a data center that are monitored include security, performance, accessibility, and capacity.

✓ ***Reporting*** is done periodically on resource performance, capacity, and utilization.

Reporting tasks help to establish business justifications and chargeback of costs associated with data center operations.

- ✓ ***Provisioning*** is the process of providing the hardware, software, and other resources needed to run a data center. Provisioning activities include capacity and resource planning.

  Capacity planning ensures that the user's and the application's future needs will be addressed in the most cost-effective and controlled manner.

  Resource planning is the process of evaluating and identifying required resources, such as personnel, the facility (site), and the technology. Resource planning ensures that adequate resources are available to meet user and application requirements.

For example, the utilization of an application's allocated storage capacity may be monitored. As soon as utilization of the storage capacity reaches a critical value, additional storage capacity may be provisioned to the application. If uti- lization of the storage capacity is properly monitored and reported, business growth can be understood and future capacity requirements can be anticipated. This helps to frame a proactive data management policy.

KEY CHALLENGES IN MANAGING INFORMATION:

In order to frame an effective information management policy, businesses need to consider the following key challenges of information management:

- **Exploding digital universe:**

  The rate of information growth is increasing exponentially. Duplication of data to ensure high availability and repurpos- ing has also 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 market place.

- **Changing value of information:**

  Information that is valuable today may become less important tomorrow.

The value of information often changes over time.Framing a policy to meet these

challenges involves understanding the value of information over its lifecycle.

➔ EVOLUTION OF STORAGE TECHNOLOGY AND ARCHITECTURE:

- Historically, organizations had centralized computers (mainframe) and information storage devices (tape reels and disk packs) in their data center.
- The evolution of open systems and the affordability and ease of deployment that they offer made it possible for business units/departments to have their own servers and storage.
- In earlier implementations of open systems, the storage was typically internal to the server.
- The proliferation of departmental servers in an enterprise resulted in unpro- tected, unmanaged, fragmented islands of information and increased operating cost.
- Originally, there were very limited policies and processes for managing these servers and the data created.

To overcome these challenges, storage tech- nology evolved from non-intelligent internal storage to intelligent networked storage (see Figure 1-4). Highlights of this technology evolution include:

- **Redundant Array of Independent Disks (RAID):** This technology was developed to address the cost, performance, and availability requirements of data. It continues to evolve today and is used in all storage architectures such as DAS, SAN, and so on.

- **Direct-attached storage (DAS):** This type of storage connects directly to a server (host) or a group of servers in a cluster. Storage can be either internal or external to the server. External DAS alleviated the challenges of limited internal storage capacity.

- **Storage area network (SAN):** This is a dedicated, high-performance *Fibre Channel (FC)* network to facilitate *block-level* communication between servers and storage. Storage is partitioned and assigned to a server for accessing its data. SAN offers scalability, availability, performance, and cost benefits compared to DAS.

- **Network-attached storage (NAS):** This is dedicated storage for *file serving* applications. Unlike a SAN, it connects to an existing communication network (LAN) and provides file access to heterogeneous clients. Because it is purposely built for providing storage to file server applications, it offers higher scalability, availability, performance, and cost benefits compared to general purpose file servers.

- **Internet Protocol SAN (IP-SAN):** One of the latest evolutions in stor- age architecture, IP-SAN is a convergence of technologies used in SAN and NAS. IP-SAN provides block-level communication across a local or wide area network (LAN or WAN), resulting in greater consolidation and availability of data.

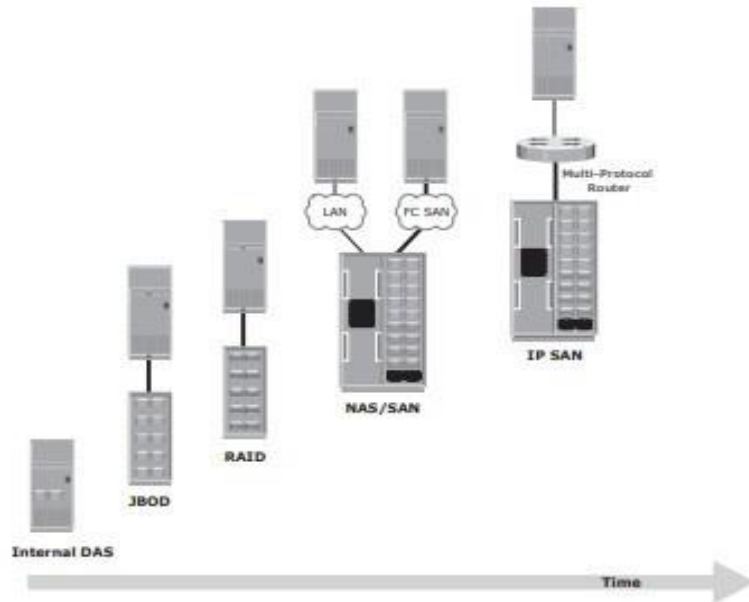


Figure 1-4: Evolution of storage architectures

➔ INFORMATION LIFECYCLE MANAGEMENT:

INFORMATION LIFECYCLE

- *The information lifecycle is the "change in the value of information" over time.*
- When data is first created, it often has the highest value and is used frequently. As data ages, it is accessed less frequently and is of less value to the organization

- Understanding the information lifecycle helps to deploy appropriate storage infrastructure, according to the changing value of information.

  For example, in a sales order application, the value of the information changes from the time the order is placed until the time that the warranty becomes void (see Figure 1-7).

  - The value of the information is highest when a company receives a new sales order and processes it to deliver the product.After order fulfillment, the customer or order data need not be available for real-time access.
    The company can transfer this data to less expensive secondary storage with lower accessibility and availability requirements unless or until a warranty claim or another event triggers its need.
    After the warranty becomes void, the company can archive or dispose of data to create space for other high-value information

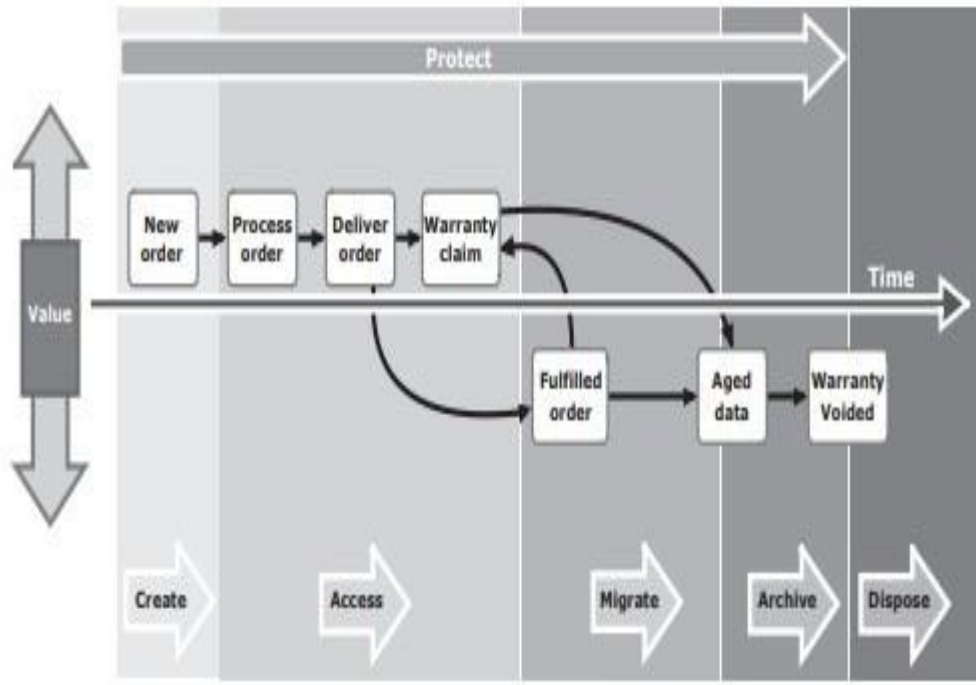


Figure 1-7: Changing value of sales order information

INFORMATION LIFECYCLE MANAGEMENT:

- Today's business requires data to be protected and available 24 × 7.
  Data centers can accomplish this with the optimal and appropriate use of storage infrastruc- ture.
- An effective information management policy is required to support this infrastructure and leverage its benefits.

Information lifecycle management (ILM) is a proactive strategy that enables an IT organization to effectively manage the data throughout its lifecycle, based on predefined business policies.

This allows an IT organization to optimize the storage infrastructure for maximum return on investment.

An ILM strategy should include the following characteristics:

- **Business-centric:** It should be integrated with key processes, applications, and initiatives of the business to meet both current and future growth in information.
- **Centrally managed:** All the information assets of a business should be under the purview of the ILM strategy.
- **Policy-based:** The implementation of ILM should not be restricted to a few departments. ILM should be implemented as a policy and encompass all business applications, processes, and resources.
- **Heterogeneous:** An ILM strategy should take into account all types of storage platforms and operating systems.
- **Optimized:** Because the value of information varies, an ILM strategy should consider the different storage requirements and allocate storage resources based on the information's value to the business.

ILM IMPLEMENTATION:

*The process of developing an ILM strategy includes **four** activities—classifying, implementing, managing, and organizing:*

- ***Classifying*** data and applications on the basis of business rules and poli- cies to

enable differentiated treatment of information

- ***Implementing*** policies by using information management tools, starting from the creation of data and ending with its disposal
- ***Managing*** the environment by using integrated tools to reduce operational complexity
- ***Organizing*** storage resources in tiers to align the resources with data classes, and storing information in the right type of infrastructure based on the information's current value.

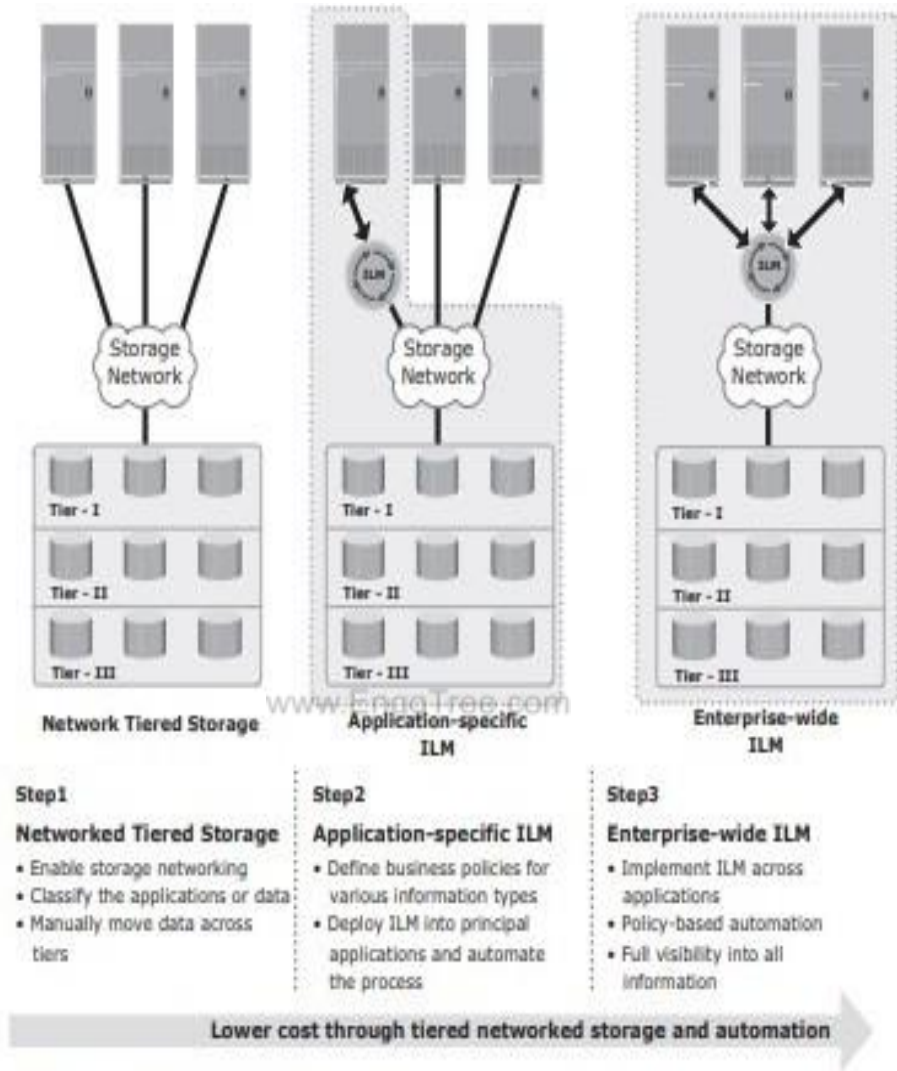


Figure 1-8: Implementation of ILM

Implementing ILM across an enterprise is an ongoing process.

Steps 1 and 2 are aimed at implementing ILM in a limited way across a few enterprise-critical applications.

- Step 1 : the goal is to implement a storage net- working environment. Storage architectures offer varying levels of protection and performance and this acts as a foundation for future policy-based informa- tion management in Steps 2 and 3.

  The value of tiered storage platforms can be exploited by allocating appropriate storage resources to the applications based on the value of the information processed.
- Step 2 : takes ILM to the next level, with detailed application or data classification and linkage of the storage infrastructure to business policies.

  These classification and the resultant policies can be automatically executed using tools for one or more applications, resulting in better management and optimal allocation of storage resources.
- Step 3 : of the implementation is to automate more of the applications or data classification and policy management activities in order to scale to a wider set of enterprise applications.

ILM BENEFITS:

Implementing an ILM strategy has the following key benefits that directly address the challenges of information management:

- ***Improved utilization*** by using tiered storage platforms and increased vis ibility of all enterprise information.
- ***Simplified management*** by integrating process steps and interfaces with individual tools and by increasing automation.
- ***A wider range of options*** for backup, and recovery to balance the need for business continuity.
- ***Maintaining compliance*** by knowing what data needs to be protected for what length of time.
- ***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.

➔ CLOUD COMPUTING AND CHARACTERISTICS:

- *Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Cloud computing allows you to set up a virtual office to give you the flexibility of connecting to your business anywhere, any time.*
- Moving to cloud computing may reduce the cost of managing and maintaining your IT systems. Rather than purchasing expensive systems and equipment for your business.
- Cloud computing refers to both the applications delivered as services over the Internet and the hardware and system software in the datacenters that provide those services.
- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- A cloud is a type of parallel and distributed system consisting of a collection of interconnected. virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.

There are many characteristics of Cloud Computing here are few of them:

1. **On-demand self-services:**

The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.

2. **Broad network access:**

The Computing services are generally provided over standard networks and heterogeneous devices.

3. **Rapid elasticity:**

The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user requires services it is provided to him and it is scale out as soon as its requirement gets over.

4. **Resource pooling:**

The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.

5. **Measured service:**

The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.

6. **Multi-tenancy:**

Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources

.

7. **Virtualization:**

Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.

8. **Resilient computing:**

Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.

9. **Flexible pricing models:**

Cloud providers offer a variety of pricing models, including pay-per-use, subscription-based, and spot pricing, allowing users to choose the option that best suits their needs.

10. Security:

Cloud providers invest heavily in security measures to protect their users' data and ensure the privacy of sensitive information.

11. Automation:

Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.

12. Sustainability:

Cloud providers are increasingly focused on sustainable practices, such as energy-efficient data centers and the use of renewable energy sources, to reduce their environmental impact.

Advantages:

1. Easy implementation
2. Accessibility
3. No hardware required
4. Cost per head
5. Flexibility for growth
6. Efficient recovery

Disadvantages:

1. No longer in control
2. May not get all the features
3. Doesn't mean you should do away with servers
4. No Redundancy
5. Bandwidth issues

➔ CLOUD MODELS :

The Cloud Models are as follows :

- ❖ Cloud Service models
- ❖ Cloud Deployment models.

CLOUD SERVICES :

- ➢ The term "cloud services" refers to a wide range of services delivered on demand to companies and customers over the internet.
- ➢ These services are designed to provide easy, affordable access to applications and resources, without the need for internal infrastructure or hardware.

- From checking email to collaborating on documents, most employees use cloud services throughout the workday, whether they're aware of it or not.
- Cloud services are fully managed by cloud computing vendors and service providers.
- They're made available to customers from the providers' servers, so there's no need for a company to host applications on its own on-premises servers.

There are the following three types of cloud service models -

1. *Infrastructure as a Service (IaaS)*
2. *Platform as a Service (PaaS)*
3. *Software as a Service (SaaS)*

Basis Of	IAAS	PAAS	SAAS
Stands for	Infrastructure as a service.	Platform as a service.	Software as a service.
Uses	IAAS is used by network architects.	PAAS is used by developers.	SAAS is used by the end user.
Access	IAAS gives access to the resources like virtual machines and virtual storage.	PAAS gives access to run time environment to deployment and development tools for application.	SAAS gives access to the end user.
Model	It is a service model that provides virtualized computing resources over the internet.	It is a cloud computing model that delivers tools that are used for the development of applications.	It is a service model in cloud computing that hosts software to make it available to clients.
Technical understanding.	It requires technical knowledge.	Some knowledge is required for the basic setup.	There is no requirement about technicalities company handles everything.
Popularity	It is popular among developers and researchers.	It is popular among developers who focus on the development of	It is popular among consumers and companies, such as file sharing, email,

Basis Of	IAAS	PAAS	SAAS
		apps and scripts.	and networking.
Percentage rise	It has around a 12% increment.	It has around 32% increment.	It has about a 27 % rise in the cloud computing model.
Usage	Used by the skilled developer to develop unique applications.	Used by mid-level developers to build applications.	Used among the users of entertainment.
Cloud services.	Amazon Web Services, sun, vCloud Express.	Facebook, and Google search engine.	MS Office web, Facebook and Google Apps.
Enterprise services.	AWS virtual private cloud.	Microsoft Azure.	IBM cloud analysis.
Outsourced cloud services.	Salesforce	Force.com, Gigaspaces.	AWS, Terremark
User Controls	Operating System, Runtime, Middleware, and Application data	Data of the application	Nothing
Others	It is highly scalable and flexible.	It is highly scalable to suit the different businesses according to resources.	It is highly scalable to suit the small, mid and enterprise level business

ADVANTAGES OF IAAS:

- The resources can be deployed by the provider to a customer's environment at any given time.
- Its ability to offer the users to scale the business based on their requirements.The provider has various options when deploying resources including virtual machines, applications, storage, and networks.

- It has the potential to handle an immense number of users.
- It is easy to expand and saves a lot of money.
- Companies can afford the huge costs associated with theimplementation of advanced technologies.
- Cloud provides the architecture.
- Enhanced scalability and quite flexible.
- Dynamic workloads are supported.

DISADVANTAGES OF IAAS:

- Security issues are there.
- Service and Network delays are quite a issue in IaaS.

ADVANTAGES OF PAAS :

- Programmers need not worry about what specific database or language the application has been programmed in.
- It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.
- Provides the freedom to developers to focus on the application's design while the platform takes care of the language and the database.
- It is flexible and portable.
- It is quite affordable.
- It manages application development phases in the cloud very efficiently.

DISADVANTAGES OF PAAS

- Data is not secure and is at big risk.
- As data is stored both in local storage and cloud, there are high chances of data mismatch while integrating the data.

ADVANTAGES OF SAAS:

- It is a cloud computing service category providing a wide range of hosted capabilities and services. These can be used to build and deploy web-based software applications.
- It provides a lower cost of ownership than on-premises software. The reason is it does not require the purchase or installation of hardware or licenses.
- It can be easily accessed through a browser along a thin client.
- No cost is required for initial setup.
- Low maintenance costs.
- Installation time is less, so time is managed properly.

DISADVANTAGES OF SAAS:

- Low performance.
- It has limited customization options.
- It has security and data concerns.

CLOUD DEPLOYMENT MODEL:

A cloud deployment model defines the cloud services you are consuming and the responsibility model for who manages them. It defines your cloud architecture, scalability of your computing resources, what you can change, the services provided to you, and how much of the build you own.

Cloud Deployment Model functions as a virtual computing environment with a deployment architecture that varies depending on the amount of data you want to store and who has access to the infrastructure.

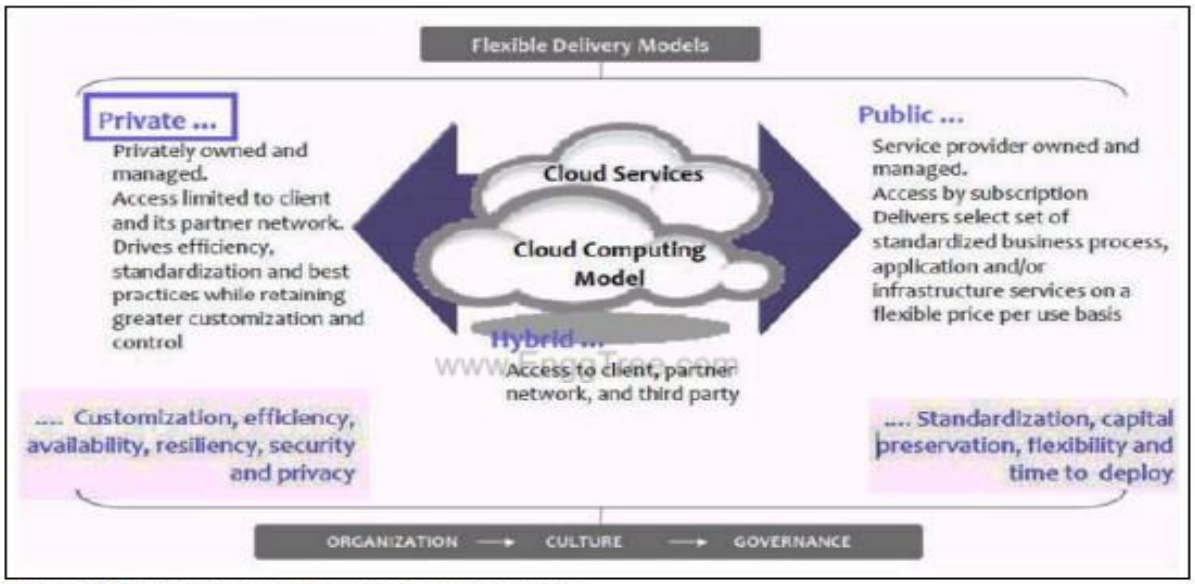


Figure 6-3 Cloud computing deployment models

PRIVATE CLOUD : The cloud infrastructure is owned or leased by a single organization and operated solely for that organization.

Advantages of the private cloud model:

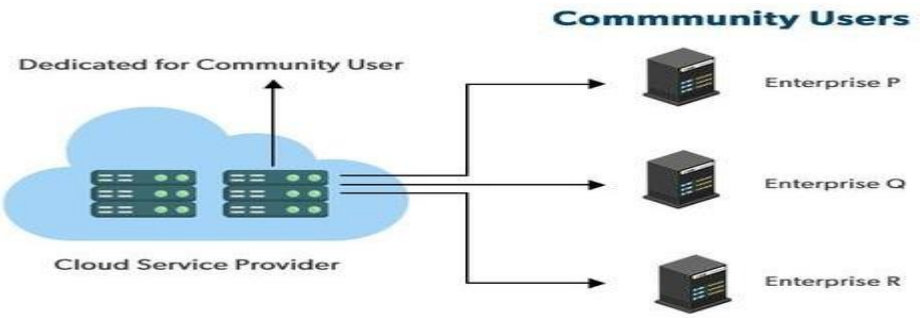
- **Better Control:** You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behavior.

- **Data Security and Privacy:** It's suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.
- **Supports Legacy Systems:** This approach is designed to work with legacy systems that are unable to access the public cloud.
- **Customization:** Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

Disadvantages of the private cloud model:

- **Less scalable:** Private clouds are scaled within a certain range as there is less number of clients.
- **Costly:** Private clouds are more costly as they provide personalized facilities.

COMMUNITY CLOUD : The cloud infrastructure is shared by several organizations and supports a specific community that shares, for example, mission, security requirements, policy, and compliance considerations.



Advantages of the community cloud model:

- **Cost Effective:** It is cost-effective because the cloud is shared by multiple organizations or communities.
- **Security:** Community cloud provides better security.
- **Shared resources:** It allows you to share resources, infrastructure, etc. with multiple organizations.
- **Collaboration and data sharing:** It is suitable for both collaboration and data sharing.

Disadvantages of the community cloud model:

- **Limited Scalability:** Community cloud is relatively less scalable as many organizations share the same resources according to their collaborative interests.
- **Rigid in customization:** As the data and resources are shared among different organizations according to their mutual interests if an organization wants some changes according to their needs they cannot do so because it will have an impact on other organizations.

PUBLIC CLOUD : The cloud infrastructure is owned by an organization that sells cloud services to the general public or to a large industry group.

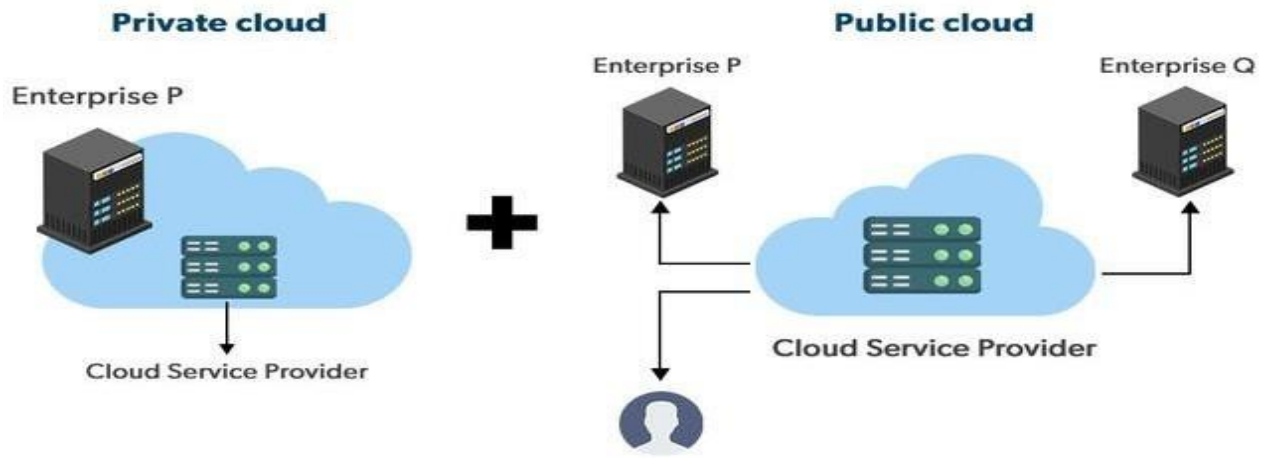
Advantages of the public cloud model:

- **Minimal Investment:** Because it is a pay-per-use service, there is no substantial upfront fee, making it excellent for enterprises that require immediate access to resources.
- **No setup cost:** The entire infrastructure is fully subsidized by the cloud service providers, thus there is no need to set up any hardware.
- **Infrastructure Management is not required:** Using the public cloud does not necessitate infrastructure management.
- **No maintenance:** The maintenance work is done by the service provider (not users).
- **Dynamic Scalability:** To fulfill your company's needs, on-demand resources are accessible.

Disadvantages of the Public Cloud Model:

- **Less secure:** Public cloud is less secure as resources are public so there is no guarantee of high-level security.
- **Low customization:** It is accessed by many public so it can't be customized according to personal requirements.

HYBRID CLOUD: The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities. However, these entities are bound together by standardized or proprietary technology that enables data and application portability, for example, cloud bursting. Figure 6-3 shows cloud computing deployment models



Advantages of the hybrid cloud model:

- **Flexibility and control:** Businesses with more flexibility can design personalized solutions that meet their particular needs.
- **Cost:** Because public clouds provide scalability, you'll only be responsible for paying for the extra capacity if you require it.
- **Security:** Because data is properly separated, the chances of data theft by attackers are considerably reduced.

Disadvantages of the hybrid cloud model:

- **Difficult to manage:** Hybrid clouds are difficult to manage as it is a combination of both public and private cloud. So, it is complex.
- **Slow data transmission:** Data transmission in the hybrid cloud takes place through the public cloud so latency occurs.

➔ BIG DATA ANALYTICS :

- Big data analytics is the process of collecting, examining, and analysing large amounts of data to discover market trends, insights, and patterns that can help companies make better business decisions.
- This information is available quickly and efficiently so that companies can be agile in crafting plans to maintain their competitive advantage.
- Technologies such as business intelligence (BI) tools and systems help organisations take unstructured and structured data from multiple sources.
- Users (typically employees) input queries into these tools to understand business operations and performance.
- Big data analytics uses the four data analysis methods to uncover meaningful insights and derive solutions.
    - *For example, big data analytics is integral to the modern health care industry. As you can imagine, systems that must manage thousands of patient records, insurance plans, prescriptions, and vaccine information.*

THE IMPORTANCE OF BIG DATA ANALYTICS:

- Big data analytics is important because it helps companies leverage their data to identify opportunities for improvement and optimisation.
- Across different business segments, increasing efficiency leads to overall more intelligent operations, higher profits, and satisfied customers.
- Big data analytics helps companies reduce costs and develop better, customer-centric products and services.
- Data analytics helps provide insights that improve the way our society functions. In health care, big data analytics not only keeps track of and analyses individual records but it plays a critical role in measuring outcomes on a global scale.
- During the COVID-19 pandemic, big data-informed health ministries within each nation's government on how to proceed with vaccinations and devised solutions for mitigating pandemic outbreaks in the future.

BENEFITS OF BIG DATA ANALYTICS:

Incorporating big data analytics into a business or organisation has several advantages. These include:

- ***Cost reduction*:** Big data can reduce costs in storing all business data in one place. Tracking analytics also helps companies find ways to work more efficiently to cut costs wherever possible.
- ***Product development:*** Developing and marketing new products, services, or brands is much easier when based on data collected from customers' needs and wants. Big data analytics also helps businesses understand product viability and to keep up with trends.
- ***Strategic business decisions*:** The ability to constantly analyse data helps businesses make better and faster decisions, such as cost and supply chain optimisation.
- ***Customer experience*:** Data-driven algorithms help marketing efforts (targeted ads, for example) and increase customer satisfaction by delivering an enhanced customer experience.
- ***Risk management*:** Businesses can identify risks by analysing data patterns and developing solutions for managing those risks.

BIG DATA IN THE REAL WORLD:

Big data analytics helps companies and governments make sense of data and make better, informed decisions.

• **Entertainment:** Providing a personalised recommendation of movies and music according to a customer's preferences has been transformative for the entertainment industry (think Spotify and Netflix).

• **Education:** Big data helps schools and educational technology companies develop new curriculums while improving existing plans based on needs and demands.

• **Health care:** Monitoring patients' medical histories helps doctors detect and prevent diseases.

• **Government:** Big data can be used to collect data from CCTV and traffic cameras, satellites, body cameras and sensors, emails, calls, and more, to help manage the public sector.

• **Marketing:** Customer information and preferences can be used to create targeted advertising campaigns with a high return on investment (ROI).

• **Banking:** Data analytics can help track and monitor illegal money laundering.

TYPES OF BIG DATA ANALYTICS (+ EXAMPLES):

Four main types of big data analytics support and inform different business decisions.

1. Descriptive analytics:

Descriptive analytics refers to data that can be easily read and interpreted. This data helps create reports and visualise information that can detail company profits and sales**.**

Example: During the pandemic, a leading pharmaceutical company conducted data analysis on its offices and research labs. Descriptive analytics helped them identify consolidated unutilised spaces and departments, saving the company millions of pounds.

2. Diagnostics analytics:

Diagnostics analytics helps companies understand why a problem occurred. Big data technologies and tools allow users to mine and recover data that helps dissect an issue and prevent it from happening in the future.

Example: An online retailer's sales have decreased even though customers continue to add items to their shopping carts. Diagnostics analytics helped to understand that the payment page was not working correctly for a few weeks.

3. Predictive analytics:

Predictive analytics looks at past and present data to make predictions. With artificial intelligence (AI), machine learning, and data mining, users can analyse the data to predict market trends.

Example: In the manufacturing sector, companies can use algorithms based on historical data to predict if or when a piece of equipment will malfunction or break down.

4. Prescriptive analytics:

Prescriptive analytics solves a problem, relying on AI and machine learning to gather and use data for risk management.

Example: Within the energy sector, utility companies, gas producers, and pipeline owners identify factors that affect the price of oil and gas to hedge risks.

BIG DATA ANALYTICS TOOLS:

Harnessing all of that data requires tools. Thankfully, technology has advanced so that many intuitive software systems are available for data analysts to use.

- **Hadoop:** An open-source framework that stores and processes big data sets. Hadoop can handle and analyses structured and unstructured data.

- **Spark:** An open-source cluster computing framework for real-time processing and data analysis.

- **Data integration software**: Programs that allow big data to be streamlined across different platforms, such as MongoDB, Apache, Hadoop, and Amazon EMR.

- **Stream analytics tools:** Systems that filter, aggregate, and analyse data that might be stored in different platforms and formats, such as Kafka.

- **Distributed storage:** Databases that can split data across multiple servers and can identify lost or corrupt data, such as Cassandra.

- **Predictive analytics hardware and software:** Systems that process large amounts of complex data, using machine learning and algorithms to predict future outcomes, such as fraud detection, marketing, and risk assessments.

- **Data mining tools:** Programs that allow users to search within structured and unstructured big data.

- **NoSQL databases:** non-relational data management systems ideal for dealing with raw and unstructured data.

- **Data warehouses:** Storage for large amounts of data collected from many different sources, typically using predefined schemas.

➔ SOCIAL NETWORKING:

Social Networking refers to grouping of individuals and organizations together via some medium, in order to share thoughts, interests, and activities.

There are several web based social network services are available such as facebook, twitter, linkedin, Google+ etc. which offer easy to use and interactive interface to connect with people with in the country an overseas as well. There are also several mobile based social networking services in for of apps such as Whatsapp, hike, Line etc.

Available Social networking Services:

The following table describes some of the famous social networking services provided over web and mobile:

S.N.	Service Description
1.	**Facebook** Allows to share text, photos, video etc. It also offers interesting online games.
2.	**Google+** It is pronounced as Google Plus. It is owned and operated by Google.
3.	**Twitter**

Twitter allows the user to send and reply messages in form of tweets. These tweets are the small message characters.
Faceparty Faceparty is a UK based social networking site. It allows the users to create profiles and interact with eac messages.
Linkedin Linkedin is a business and professional networking site.
Flickr Flickr offers image hosting and video hosting.
Ibibio Ibibio is a talent based social networking site. It allows the users to promote one's self and also discover ne
 WhatsApp It is a mobile based messaging app. It allows to send text, video, and audio messages
Line It is same as whatsapp. Allows to make free calls and messages.
Hike It is also mobile based messager allows to send messages and exciting emoticons.

Website like linkedin allows us to create connection with professionals and helps to find the suitable job based on one's specific skills set.

Online News:

On social networking sites, people also post daily news which helps us to keep us updated.

Chatting:

Social networking allows us to keep in contact with friends and family. We can communicate with them via messages.

Share Picture, Audio and video:

One can share picture, audio and video using social networking sites.

➔ MOBILE COMPUTING:

- Mobile Computing is a technology that provides an environment that enables users to transmit data from one device to another device without the use of any physical link or cables.

- In other words, you can say that mobile computing allows transmission of data, voice and video via a computer or any other wireless-enabled device without being connected to a fixed physical link. In this technology, data transmission is done wirelessly with the help of wireless devices such as mobiles, laptops etc.

- This is only because of Mobile Computing technology that you can access and transmit data from any remote locations without being present there physically. Mobile computing technology provides a vast coverage diameter for communication. It is one of the fastest and most reliable sectors of the computing technology field.

The concept of Mobile Computing can be divided into three parts:

- *Mobile Communication*
- *Mobile Hardware*
- *Mobile Software*

MOBILE COMMUNICATION:

- Mobile Communication specifies a framework that is responsible for the working of mobile computing technology. In this case, mobile communication refers to an infrastructure that ensures seamless and reliable communication among wireless devices.
- This framework ensures the consistency and reliability of communication between wireless devices. The mobile communication framework consists of communication devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. These devices are responsible for delivering a smooth communication process.

Mobile communication can be divided in the following four types:

1. Fixed and Wired
2. Fixed and Wireless
3. Mobile and Wired
4. Mobile and Wireless

Fixed and Wired: In Fixed and Wired configuration, the devices are fixed at a position, and they are connected through a physical link to communicate with other devices.

For Example, Desktop Computer.

Fixed and Wireless: In Fixed and Wireless configuration, the devices are fixed at a position, and they are connected through a wireless link to make communication with other devices.

For Example, Communication Towers, WiFi router

Mobile and Wired: In Mobile and Wired configuration, some devices are wired, and some are mobile. They altogether make communication with other devices.

For Example, Laptops.

Mobile and Wireless: In Mobile and Wireless configuration, the devices can communicate with each other irrespective of their position. They can also connect to any network without the use of any wired device.

For Example, WiFi Dongle.

MOBILE HARDWARE:

- Mobile hardware consists of mobile devices or device components that can be used to receive or access the service of mobility.
- Examples of mobile hardware can be smartphones, laptops, portable PCs, tablet PCs, Personal Digital Assistants, etc.
- Hose devices are inbuilt with a receptor medium that can send and receive signals. These devices are capable of operating in full duplex.
- It means they can send and receive signals at the same time.
- They don't have to wait until one device has finished communicating for the other device to initiate communications.

MOBILE SOFTWARE:

- Mobile software is a program that runs on mobile hardware. This is designed to deal capably with the characteristics and requirements of mobile applications.
- This is the operating system for the appliance of mobile devices. In other words, you can say it the heart of the mobile systems.
- This is an essential component that operates the mobile device.

.

APPLICATIONS OF MOBILE COMPUTING:

- Web or Internet access.
- Global Position System (GPS).
- Emergency services.
- Entertainment services.
- Educational services.

ADVANTAGES OF MOBILE COMPUTING :

The advantages of mobile, ubiquitous computing include the following:

Portability:

- Mobile devices are smaller and more portable than traditional computers, making them easy to carry and use in a range of contexts.
- They work disconnected from a power source and without a physical network connection and when disconnected from the network.

Affordability:

- Over time, mobile devices have become less expensive and easier to obtain. Increasingly, people opt for smartphones and tablets as their primary means of online connectivity.
- And it is often cheaper to buy a smartphone than a desktop PC.

Wireless communications:

- Mobile devices let users engage in phone, video and various text and instant messaging applications.

LIMITATIONS OF MOBILE COMPUTING:

Mobile computing is not without issues such as the following ones:

Power:

- Despite increasing battery life, power consumption continues to be an issue, and mobile devices must be recharged regularly.

Connectivity:

- While the mobile infrastructure continues to improve, there are areas where signal strength is poor or nonexistent.

Data security:

- Mobile computing raises significant data security vulnerabilities because business users, especially, may have sensitive data on their devices while traveling or working remotely.
- Companies must implement security measures and policies to keep corporate data secure.

Dependence:

- The flip side to the convenience of mobile devices is that consumers may become overly reliant on them, which can lead to compulsive or unhealthy behaviors such as smartphone addiction.

Distraction:

- Mobile devices can be distracting and potentially dangerous in a hazardous work envronment that requires the employee's attention, such as a construction site.
  They pose dangers if used inappropriately while driving.

➔ THIRD PLATFORM TECHNOLOGIES

First Platform:

First Platform (Mainframe) - late 1950s to present

The first platform is the mainframe computer system, which began in the late 1950s and continues today.

Second Platform:

Second Platform (Client/Server) - mid 1980s to present

The second platform is the client/server system, which began in the mid-1980s with PCs tapping into mainframe databases and applications.

Third Platform:

Third Platform (Social, Mobile, Cloud & Analytics, possibly IoT) - early 2010s to present

The third platform is a term coined by marketing firm International Data Corporation (IDC) to describe a model of computing platform. It was promoted as an interdependence between mobile computing, social media, cloud computing, information/analytics (big data), and possibly the Internet of Things.

A Facebook page on a mobile device.

No single "third platform" product has emerged, but there are a number of proprietary and free software products that enterprises can use to create, deploy and operate solutions that use third platform technologies.

Within an enterprise, a combination of these products that meet enterprise needs is a "third platform" for that enterprise. Its design can be considered part of Enterprise Architecture.

Suitable products include:

- The Eclipse integrated development environment
- The Cloud Foundry cloud application platform as a service
- The Docker container environment
- The Kubernetes container deployment and management environment
- The Apache Hadoop big data framework

THE PILLARS OF THE THIRD PLATFORM :

Social technology

- Gartner defined a social technology as, "Any technology that facilitates social interactions and is enabled by a communications capability, such as the Internet or a mobile device." This extends not only to social media but also to all social technologies that make social interaction possible. A VoIP service, for example, would be considered a social technology.
- In a trend that has been described as 'social everything', companies both big and small, will continue to inject a social element into every product and service.
- The cloud provides the infrastructure that makes the information accessible, the social technology helps to organise the data and facilitate access, and the mobile devices will provide the means by which most people receive the data.

Mobile devices

- The third platform is designed to give everybody access to big data via mobile devices; it is this mobility that really defines the third platform. A company representative on the road or working from home will have instant access to data through his or her mobile device with this third platform whenever and wherever they need it.
- An example of the use of mobile devices in the third platform would be a school that gives every student a tablet. The tablet would take the place of textbooks and paper used in assignments, but more importantly, the student will have access to a virtual classroom at additional times.[11]

Analytics (big data)

- The concept behind big data is to maximize the utility of all data. An executive at a company that streamlines its business functions with the third platform would have easy access to all of the data, including sales figures, personnel information, accounting data, financials and so on. This data can then be used to inform more areas of the business.
- Big data can be further differentiated once we analyze its three distinguishing features: **variety, volume, and velocity.**
    - *Variety* means that many forms of data are collected, with formats ranging from audio and video to client log files and Tweets.
    - *Volume* represents the fact that big data must come in massive quantities, often over a petabyte.
    - *Velocity* signifies that big data must be constantly collected for maximum effectiveness; even data that is a few days old is not ideal.

Cloud services

- Cloud services are at the heart of the third platform. Having big data and mobile devices is one thing, but without the cloud, there will be no way to access this data from outside of the office.
- This differs greatly from the first platform, where computer networks consisted of large mainframes. All of a company's employees had access to the data in the mainframe but they could only access it through their desktop computers.

- In the second platform, a company's employees could access the data in the mainframe as well as outside data, via an Internet connection.
- The third platform will allow all of a company's IT solutions to be available through the cloud, accessible via a variety of mobile devices. Data storage, servers and many IT solutions, which are on-site, can now be cloud-based.

Internet of Things (IOT)

- The Internet of Things is the network of connected devices that enable computer systems to monitor and control aspects of the physical environment. It has applications in personal and home environments, smart cities, factory automation, transport, and many other areas.
- The incorporation of the Internet of Things in the third platform gives enterprises the ability to interact with these systems and use these applications.
- Sensors and actuators have been used in computer systems for many years. It is the ability to connect to such devices anywhere in the world through the Internet that characterizes the Internet of things.

WHY BUSINESSES WILL NEVER SUCCEED WITHOUT THE THIRD PLATFORM? (or) ADVANTAGES

1) Can't keep up without the Third Platform solutions

The Third Platform consists of trillions of systems, electronics, devices, and sensors. It involves not only the users of apps or services that are interlinked to the devices but also anything with an IP address.

Social networking coupled with continually connected smart devices and a cloud-based server means that people have a greater online presence than ever and those businesses which do not accept this fact and adapt accordingly will not be able to either compete or keep up.

The point to note is that Third platform technologies solutions will predict problems, alert, suggest and even implement – in some cases – the solution, before the businesses will even register a problem exists.

Consider for example, sending an electrician to figure out exactly what is causing energy wastage in a building versus an automatic alert providing exact information about the burnt up wires in sector A, room B, slot C of that building.

The Third Platform offers speed, growth, results, innovation, adaptability and consolidation. Together, this will help make businesses -large and small – be more competitive, agile, effective and efficient.

2) You won't be able to go fully mobile or leverage the cloud without the Third Platform

Given that cloud computing is one futuristic solution that offers agile businesses deployment, network virtualisation and safe, scalable and sustainable business operations, businesses worldwide have already started to embrace it.

This trend is set to increase; just last year Forbes highlighted that 83% of enterprises' workloads would be interlinked to the cloud by next year.

3) Consumer interaction will go downhill

Third platform services are structured in a way to boost connectivity. With hyper-competition and relatively similar service offerings, customer-centricity put front and centre will be one way that suppliers could gain genuine competitive advantage.

With the 4 pillars of Cloud, Mobile, Social and Analytics getting established, both Gartner and IDC are prediction a new digital era that Gartner calls the Digital Industrial Revolution. ***IDC refers to 6 innovations accelerators sitting on top of the 4 pillars and accelerating the transformation to Digital.***

The 6 innovations accelerators are:

1. The Internet of Things (IoT)

As evidenced by the wave of new IoT devices and solutions at display at several tradeshows this year, the physical world is soon entering the digital era with future connected cars, houses, wallets, etc.

2. Cognitive systems

Analyzing the vast amount of IoT data created by the connected devices with the next wave of analytics tools (diagnostic, predictive and prescriptive), cognitive systems with observe, learn and offer suggestion thus reshaping the services industry.

3. Pervasive robotics

A new era of automation driven by knowledge gained from the digital world and set in action in the physical world with self-driving cars, drones, robots, etc.

4. 3-D printing of all kinds

Those printers will be creating physical things of all kind from a digital drawing: not only plastic parts (quite common now, my local library even has a 3D printer for plastic parts) and fine resolution metal parts but also food and clothing items, and, eventually, living tissues and organs!

5. Natural interfaces

Beyond mouse and keyboards, using touch and motion, speech (starting to be common on smartphones and cars nowadays) and also vision to connect people to their devices and 3rd Platform solutions.

6. Optimized security technologies and solutions

With the predicted massive amount of new connected IoT devices, a better way to secure access to systems and devices is required to avoid the security breaches we have experienced in 2014.

CHARACTERISTICS OF THIRD PLATFORM

1. On-Demand Self-Service

You can provision computing services, like server time and network storage, automatically.

You won’t need to interact with the service provider. Cloud customers can access their cloud accounts through a web self-service portal to view their cloud services, monitor their usage, and provision and de-provision services.

2. Broad Network Access

You can access services over the network and on portable devices like mobile phones, tablets, laptops, and desktop computers. Anyone, anywhere, anytime can connect, this should be guaranteed at all times.

3. Resource Pooling

With resource pooling, multiple customers can share physical resources using a multi-tenant model. This model assigns and reassigns physical and virtual resources based on demand. Multi-tenancy allows customers to share the same applications or infrastructure while maintaining privacy and security.

Though customers won't know the exact location of their resources, they may be able to specify the location at a higher level of abstraction, such as a country, state, or data center. Memory, processing, and bandwidth are among the resources that customers can pool.

4. Rapid Elasticity

It should be capable of handling massive expansion as no. of resources connected increasing sometimes automatically, so customers can scale quickly based on demand. The capabilities available for provisioning are practically unlimited.

Customers can engage with these capabilities at any time in any quantity.

5. Dynamic and Self-Adapting (Complexity)

Devices should dynamically adapt themselves to changing contexts and scenarios. Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, and night).

➔ Digital Transformation

Digital transformation is the incorporation of computer-based technologies into an organization's products, processes and strategies. Organizations undertake digital transformation to better engage and serve their workforce and customers and thus improve their ability to compete.

A digital transformation initiative can require an examination and reinvention of all facets of an organization, from supply chains and workflows, to employee skill sets and org charts, to customer interactions and value proposition to stakeholders.

➔ IMPERATIVES FOR THIRD PLATFORM TRANSFORMATION :

Five digital imperatives customers need to achieve:

1. Migrate to the Cloud
2. Empower Fusion Teams
3. Unify Data and Apply AI Models

4. Implement Collaborative Business Processes
5. Prioritize Security

Digital Imperative #1: Migrate to the Cloud

- Microsoft CEO Satya Nadella cited a Gartner report that estimates businesses will deploy 95% of new digital workloads on cloud-native platforms to serve as the foundation to be competitive.
- Businesses can scale IT resources on demand while also converting their IT spending model from CapEx to OpEX. The cloud also improves the operational efficiency of internal workflows and speeds up the time it takes to deliver new services to customers and internal users.

Digital Imperative #2: Empower Fusion Teams

- As defined by Gartner, a fusion team is a multidisciplinary team that blends technology with business domain expertise and shares accountability for business and technology outcomes. Given that every company is a digital company in today's economy, leveraging or outsourcing to a fusion team is critical.
- The challenge is, there's more demand for developers in some industries than available in the entire tech industry. To help solve this challenge, the Microsoft Power Platform provides the most complete developer platform. Gartner estimates by 2025, 70% of new enterprise applications will be built with low code or no code tools.

Digital Imperative #3: Unify Data and Apply AI Models

- Gartner projects that by 2025, 10% of all data will be produced by generative AI models. This illustrates how analytics is becoming a critical component for improving product experiences. Companies need to collect and leverage information on how customers use their products to generate insights on how to improve product performance.

Digital Imperative #4: Implement Collaborative Business Processes

- Hybrid work is here to stay—73% of employees want the flexibility to work remotely, and life balance and their well-being are non-negotiable. With this trend, you need to consider the changes in how people work and how this impacts your business processes.
- Automated collaboration is vital in meeting employee workstyle preferences, and you also need digital fabric to connect people, places, and processes.
- Microsoft Teams is particularly helpful in bridging the gap between people working in-person and remotely. Views in Teams can make it look like everyone is in the same room. With intelligent cameras, individual people in physical rooms are tracked when they're speaking. This ensures every meeting attendee is an active participant.

Digital Imperative #5: Security

- Cybercrime is expected to cost the world $10.5 trillion annually by 2025 so security must be a top priority. At the same time, there are 24 trillion threat signals a day across the globe.
- The Microsoft Cloud helps take on this challenge by bringing together technology and experts to offer the most comprehensive security, identity, compliance, and management solutions possible.
- The solution works across multiple cloud environments, and customers can expect to save more than 60% in cyber security costs on average when they use Microsoft solutions.

- One particularly important new ability that Microsoft has launched is encrypting data while it's in use without changing applications. This quickly safeguards digital assets and will help with compliance for customers in regulated industries.

➔ DATA CENTER ENVIRONMENT

What is a Data Center?

- A data center is a facility that provides shared access to applications and data using a complex network, compute, and storage infrastructure. Industry standards exist to assist in designing, constructing, and maintaining data center facilities and infrastructures to ensure the data is both secure and highly available.

TYPES OF DATA CENTERS

- Data centers vary in size, from a small server room all the way up to groups of geographically distributed buildings, but they all share one thing in common: they are a critical business asset where companies often invest in and deploy the latest advancements in data center networking, compute and storage technologies.
- The modern data center has evolved from a facility containing an on-premises infrastructure to one that connects on-premises systems with cloud infrastructures where networks, applications and workloads are virtualized in multiple private and public clouds.

Enterprise data centers are typically constructed and used by a single organization for their own internal purposes. These are common among tech giants.

Colocation data centers function as a kind of rental property where the space and resources of a data center are made available to the people willing to rent it.

Managed service data centers offer aspects such as data storage, computing, and other services as a third party, serving customers directly.

Cloud data centers are distributed and are sometimes offered to customers with the help of a third-party managed service provider.

EVOLUTION OF THE DATA CENTER TO THE CLOUD

- The fact that virtual cloud DC can be provisioned or scaled-down with only a few clicks is a major reason for shifting to the cloud. In modern data centers, software-defined networking (SDN) manages the traffic flows via software.
- Infrastructure as a Service (IaaS) offerings, hosted on private and public clouds, spin up whole systems on-demand. When new apps are needed, Platform as a Service (PaaS) and container technologies are available in an instant.

➔ DATA CENTER ARCHITECTURE COMPONENTS OR BUILDING BLOCKS OF A DATA CENTER :

Data centers are made up of three primary types of components:
compute, storage, and network.

Apart from the Data Centers, support infrastructure is essential to meeting the service level agreements of an enterprise data center.

Data Center Computing

- Servers are the engines of the data center. On servers, the processing and memory used to run applications may be physical, virtualized, distributed across containers, or distributed among remote nodes in an edge computing model.
- Data centers must use processors that are best suited for the task, e.g. general purpose CPUs may not be the best choice to solve artificial intelligence (AI) and machine learning (ML) problems.

Data Center Storage

- Data centers host large quantities of sensitive information, both for their own purposes and the needs of their customers. Decreasing costs of storage media increases the amount of storage available for backing up the data either locally, remote, or both.
- Advancements in non-volatile storage media lowers data access times.
- In addition, as in any other thing that is software-defined, software-defined storage technologies increase staff efficiency for managing a storage system.

Data Center Networks

- Datacenter network equipment includes cabling, switches, routers, and firewalls that connect servers together and to the outside world. Properly configured and structured, they can manage high volumes of traffic without compromising performance.
- A typical three-tier network topology is made up of core switches at the edge connecting the data center to the Internet and a middle aggregate layer that connects the core layer to the access layer where the servers reside.
- Advancements, such as hyperscale network security and software-defined networking, bring cloud-level agility and scalability to on-premises networks.

➔ COMPUTE SYSTEMS OF DATA CENTER :

In the data center, compute refers to the processing power and memory required to run applications on a server. It is one of the three major components of data center along with storage and networking. A good compute platform should scale easily and provide flexible connections for Any-Prem workloads: on-premises, hybrid, or cloud.

➔ DATA CENTER VIRTUALIZATION

Data center virtualization is the transfer of physical data centers into digital data centers (i.e., virtual) using a cloud software platform, enabling companies to remotely access information and applications.

Data center virtualization is the process of creating a virtual server—sometimes called a **software defined data center (SDCC)**—from traditional, physical servers.

➔ SOFTWARE - DEFINED DATA CENTER (SDDC)

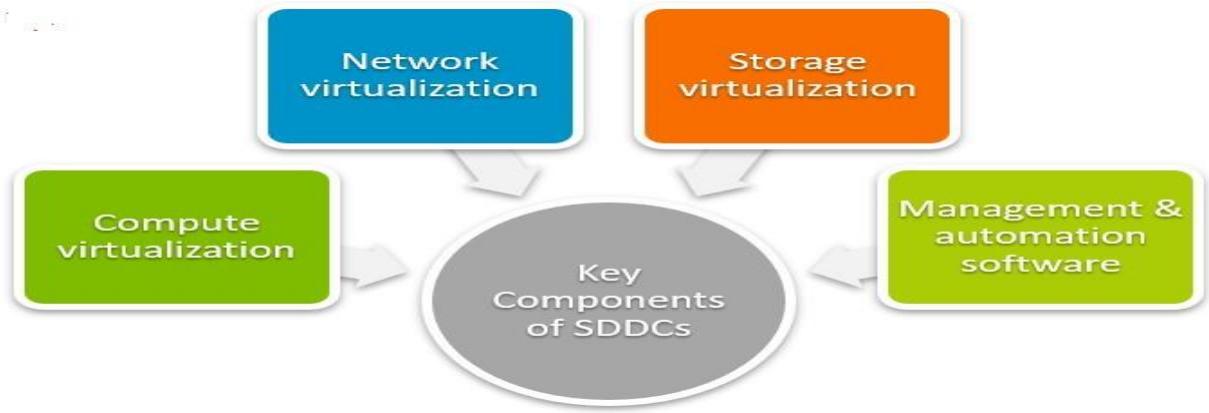
A traditional data center is a facility where organizational data, applications, networks, and infrastructure are centrally housed and accessed. It is the hub for IT operations and physical infrastructure equipment, including servers, storage devices, network equipment, and security devices. Traditional data centers can be hosted:

- On-premise
- With a managed service provider (MSP)
- In the cloud

In contrast, a software-defined data center is an IT-as-a-Service (ITaaS) platform that services an organization's software, infrastructure, or platform needs. An SDDC can be housed on-premise, at an MSP, and in private, public, or hosted clouds. (For our purposes, we will discuss the benefits of hosting an SDDC in the cloud.) Like traditional data centers, SDDCs also host servers, storage devices, network equipment, and security devices. You can manage SDDCs from any location, using remote APIs and Web browser interfaces. SDDCs also make extensive use of automation capabilities to:

- Reduce IT resource usage
- Provide automated deployment and management for many core functions

KEY COMPONENTS OF SDDC



- **Compute virtualization**, where virtual machines (VMs)—including their operating systems, CPUs, memory, and software—reside on cloud servers. Compute virtualization allows users to create software implementations of computers that can be spun up or spun down as needed, decreasing provisioning time.
- **Network virtualization**, where the network infrastructure servicing your VMs can be provisioned without worrying about the underlying hardware. Network infrastructure needs—telecommunications,

firewalls, subnets, routing, administration, DNS, etc.—are configured inside your cloud SDDC on the vendor's abstracted hardware. No network hardware assembly is required.

- **Storage virtualization**, where disk storage is provisioned from the SDDC vendor's storage pool. You get to choose your storage types, based on your needs and costs. You can quickly add storage to a VM when needed.
- **Management and automation software.** SDDCs use management and automation software to keep business critical functions working around the clock, reducing the need for IT manpower. Remote management and automation is delivered via a software platform accessible from any suitable location, via APIs or Web browser access.

You can also connect additional critical software to connect with and customize your SDDC platform. But, for companies just moving to an SDDC, your first goal is to get your basic operations software infrastructure ready for the transition. Customizing can come later.

Benefits of SDDCs

1. Business agility

An SDDC offers several benefits that improve business agility with a focus on three key areas:

- Balance
- Flexibility
- Adaptability

2. Reduced cost

In general, it costs less to operate an SDDC than housing data in brick-and-mortar data centers. Cloud SDDCs operate similarly to SaaS platforms that charge a recurring monthly cost.

This is usually an affordable rate, making an SDDC accessible to all types of businesses, even those who may not have a big budget for technology spending.

3. Increased scalability

By design, cloud SDDCs can easily expand along with your business. Increasing your storage space or adding functions is usually as easy as contacting the data facility to get a revised monthly service quote.

UNIT II

INTELLIGENT STORAGE SYSTEMS AND RAID

INTELLIGENT STORAGE SYSTEM :

Business-critical applications require high levels of performance, availability, security, and scalability. A hard disk drive is a core element of storage that governs the perfor- mance of any storage system.

Some of the older disk array technologies could not overcome per- formance constraints due to the limitations of a hard disk and its mechanical components. RAID technology made an important contribution to enhancing storage performance and reliability, but hard disk drives even with a RAID implementation could not meet performance require- ments of today's applications.

With advancements in technology, a new breed of storage solutions known as an *intelligent storage system* has evolved. These storage systems are configured with large amounts of memory called *cache* and use sophisticated algorithms to meet the I/O requirements of performance- sensitive applications.

➔ COMPONENTS OF AN INTELLIGENT STORAGE SYSTEM

An intelligent storage system consists of four key components: *front end, cache, back end,* and *physical disks*.

Figure 4-1 illustrates these components and their interconnections.

An I/O request received from the host at the front-end port is processed through cache and the back end, to enable storage and retrieval of data from the physical disk**.** A read request can be serviced directly from cache if the requested data is found in cache.

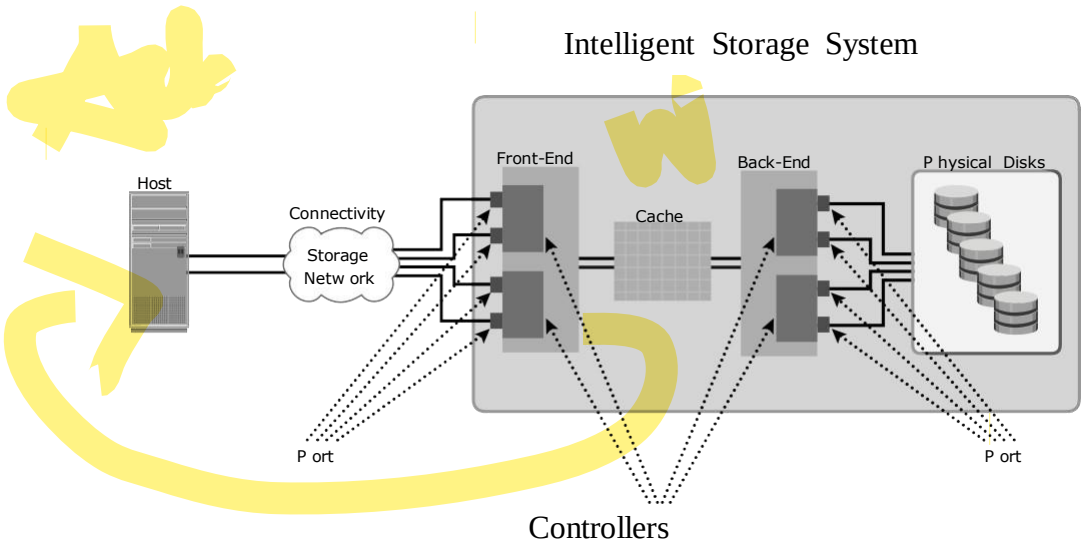


Figure 4-1: Components of an intelligent storage system

FRONT END

- The front end provides the interface between the storage system and the host. It consists of two components: front-end ports and front-end controllers.
- The *front-end ports* enable hosts to connect to the intelligent storage system. Each front-end port has processing logic that executes the appropriate transport protocol, such as SCSI, Fibre Channel, or iSCSI, for storage connections.
- Redundant ports are provided on the front end for high availability.
- *Front-end controllers* route data to and from cache via the internal data bus.
- When cache receives write data, the controller sends an acknowledgment message back to the host. Controllers optimize I/O processing by using command queuing algorithms.

Front-End Command Queuing

- *Command queuing* is a technique implemented on front-end controllers. It determines the execution order of received commands and can reduce unnecessary drive head movements and improve disk performance.
- When a command is received for execution, the command queuing algorithms assigns a tag that defines a sequence in which commands should be

executed.

- With command queuing, multiple commands can be executed concurrently based on the organization of data on the disk, regardless of the order in which the commands were received.
- ***The most commonly used command queuing algorithms are as follows:***
  - **First In First Out** (FIFO)**:** This is the default algorithm where commands are executed in the order in which they are received (Figure 4-2 [a]). There is no reordering of requests for optimization; therefore, it is inef- ficient in terms of performance.
  - **Seek Time Optimization:** Commands are executed based on optimizing read/write head movements, which may result in reordering of com-mands.

    Without seek time optimization, the commands are executed in the order they are received.

    For example, as shown in Figure 4-2(a), the commands are executed in the order A, B, C and D. The radial movement required by the head to execute C immediately after A is less than what would be required to execute B.

    With seek time optimization, the command execution sequence would be A, C, B and D, as shown in Figure 4-2(b).

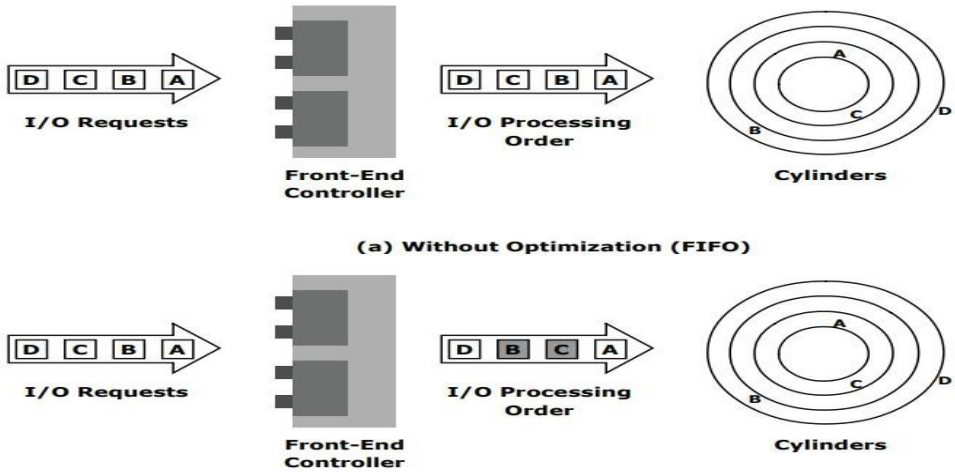


Figure 4-2: Front-end command queuing

- **Access Time Optimization:** Commands are executed based on the combination of seek time optimization and an analysis of rotational latency for optimal performance.

CACHE

- Cache is an important component that enhances the I/O performance in an intelligent storage system.
- Cache is semiconductor memory where data is placed temporarily to reduce the time required to service I/O requests from the host.
- Cache improves storage system performance by isolating hosts from the mechanical delays associated with physical disks, which are the slowest compo- nents of an intelligent storage system.
- Accessing data from a physical disk usu- ally takes a few milliseconds because of seek times and rotational latency. If a disk has to be accessed by the host for every I/O operation, requests are queued, which results in a delayed response.
- Accessing data from cache takes less than a millisecond. Write data is placed in cache and then written to disk. After the data is securely placed in cache, the host is acknowledged immediately.

Structure of Cache

✓ Cache is organized into pages or slots, which is the smallest unit of cache allo- cation.

✓ The size of a cache page is configured according to the application I/O size. Cache consists of the *data store* and *tag RAM*.

✓ The data store holds the data while tag RAM tracks the location of the data in the data store (see Figure 4-3) and in disk.

✓ Entries in tag RAM indicate where data is found in cache and where the data belongs on the disk. Tag RAM includes a *dirty bit* flag, which indicates whether the data in cache has been committed to the disk or not.

✓ It also contains time-based information, such as the time of last access, which is used to identify cached information that has not been accessed for a long period and may be freed up.

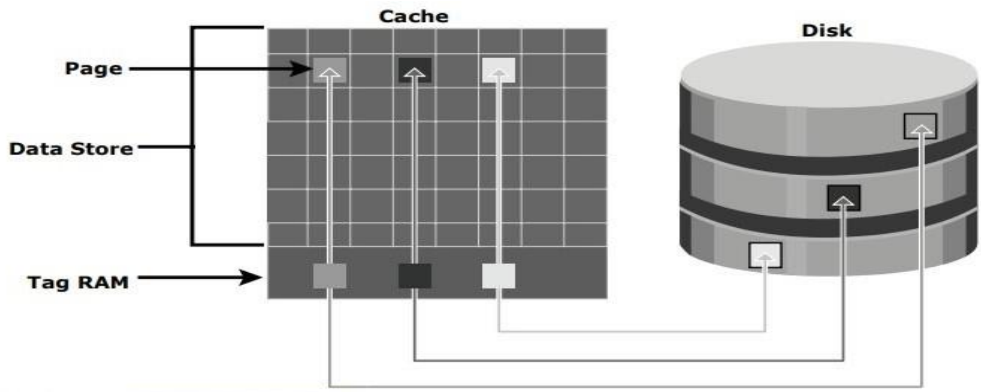


Figure 4-3: Structure of cache

Read Operation with Cache

✓ When a host issues a read request, the front-end controller accesses the tag RAM to determine whether the required data is available in cache.

✓ If the requested data is found in the cache, it is called a *read cache hit* or *read hit* and data is sent directly to the host, without any disk operation (see Figure 4-4[a]). This provides a fast response time to the host (about a millisecond).

✓ If the requested data is not found in cache, it is called a *cache miss* and the data must be read from the disk (see Figure 4-4[b]).

✓ The back-end controller accesses the appropriate disk and retrieves the requested data. Data is then placed in cache and is finally sent to the host through the front-end controller. Cache misses increase I/O response time.

✓ A *pre-fetch,* or *read-ahead,* algorithm is used when read requests are sequential. In a sequential read request, a contiguous set of associated blocks is retrieved. Several other blocks that have not yet been requested by the host can be read from the disk and placed into cache in advance.

✓ The intelligent storage system offers fixed and variable pre-fetch sizes.

✓ In *fixed pre-fetch*, the intelligent storage system pre-fetches a fixed amount of data. It is most suitable when I/O sizes are uniform.
In *variable pre-fetch*, the storage system pre-fetches an amount of data in multiples of the size of the host request.

✓ Read performance is measured in terms of the ***read hit ratio,*** **or the** ***hit rate***, usually expressed as a percentage.

This ratio is the number of read hits with respect to the total number of read requests. A higher read hit ratio improves the read performance.

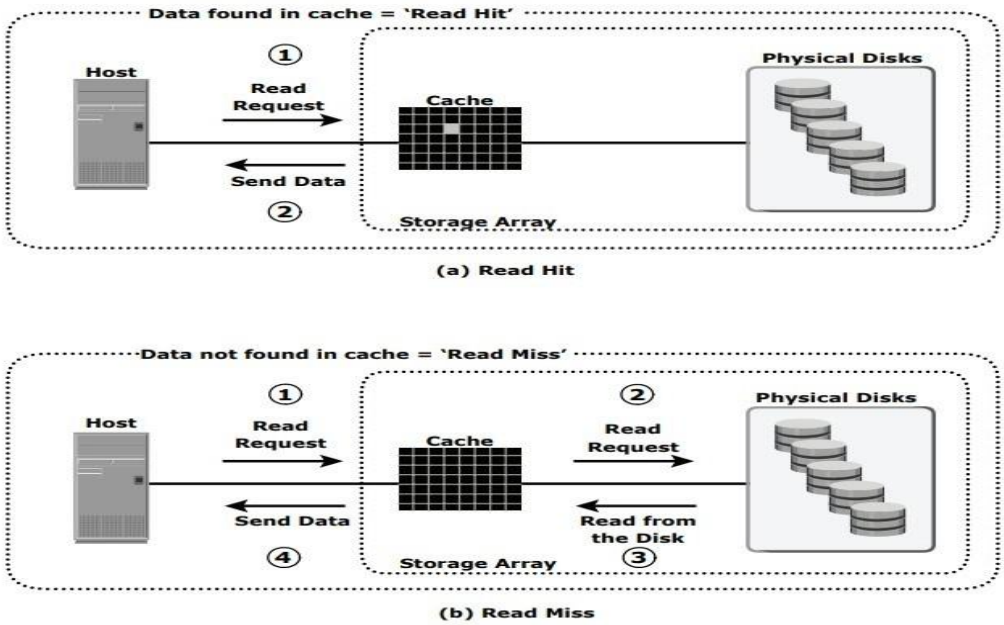


Figure 4-4: Read hit and read miss

Write Operation with Cache

✓ Write operations with cache provide performance advantages over writing directly to disks. When an I/O is written to cache and acknowledged, it is completed in far less time (from the host's perspective) than it would take to write directly to disk.

✓ A write operation with cache is implemented in the following ways:

- **Write-back cache:** Data is placed in cache and an acknowledgment is sent to the host immediately. Later, data from several writes are committed (de-staged) to the disk. Write response times are much faster, as the write operations are isolated from the mechanical delays of the disk. However, uncommitted data is at risk of loss in the event of cache failures.
- **Write-through cache:** Data is placed in the cache and immediately writ- ten to the disk, and an acknowledgment is sent to the host. Because data is committed to disk as it arrives, the risks of data loss are low but write response time is longer because of the disk operations.

Cache can be bypassed under certain conditions, such as very large size write I/O.

In this implementation, if the size of an I/O request exceeds the pre- defined size, called *write aside size*, writes are sent to the disk directly to reduce the impact of large writes consuming a large cache area.

Cache Implementation

✓ Cache can be implemented as either dedicated cache or global cache. With dedicated cache, separate sets of memory locations are reserved for reads and writes. In global cache, both reads and writes can use any of the available memory addresses. Cache management is more efficient in a global cache implementation, as only one global set of addresses has to be managed.

Cache Management

✓ Cache is a finite and expensive resource that needs proper management.

✓ Even though intelligent storage systems can be configured with large amounts of cache, when all cache pages are filled, some pages have to be freed up to accom modate new data and avoid performance degradation.

✓ Various cache manage- ment algorithms are implemented in intelligent storage systems :

- **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.

- **Most Recently Used (MRU):** An algorithm that is the converse of LRU. In MRU, the pages that have been accessed most recently are freed up or marked for reuse.

✓ As cache fills, the storage system must take action to flush dirty pages (data written into the cahce but not yet written to the disk) in order to manage its availability.

✓ **Flushing** is the process of committing data from cache to the disk. On the basis of the I/O access rate and pattern, high and low levels called *watermarks* are set in cache to manage the flushing process.

✓ *High watermark (HWM)* is the cache utilization level at which the storage system starts high- speed flushing of cache data.

Low watermark (LWM) is the point at which the storage system stops the high-speed or forced flushing and returns to idle flush behavior.

The cache utilization level, as shown in Figure 4-5, 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 to flushing.
- **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, dirty pages are forcibly flushed to disk.

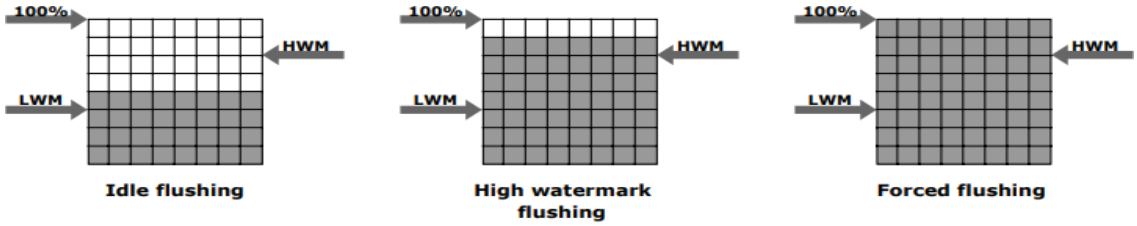


Figure 4-5: Types of flushing

Cache Data Protection

✓ Cache is volatile memory, so a power failure or any kind of cache failure will cause the loss of data not yet committed to the disk.
This risk of losing uncommitted data held in cache can be mitigated using *cache mirroring* and *cache vaulting*:

- **Cache mirroring:** Each write to cache is held in two different memory locations on two independent memory cards. In the event of a cache failure, the write data will still be safe in the mirrored location and can be committed to the disk.
  In cache mirroring approaches, the problem of maintaining *cache coherency* is introduced.
  Cache coherency means that data in two different cache locations must be identical at all times.
- **Cache vaulting:** Cache is exposed to the risk of uncommitted data loss due to power failure.
  This problem can be addressed in various ways:
  power- ing the memory with a battery until AC power is restored or using battery power to write the cache content to the disk.

BACK END

- The *back end* provides an interface between cache and the physical disks. It con- sists of two components: back-end ports and back-end controllers.
- The back end controls data transfers between cache and the physical disks. From cache, data is sent to the back end and then routed to the destination disk. Physical disks are connected to ports on the back end.
- The back end controller communicates with the disks when performing reads and writes

and also provides additional, but lim ited, temporary data storage.

PHYSICAL DISK

A physical disk stores data persistently.

Disks are connected to the back-end with either SCSI or a Fibre Channel interface.

An intelligent storage system enables the use of a mixture of SCSI or Fibre Channel drives and IDE/ATA drives.

Logical Unit Number

- ✓ Physical drives or groups of RAID protected drives can be logically split into vol- umes known as logical volumes, commonly referred to as *Logical Unit Numbers* (LUNs).
- ✓ The use of LUNs improves disk utilization.
- ✓ For example, without the use of LUNs, a host requiring only 200 GB could be allocated an entire 1TB physical disk. Using LUNs, only the required 200 GB would be allocated to the host, allowing the remaining 800 GB to be allocated to other hosts.

For example, Figure 4-6 shows a RAID set consisting of five disks that have been sliced, or partitioned, into several LUNs. LUNs 0 and 1 are shown in the figure.

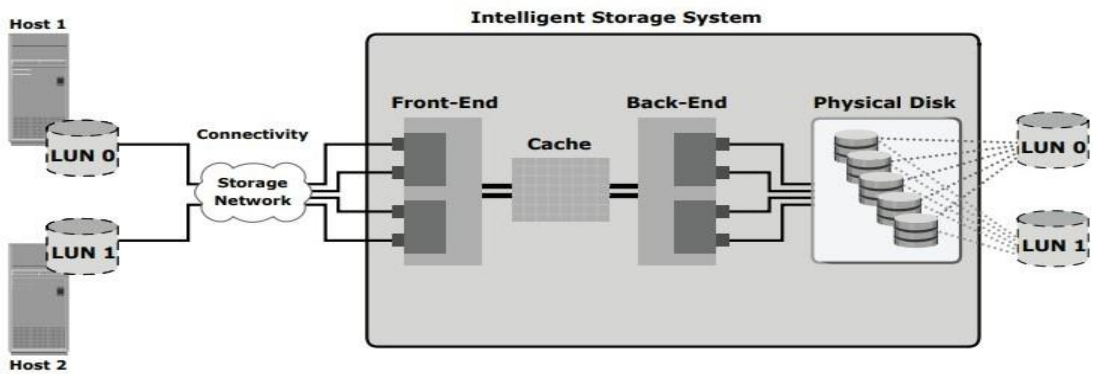


Figure 4-6: Logical unit number

Note how a portion of each LUN resides on each physical disk in the RAID set.

LUNs 0 and 1 are presented to hosts 1 and 2, respectively, as physical vol- umes for storing and retrieving data. Usable capacity of the physical volumes is determined by the RAID type of the RAID set.

The capacity of a LUN can be expanded by aggregating other LUNs with it. The result of this aggregation is a larger capacity LUN, known as a *meta- LUN*. The mapping of LUNs to their physical location on the drives is man- aged by the operating environment of an intelligent storage system.

LUN Masking

- ✓ *LUN masking* is a process that provides data access control by defining which LUNs a host can access.
- ✓ LUN masking function is typically implemented at the front end controller. This ensures that volume access by servers is controlled appropriately, preventing unauthorized or accidental use in a distributed 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.

➔ DISK DRIVE COMPONENTS

- A disk drive uses a rapidly moving arm to read and write data across a flat platter coated with magnetic particles. Data is transferred from the magnetic platter through the R/W head to the computer.
- Several platters are assembled together with the R/W head and controller, most commonly referred to as a *hard disk drive (HDD)*.
    - ○

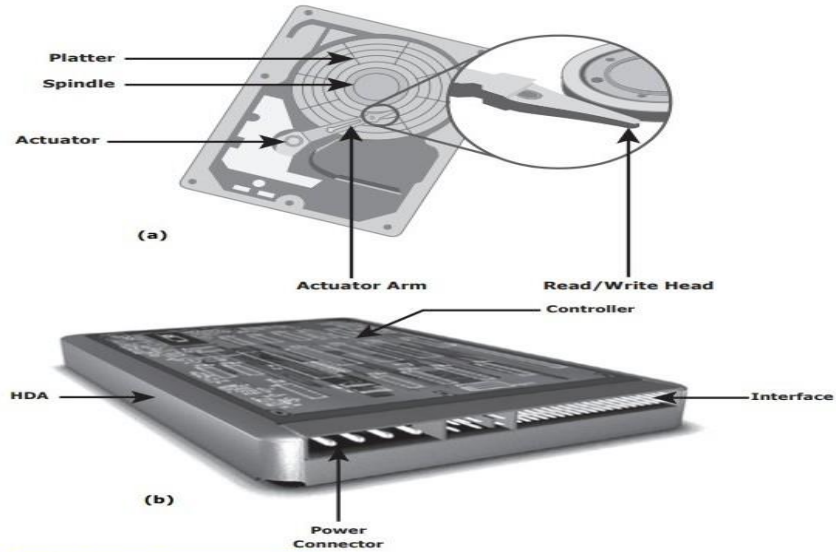


Figure 2-2: Disk Drive Components

- Data can be recorded and erased on a magnetic disk any number of times.

Key components of a disk drive are *platter, spindle, read/write head, actuator arm assembly, and controller* (Figure 2-2):

PLATTER

✓ A typical HDD consists of one or more flat circular disks called *platters* (Figure 2-3). The data is recorded on these platters in binary codes (0s and 1s).

✓ The set of rotating platters is sealed in a case, called a *Head Disk Assembly (HDA)*. A platter is a rigid, round disk coated with magnetic material on both surfaces (top and bottom).

✓ The data is encoded by polarizing the magnetic area, or domains, of the disk surface. Data can be written to or read from both surfaces of the platter.

✓ The number of platters and the storage capacity of each platter determine the total capacity of the drive.

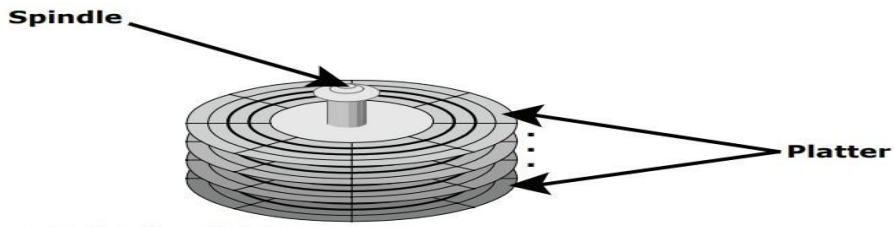


Figure 2-3: Spindle and platter

SPINDLE

- ✓ A spindle connects all the platters, as shown in Figure 2-3, and is connected to a motor. The motor of the spindle rotates with a constant speed.
- ✓ The disk platter spins at a speed of several thousands of revolutions per minute (rpm). Disk drives have spindle speeds of 7,200 rpm, 10,000 rpm, or 15,000 rpm. Disks used on current storage systems have a platter diameter of 3.5" (90 mm).
- ✓ When the platter spins at 15,000 rpm, the outer edge is moving at around 25 percent of the speed of sound.

READ/WRITE HEAD

- ✓ *Read/Write (R/W) heads*, shown in Figure 2-4, read and write data from or to a platter.
- ✓ Drives have two R/W heads per platter, one for each surface of the platter.
- ✓ The R/W head changes the magnetic polarization on the surface ofthe platter when writing data. While reading data, this head detects magnetic polarization on the surface of the platter.
- ✓ During reads and writes, the R/W head senses the magnetic polarization and never touches the surface of the platter. When the spindle is rotating, there is a microscopic air gap between the R/W heads and the platters, known as the *head flying height*.
- ✓ This air gap is removed when the spindle stops rotating and the R/W head rests on a special area on the platter near the spindle. This area is called the *landing zone*. The landing zone is coated with a lubricant to reduce friction between the head and the

platter.

✓ The logic on the disk drive ensures that heads are moved to the landing zone before they touch the surface. If the drive malfunctions and the R/W head accidentally touches the surface of the platter outside the landing zone, a *head crash* occurs.

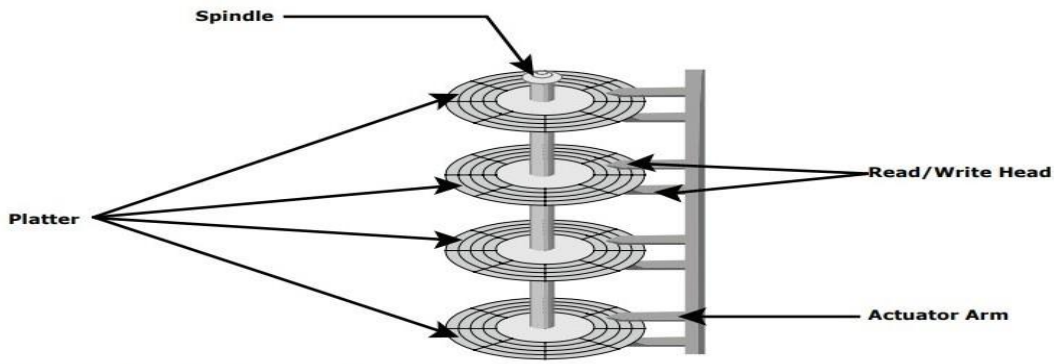


Figure 2-4: Actuator arm assembly

ACTUATOR ARM ASSEMBLY

✓ The R/W heads are mounted on the *actuator arm assembly* (refer to Figure 2-2 [a]), which positions the R/W head at the location on the platter where the data needs to be written or read. The R/W heads for all platters on a drive are attached to one actuator arm assembly and move across the platters simultaneously.

CONTROLLER

✓ The *controller* (see Figure 2-2 [b]) is a printed circuit board, mounted at the bot- tom of a disk drive. It consists of a microprocessor, internal memory, circuitry, and firmware.

✓ The firmware controls power to the spindle motor and the speed of the motor. It also manages communication between the drive and the host.

✓ In addition, it controls the R/W operations by moving the actuator arm and switching between different R/W heads, and performs the optimization of data access.

2

Physical Disk Structure

- Data on the disk is recorded on *tracks*, which are concentric rings on the platter around the spindle, as shown in Figure 2-5. The tracks are numbered, starting from zero, from the outer edge of the platter. The number of *tracks per inch (TPI)* on the platter (or the *track density*) measures how tightly the tracks are packed on a platter.
- Each track is divided into smaller units called *sectors*. A sector is the smallest, individually addressable unit of storage. The track and sector structure is written on the platter by the drive manufacturer using a formatting operation. The number of sectors per track varies according to the specific drive.

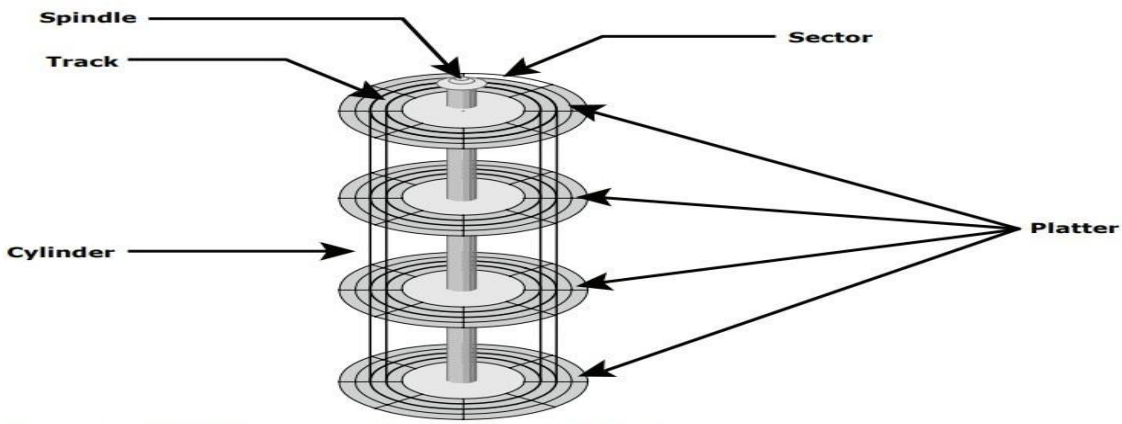


Figure 2-5: Disk structure: sectors, tracks, and cylinders

Typically, a sector holds 512 bytes of user data, although some disks can be formatted with larger sector sizes. In addition to user data, a sector also stores other information, such as sector number, head number or platter number, and track number.

Consequently, there is a difference between the capacity of an unformatted disk and a format- ted one. Drive manufacturers generally advertise the unformatted capacity — for example, a disk advertised as being 500GB will only hold 465.7GB of user data, and the remaining 34.3GB is used for *metadata*.

A cylinder is the set of identical tracks on both surfaces of each drive plat- ter. The location of drive heads is referred to by cylinder number, not by track number.

Zoned Bit Recording

- Because the platters are made of concentric tracks, the outer tracks can hold more data than the inner tracks, because the outer tracks are physically longer than the inner tracks, as shown in Figure 2-6 (a).
- On older disk drives, the outer tracks had the same number of sectors as the inner tracks, so data density was low on the outer tracks. This was an inefficient use of available space.
  Zone bit recording utilizes the disk efficiently.
  As shown in Figure 2-6 (b), this mechanism groups tracks into zones based on their distance from the center of the disk. The zones are numbered, with the outermost zone being zone 0.

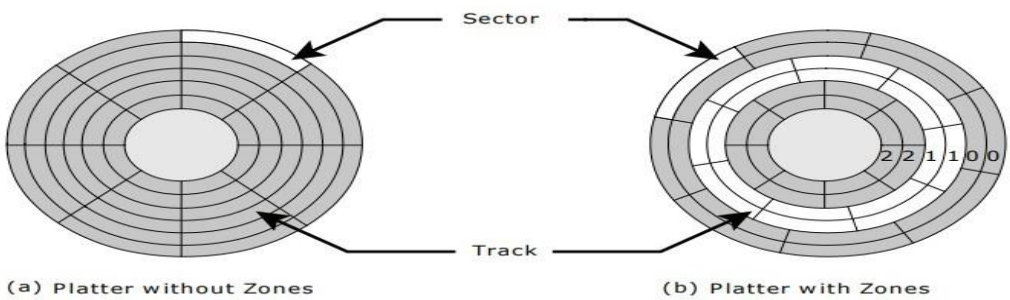


Figure 2-6: Zoned bit recording

➔ LOGICAL BLOCK ADDRESSING

Earlier drives used physical addresses consisting of the *cylinder, head, and sector (CHS)* number to refer to specific locations on the disk, as shown in Figure 2-7 (a), and the host operating system had to be aware of the geometry of each disk being used. *Logical block addressing (LBA)*, shown in Figure 2-7 (b), simplifies addressing by using a linear address to access physical blocks of data.

The disk controller translates LBA to a CHS address, and the host only needs to know the size of the disk drive in terms of the number of blocks. The logical

blocks are mapped to physical sectors on a 1:1 basis.

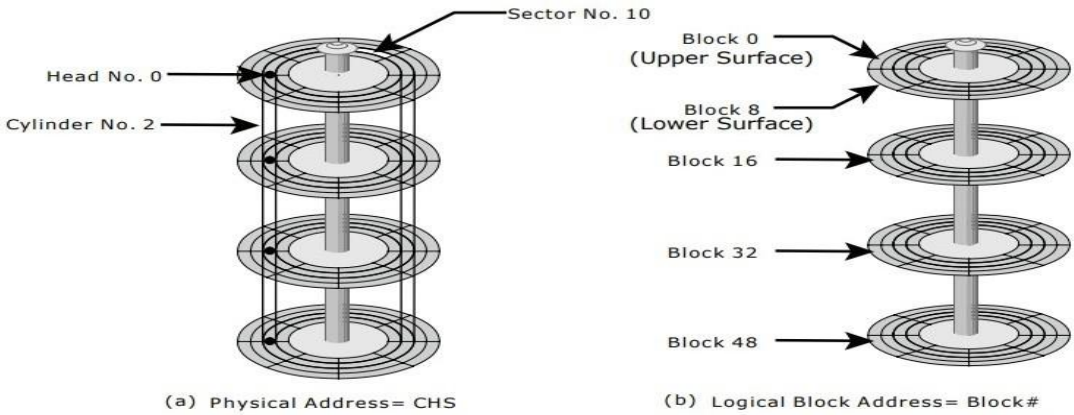


Figure 2-7: Physical address and logical block address

In Figure 2-7 (b), the drive shows eight sectors per track, eight heads, and four cylinders. This means a total of 8 × 8 × 4 = 256 blocks, so the block number ranges from 0 to 255. Each block has its own unique address. Assuming that the sector holds 512 bytes, a 500 GB drive with a formatted capacity of 465.7 GB will have in excess of 976,000,000 blocks.

➔ DISK DRIVE PERFORMANCE

A disk drive is an electromechanical device that governs the overall performance of the storage system environment. The various factors that affect the performance of disk drives are discussed in this section.

Disk Service Time

Disk service time is the time taken by a disk to complete an I/O request. Components that contribute to service time on a disk drive are *seek time*, *rota- tional 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).

In other words, it is the time taken to reposition and settle the arm and the head over the correct track. The lower the seek time, the faster the I/O operation.

Disk vendors publish the following seek time specifications:

- **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 specifications is measured in milliseconds. The average seek time on a modern disk is typically in the range of 3 to 15 milliseconds. Seek time has more impact on the read operation of random tracks rather than adjacent tracks.

To minimize the seek time, data can be written to only a subset of the available cylinders. This results in lower usable capacity than the actual capacity of the drive. For example, a 500 GB disk drive is set up to use only the first 40 percent of the cylinders and is effectively treated as a 200 GB drive. This is known as *short-stroking* the drive.

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.

Average rotational latency is around 5.5 ms for a 5,400-rpm drive, and around 2.0 ms for a 15,000-rpm drive.

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.

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

In a *write operation*, the data moves from the HBA to the internal buffer of the disk drive through the drive's interface. The data then moves from the buffer to the R/W heads. Finally, it moves from the R/W heads to the platters.

The data transfer rates during the R/W operations are measured in terms of internal and external transfer rates, as shown in Figure 2-8.

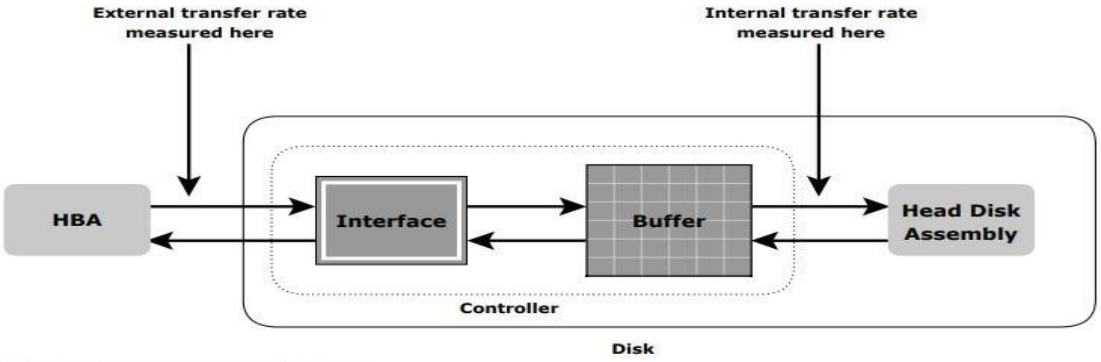


Figure 2-8: Data transfer rate

Internal transfer rate is the speed at which data moves from a single track of a platter's surface to internal buffer (cache) of the disk. Internal transfer rate takes into account factors such as the seek time.

External transfer rate is the rate at which data can be moved through the interface to the HBA. External transfer rate is generally the advertised speed of the interface, such as 133 MB/s for ATA. The sustained external transfer rate is lower than the interface speed.

➔ RAID (Redundant array of Independent Disks)

RAID is a way of storing the same data in different places on multiple hard disks or solid-state drives (SSDs) to protect data in the case of a drive failure.

There are two types of RAID implementation, hardware and software.

Software RAID

Software RAID uses host-based software to provide RAID functions.

It is implemented at the operating-system level and does not use a dedicated hardware controller to manage the RAID array.

Software RAID implementations offer cost and simplicity benefits when com- pared with hardware RAID. However, they have the following limitations:

- **Performance:** Software RAID affects overall system performance. This is due to the additional CPU cycles required to perform RAID calculations.
- **Supported features:** Software RAID does not support all RAID levels.
- **Operating system compatibility:** Software RAID is tied to the host operat- ing system hence upgrades to software RAID or to the operating system should be validated for compatibility. This leads to inflexibility in the data processing environment.

Hardware RAID

In *hardware RAID* implementations, a specialized hardware controller is imple- mented either on the host or on the array. These implementations vary in the way the storage array interacts with the host.

Controller card RAID is host-based hardware RAID implementation in which a specialized RAID controller is installed in the host and HDDs are connected to it.

The RAID Controller interacts with the hard disks using a PCI bus. Manufacturers also integrate RAID controllers on motherboards. This integra- tion reduces the overall cost of the system, but does not provide the flexibility required for high-end storage systems.

The external RAID controller is an array-based hardware RAID. It acts as an interface between the host and disks. It presents storage volumes to the host, which manage the drives using the supported protocol. Key functions of RAID controllers are:

- Management and control of disk aggregations
- Translation of I/O requests between logical disks and physical disks
- Data regeneration in the event of disk failures

R RAID Array Components

RAID array is an enclosure that contains a number of HDDs and the supporting hardware and software to implement RAID. HDDs inside a RAID array are usually contained in smaller sub-enclosures.

These sub-enclosures, or *physical arrays*, hold a fixed number of HDDs, and may also include other supporting hardware, such as power supplies. A subset of disks within a RAID array can be grouped to form logical associations called *logical arrays*, also known as a *RAID set* or a *RAID group* (see Figure 3-1).

Logical arrays are comprised of logical volumes (LV). The operating system recognizes the LVs as if they are physical HDDs managed by the RAID controller.

The number of HDDs in a logical array depends on the RAID level used. Configurations could have a logical array with multiple physical arrays or a physical array with multiple logical arrays.

RAID LEVELS

RAID levels (see Table 3-1) are defined on the basis of striping, mirroring, and parity techniques. These techniques determine the data availability and per- formance characteristics of an array. Some RAID arrays use one technique, whereas others use a combination of techniques. Application performance and data availability requirements determine the RAID level selection.

Striping

A RAID set is a group of disks. Within each disk, a predefined number of contiguously addressable disk blocks are defined as *strips*. The set of aligned strips that spans across all the disks within the RAID set is called a *stripe*. Figure 3-2 shows physical and logical representations of a striped RAID set.

Strip size (also called *stripe depth*) describes the number of blocks in a *strip*, and is the maximum amount of data that can be written to or read from a single HDD in the set before the next HDD is accessed, assuming that the accessed data starts at the beginning of the strip.

Note that all strips in a stripe have the same number of blocks, and decreasing strip size means that data is broken into smaller pieces when spread across the disks.

Stripe size is a multiple of strip size by the number of HDDs in the RAID set.
Stripe width refers to the number of data strips in a stripe.

Striped RAID does not protect data unless parity or mirroring is used. However, striping may significantly improve I/O performance. Depending on the type of RAID implementation, the RAID controller can be configured to access data across multiple HDDs simultaneously.

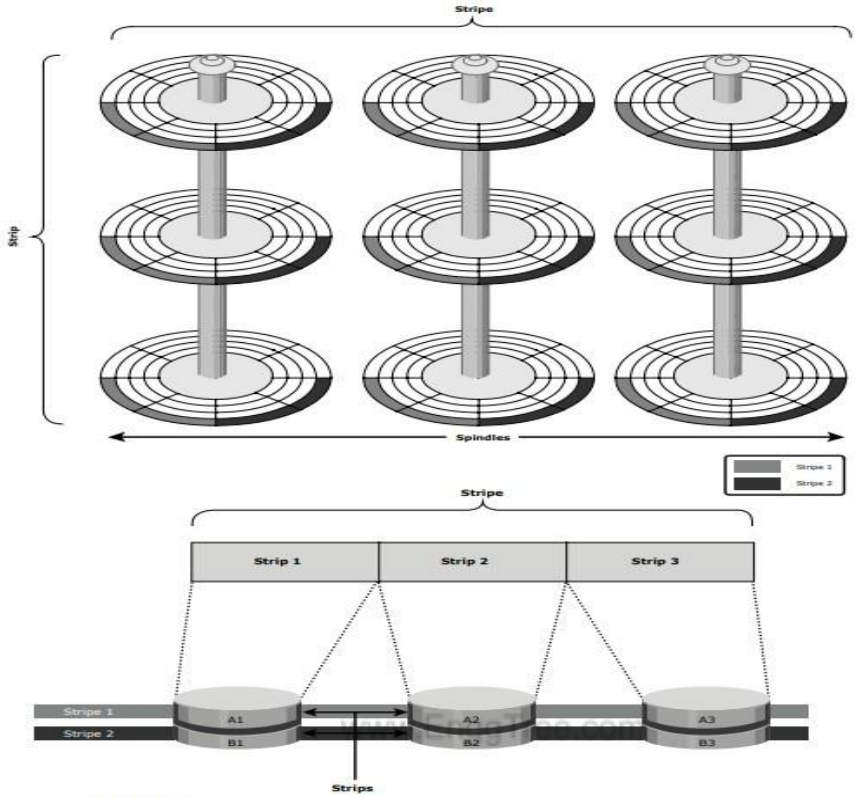


Figure 3-2: Striped RAID set

Mirroring

Mirroring is a technique whereby data is stored on two different HDDs, yield- ing two copies of data. In the event of one HDD failure, the data is intact on the surviving HDD (see Figure 3-3) and the controller continues to service the host's data requests from the surviving disk of a mirrored pair.

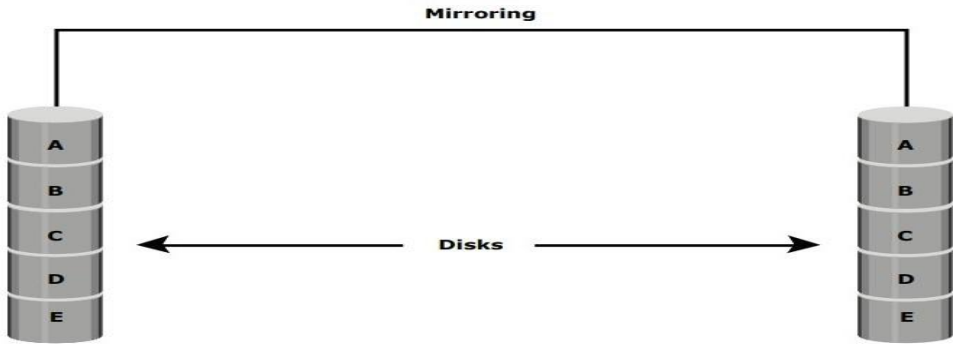


Figure 3-3: Mirrored disks in an array

When the failed disk is replaced with a new disk, the controller copies the data from the surviving disk of the mirrored pair. This activity is transparent to the host.

In addition to providing complete data redundancy, mirroring enables faster recovery

from disk failure. However, disk mirroring provides only data protection and is not a substitute for data backup. Mirroring constantly captures changes in the data, whereas a backup captures point-in-time images of data.

Mirroring involves duplication of data — the amount of storage capacity needed is twice the amount of data being stored. Therefore, mirroring is con- sidered expensive and is preferred for mission-critical applications that cannot afford data loss.

Mirroring improves read performance because read requests can be serviced by both disks. However, write performance deteriorates, as each write request manifests as two writes on the HDDs. In other words, mirroring does not deliver the same levels of write performance as a striped RAID.

Parity

Parity is a method of protecting striped data from HDD failure without the cost of mirroring. An additional HDD is added to the stripe width to hold parity, a mathematical construct that allows re-creation of the missing data.

Parity is a redundancy check that ensures full protection of data without maintaining a full set of duplicate data.

Parity information can be stored on separate, dedicated HDDs or distributed across all the drives in a RAID set. Figure 3-4 shows a parity RAID. The first four disks, labeled *D*, contain the data.

The fifth disk, labeled *P*, stores the parity information, which in this case is the sum of the elements in each row. Now, if one of the *D*s fails, the missing value can be calculated by subtracting the sum of the rest of the elements from the parity value.

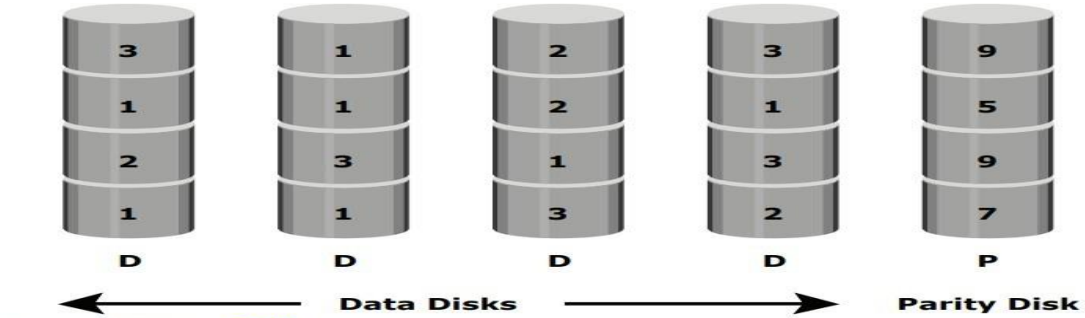


Figure 3-4: Parity RAID

In Figure 3-4, the computation of parity is represented as a simple arithmetic operation on the data. However, parity calculation is a *bitwise XOR* operation. Calculation of parity is a function of the RAID controller.

Compared to mirroring, parity implementation considerably reduces the cost associated with data protection. Consider a RAID configuration with five disks. Four of these disks hold data, and the fifth holds parity information. Parity requires 25 percent extra disk space compared to mirroring, which requires 100 percent extra disk space.

However, there are some disadvantages of using parity. Parity information is generated from data on the data disk. Therefore, parity is recalculated every time there is a

change in data. This recalculation is time-consuming and affects the performance of the RAID controller.

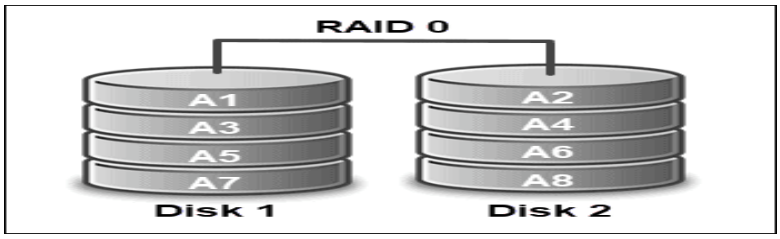
Table 3-1: Raid Levels

LEVELS	BRIEF DESCRIPTION
RAID 0	Striped array with no fault tolerance
RAID 1	Disk mirroring
RAID 3	Parallel access array with dedicated parity disk
RAID 4	Striped array with independent disks and a dedicated parity disk
RAID 5	Striped array with independent disks and distributed parity
RAID 6	Striped array with independent disks and dual distributed parity
Nested	Combinations of RAID levels. Example: RAID 1 + RAID 0

RAID 0: Striping

RAID 0, also known as a striped set or a striped volume, requires a minimum of two disks. The disks are merged into a single large volume where data is stored evenly across the number of disks in the array.

This process is called disk striping and involves splitting data into blocks and writing it simultaneously/sequentially on multiple disks. Configuring the striped disks as a single partition increases performance since multiple disks do reading and writing operations simultaneously. Therefore, RAID 0 is generally implemented to improve speed and efficiency.



It is important to note that if an array consists of disks of different sizes, each will be limited to the smallest disk size in the setup. This means that an array composed of two disks, where one is 320 GB, and the other is 120 GB, actually has the capacity of 2 x 120 GB (or 240 GB in total).

Certain implementations allow you to utilize the remaining 200 GB for different use. Additionally, developers can implement multiple controllers (or even one per disk) to improve performance.

RAID 0 is the most affordable type of redundant disk configuration and is relatively easy to set up. Still, it does not include any redundancy, fault tolerance, or party in its composition.

Hence, problems on any of the disks in the array can result in complete data loss. This is why it should only be used for non-critical storage, such as temporary files backed up somewhere else.

Advantages of RAID 0

- Cost-efficient and straightforward to implement.
- Increased read and write performance.
- No overhead (total capacity use).

Disadvantages of RAID 0

- Doesn't provide fault tolerance or redundancy.

When Raid 0 Should Be Used

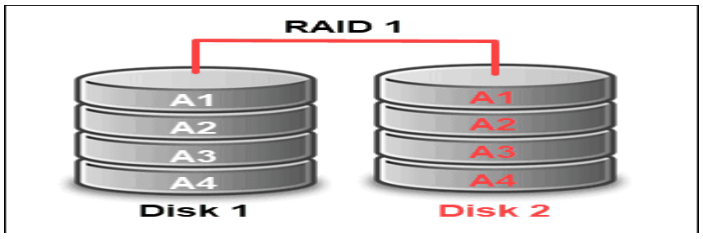
RAID 0 is used when performance is a priority and reliability is not. If you want to utilize your drives to the fullest and don't mind losing data, opt for RAID 0.

On the other hand, such a configuration does not necessarily have to be unreliable. You can set up disk striping on your system along with another RAID array that ensures data protection and redundancy.

RAID 1: Mirroring

RAID 1 is an array consisting of at least two disks where the same data is stored on each to ensure redundancy. The most common use of RAID 1 is setting up a mirrored pair consisting of two disks in which the contents of the first disk is mirrored in the second. This is why such a configuration is also called mirroring.

Unlike with RAID 0, where the focus is solely on speed and performance, the primary goal of RAID 1 is to provide redundancy. It eliminates the possibility of data loss and downtime by replacing a failed drive with its replica.



In such a setup, the array volume is as big as the smallest disk and operates as long as one drive is operational. Apart from reliability, mirroring enhances read performance as a request can be handled by any of the drives in the array. On the other hand, the write performance remains the same as with one disk and is equal to the slowest disk in the configuration.

Advantages of RAID 1

- Increased read performance.
- Provides redundancy and fault tolerance.

- Simple to configure and easy to use.

Disadvantages of RAID 1

- Uses only half of the storage capacity.
- More expensive (needs twice as many drivers).
- Requires powering down your computer to replace failed drive.

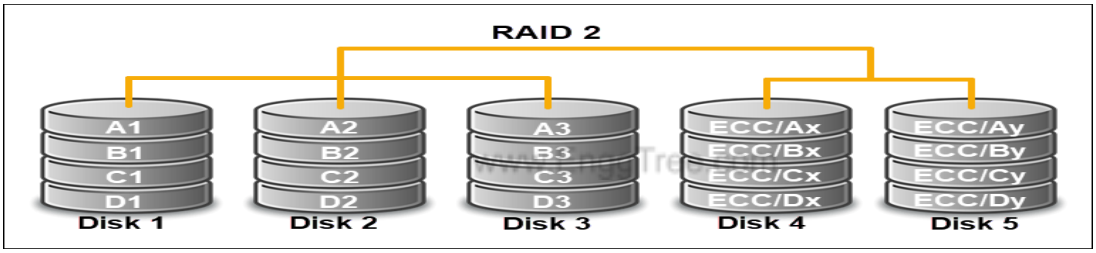
When Raid 1 Should Be Used

RAID 1 is used for mission-critical storage that requires a minimal risk of data loss. Accounting systems often opt for RAID 1 as they deal with critical data and require high reliability.
It is also suitable for smaller servers with only two disks, as well as if you are searching for a simple configuration you can easily set up (even at home).

Raid 2: Bit-Level Striping with Dedicated Hamming-Code Parity

RAID 2 is rarely used in practice today. It combines bit-level striping with error checking and information correction. This RAID implementation requires two groups of disks – one for writing the data and another for writing error correction codes. RAID 2 also requires a special controller for the synchronized spinning of all disks.

Instead of data blocks, RAID 2 stripes data at the bit level across multiple disks. Additionally, it uses the Humming error ode correction (ECC) and stores this information on the redundancy disk.



The array calculates the error code correction on the fly. While writing the data, it strips it to the data disk and writes the code to the redundancy disk. On the other hand, while reading data from the disk, it also reads from the redundancy disk to verify the data and make corrections if needed.

Advantages of RAID 2

- Reliability.
- The ability to correct stored information.

Disadvantages of RAID 2

- Expensive.
- Difficult to implement.
- Require entire disks for ECC.

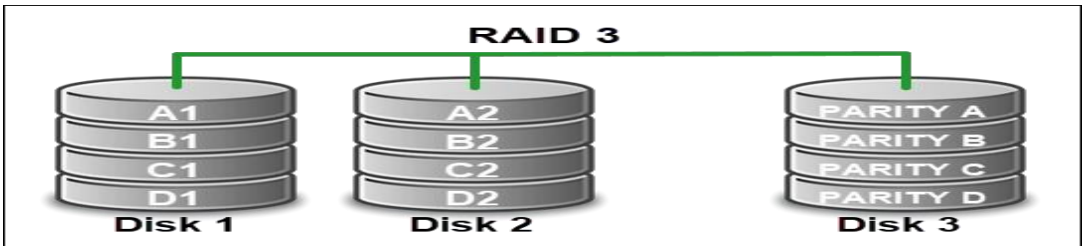
When Raid 2 Should Be Used

RAID 2 is not a common practice today as most of its features are now available on modern hard disks. Due to its cost and implementation requirements, this RAID level never became popular among developers.

Raid 3: Bit-Level Striping with Dedicated Parity

Like RAID 2, RAID 3 is rarely used in practice. This RAID implementation utilizes bit-level striping and a dedicated parity disk. Because of this, it requires at least three drives, where two are used for storing data strips, and one is used for parity.

To allow synchronized spinning, RAID 3 also needs a special controller. Due to its configuration and synchronized disk spinning, it achieves better performance rates with sequential operations than random read/write operations.



Advantages of RAID 3

- Good throughput when transferring large amounts of data.
- High efficiency with sequential operations.
- Disk failure resiliency.

Disadvantages of RAID 3

- Not suitable for transferring small files.
- Complex to implement.
- Difficult to set up as software RAID.

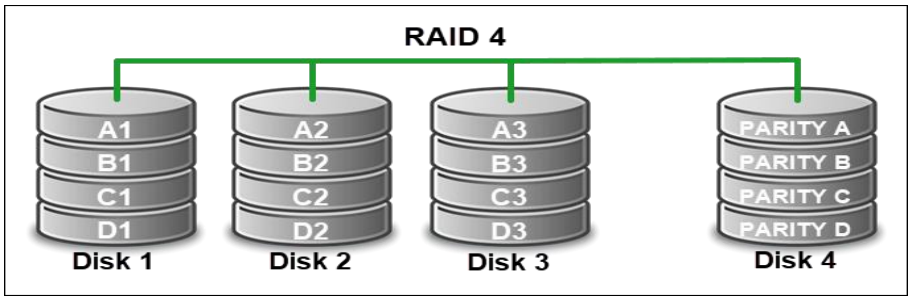
When Raid 3 Should Be Used

RAID 3 is not commonly used today. Its features are beneficial to a limited number of use cases requiring high transfer rates for long sequential reads and writes (such as video editing and production).

Raid 4: Block-Level Striping with Dedicated Parity

RAID 4 is another unpopular standard RAID level. It consists of block-level data striping across two or more independent diss and a dedicated parity disk.

The implementation requires at least three disks – two for storing data strips and one dedicated for storing parity and providing redundancy. As each disk is independent and there is no synchronized spinning, there is no need for a controller.



RAID 4 configuration is prone to bottlenecks when storing parity bits for each data block on a single drive. Such system bottlenecks have a large impact on system performance.

Advantages of RAID 4

- Fast read operations.
- Low storage overhead.
- Simultaneous I/O requests.

Disadvantages of RAID 4

- Bottlenecks that have big effect on overall performance.
- Slow write operations.
- Redundancy is lost if the parity disk fails.

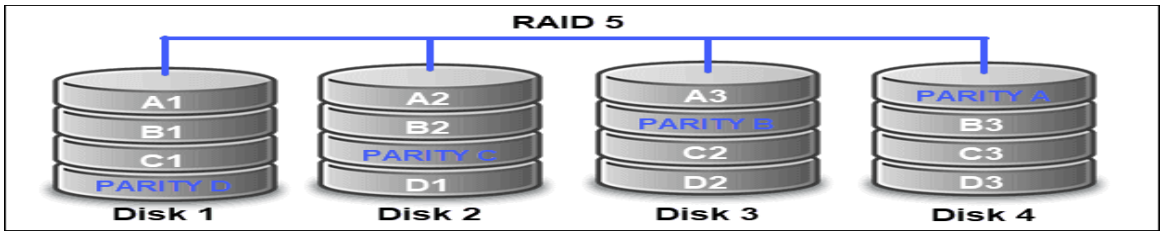
When Raid 4 Should Be Used

Considering its configuration, RAID 4 works best with use cases requiring sequential reading and writing data processes of huge files. Still, just like with RAID 3, in most solutions, RAID 4 has been replaced with RAID 5.

Raid 5: Striping with Parity

RAID 5 is considered the most secure and most common RAID implementation. It combines striping and parity to provide a fast and reliable setup. Such a configuration gives the user storage usability as with RAID 1 and the performance efficiency of RAID 0.

This RAID level consists of at least three hard drives (and at most, 16). Data is divided into data strips and distributed across different disks in the array. This allows for high performance rates due to fast read data transactions which can be done simultaneously by different drives in the array.



Parity bits are distributed evenly on all disks after each sequence of data has been saved. This feature ensures that you still have access to the data from parity bits in case of a failed drive. Therefore, RAID 5 provides redundancy through parity bits instead of mirroring.

Advantages of RAID 5

- High performance and capacity.
- Fast and reliable read speed.
- Tolerates single drive failure.

Disadvantages of RAID 5

- Longer rebuild time.
- Uses half of the storage capacity (due to parity).
- If more than one disk fails, data is lost.
- More complex to implement.

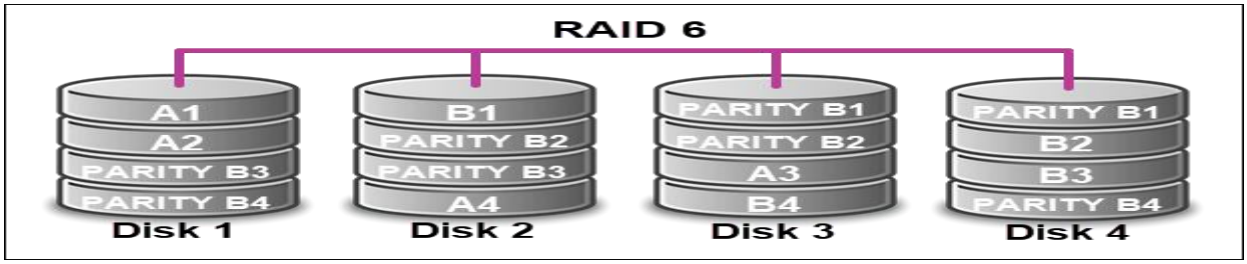
When Raid 5 Should Be Used

RAID 5 is often used for file and application servers because of its high efficiency and optimized storage. Additionally, it is the best, cost-effective solution if continuous data access is a priority and/or you require installing an operating system on the array.

Raid 6: Striping with Double Parity

RAID 6 is an array similar to RAID 5 with an addition of its double parity feature. For this reason, it is also referred to as the double-parity RAID.

This setup requires a minimum of four drives. The setup resembles RAID 5 but includes two additional parity blocks distributed across the disk. Therefore, it uses block-level striping to distribute the data across the array and stores two parity blocks for each data block.



Block-level striping with two parity blocks allows two disk failures before any data is lost. This means that in an event where two disks fail, RAID can still reconstruct the required data.

Its performance depends on how the array is implemented, as well as the total number of drives. Write operations are slower compared to other configurations due to its double parity feature.

Advantages of RAID 6

- High fault and drive-failure tolerance.
- Storage efficiency (when more than four drives are used).
- Fast read operations.

Disadvantages of RAID 6

- Rebuild time can take up to 24 hours.
- Slow write performance.
- Complex to implement.
- More expensive.

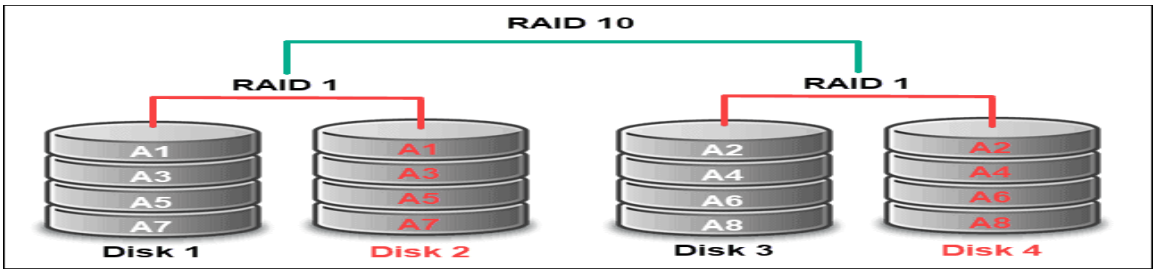
When Raid 6 Should Be Used

RAID 6 is a good solution for mission-critical applications where data loss cannot be tolerated. Therefore, it is often used for data management in defense sectors, healthcare, and banking.

Raid 10: *Mirroring with Striping*

RAID 10 is part of a group called nested or hybrid RAID, which means it is a combination of two different RAID levels. In the case of RAID 10, the array combines level 1 mirroring and level 0 striping. This RAID array is also known as RAID 1+0.

RAID 10 uses logical mirroring to write the same data on two or more drives to provide redundancy. If one disk fails, there is a mirrored image of the data stored on another disk. Additionally, the array uses block-level striping to distribute chunks of data across different drives. This improves performance and read and write speed as the data is simultaneously accessed from multiple disks.



To implement such a configuration, the array requires at least four drives, as well as a disk controller.

Advantages of RAID 10

- High performance.
- High fault-tolerance.
- Fast read and write operations.
- Fast rebuild time.

Disadvantages of RAID 10

- Limited scalability.
- Costly (compared to other RAID levels).
- Uses half of the disk space capacity.
- More complicated to set up.

When Raid 10 Should Be Used

RAID 10 is often used in use cases that require storing high volumes of data, fast read and write times, and high fault tolerance. Accordingly, this RAID level is often implemented for email servers, web hosting servers, and databases.

➔ TYPES OF INTELLIGENT STORAGE SYSTEMS

Intelligent storage systems generally fall into one of the following two categories:

- *High-end storage systems*
- *Midrange storage systems*

Traditionally, high-end storage systems have been implemented with *active-active arrays*, whereas midrange *storage systems* used typically in small- and medium- sized enterprises have been implemented with *active-passive arrays*.

Active-passive arrays provide optimal storage solutions at lower costs. Enterprises make use of this cost advantage and implement active-passive arrays to meet specific application requirements such as performance, availability, and scalability. The distinctions between these two implementations are becoming increasingly insignificant.

High-end Storage Systems

High-end storage systems, referred to as *active-active arrays*, are generally aimed at

large enterprises for centralizing corporate data. These arrays are designed with a large number of controllers and cache memory.

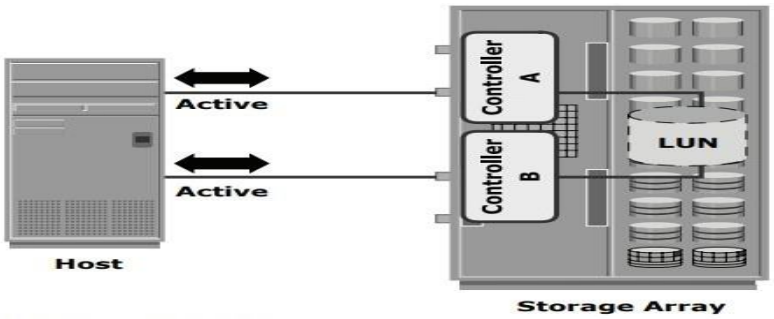


Figure 4-7: Active-active configuration

An active-active array implies that the host can perform I/Os to its LUNs across any of the available paths (see Figure 4-7).

To address the enterprise storage needs, these arrays provide the following capabilities:

- Large storage capacity
- Large amounts of cache to service host I/Os optimally
- Fault tolerance architecture to improve data availability
- Connectivity to mainframe computers and open systems hosts
- Availability of multiple front-end ports and interface protocols to serve a large number of hosts
- Availability of multiple back-end Fibre Channel or SCSI RAID controllers to manage disk processing
- Scalability to support increased connectivity, performance, and storage capacity requirements
- Ability to handle large amounts of concurrent I/Os from a number of servers and applications
- Support for array-based local and remote replication

In addition to these features, high-end arrays possess some unique features and functionals that are required for mission-critical applications in large enterprises.

Midrange Storage System

Midrange storage systems are also referred to as *active-passive arrays* and they are best suited for small- and medium-sized enterprises. In an active-passive array, a host can perform I/Os to a LUN only through the paths to the owning controller of that LUN. These paths are called *active paths*.

The other paths are passive with respect to this LUN. As shown in Figure 4-8, the host can perform reads or writes to the LUN only through the path to controller A, as controller A is the owner of that LUN. The path to controller B remains passive and no I/O activity is performed through this path.

Midrange storage systems are typically designed with two controllers, each of which

contains host interfaces, cache, RAID controllers, and disk drive interfaces.

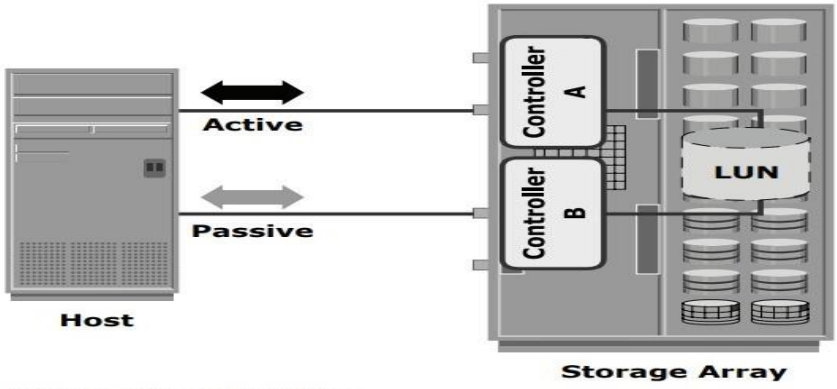


Figure 4-8: Active-passive configuration

Midrange arrays are designed to meet the requirements of small and medium enterprises; therefore, they host less storage capacity and global cache than active-active arrays.

There are also fewer front-end ports for connection to serv- ers. However, they ensure high redundancy and high performance for applications with predictable workloads. They also support array-based local and remote replication.

➔ SCALE-UP AND SCALE OUT STORAGE ARCHITECTURE

- Scaling up and scaling out are the two main methods used to increase data storage capacity.
- Scale-out and scale-up architectures—also known, respectively, as *horizontal scaling* and *vertical scaling* and scale *in* and scale *down*—refer to how companies scale their data storage: by adding more hardware *drives* (scale up/vertical scaling), or by adding more software *nodes* (scale out/horizontal scaling).
- Scale-up is the more traditional format, but it runs into space issues as data volumes grow and the need for more and more data storage increases. Hence, the advent of scale-*out* architectures.
- This is a very high-level description of the two main methods of scaling data storage capacity, so let's delve into it a little deeper.

Scale-up Architecture

In a scale-up data storage architecture, storage drives are added to increase storage capacity and performance. The drives are managed by two *controllers*. When you run out of storage capacity, you add another shelf of drives to the architecture.

Scale-up storage and applications

Organizations may need to add capacity to existing storage devices. This could be due to rapid expansion or complexity of one or more applications running on a storage device.

In this type of situation, organizations can increase storage of the specific device. This is referred to as scaling up, as the primary equipment does not change; it only increases its storage capacity.

In a scale-up approach, organizations add to existing infrastructure, such as with more disks or drives. If it is important to retain the same device rather than splitting up critical applications and data

across multiple storage devices, use a scale-up approach to scale storage. This is also known as *vertical scaling*.

IT management may determine that an existing storage device will need to increase its capacity due to expansion of key applications that use the storage component. Organizations can then configure additional servers and link them to the main system.

Advantages of Scale-up Architecture

Scaling up offers certain advantages, including:

- **Affordability:** Because there's only one large server to manage, scaling up is a cost-effective way to increase storage capacity since you'll end up paying less for your network equipment and licensing. Upgrading a pre-existing server costs less than purchasing a new one. Vertical scaling also tends to require less new backup and virtualization software.
- **Maintenance:** Since you have only one storage system to manage versus a whole cluster of different elements, scale-up architectures are easier to manage and also make it easier to address specific data quality issues.
- **Simpler communication:** Since vertical scaling means having just a single node handling all the layers of your services, you don't need to worry about your system synchronizing and communicating with other machines to work, which can lead to faster response times.

Disadvantages of Scale-up Architecture

The disadvantages of scale-up architectures include:

- **Scalability limitations:** Although scaling up is how enterprises have traditionally handled storage upgrades, this approach has slowly lost its effectiveness. The RAM, CPU, and hard drives added to a server can only perform to the level the computing housing unit allows. As a result, performance and capacity become a problem as the unit nears its physical limitations. This, in turn, impacts backup and recovery times and other mission-critical processes.
- **Upgrade headaches and downtime:** Upgrading a scale-up architecture can be extremely tedious and involve a lot of heavy lifting. Typically, you need to copy every piece of data from the old server over to a new machine, which can be costly in terms of both money and downtime. Also, adding another server to the mix usually means adding another data store, which could result in the network getting bogged down by storage pools and users not knowing where to look for files. Both of these can negatively impact productivity. Also, with a scale-up architecture, you need to take your

existing server offline while replacing it with a new, more powerful one. During this time, your apps will be unavailable.

Scale-out Architecture

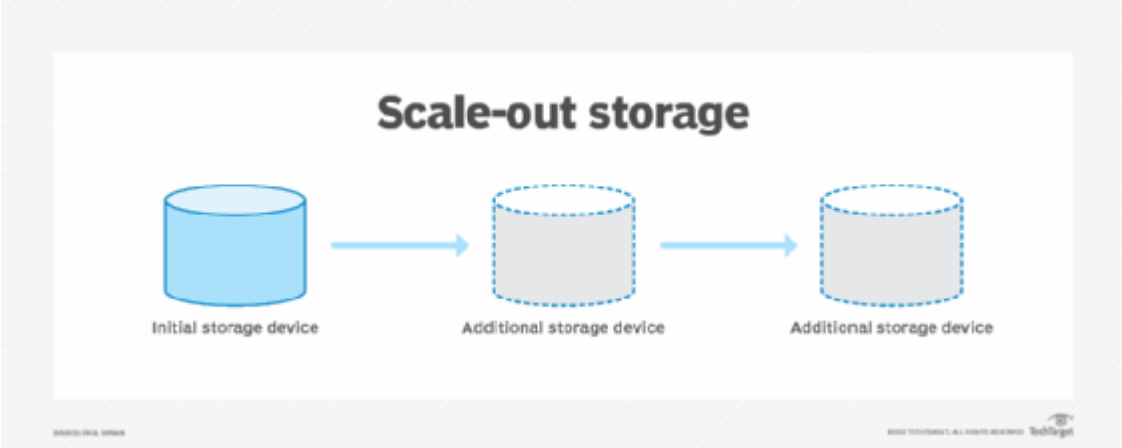
A scale-out architecture uses software-defined storage (SDS) to separate the storage hardware from the storage software, letting the software act as the controllers. This is why scale-out storage is considered to be *network attached storage* (NAS).

Scale-out NAS systems involve clusters of software nodes that work together. Nodes can be added or removed, allowing things like bandwidth, compute, and throughput to increase or decrease as needed. To upgrade a scale-out system, new clusters must be created.

Scale-out storage and applications

For long-term upgrades, management may determine that they need more storage and the unique requirements will need specialized storage devices, such as SSDs and additional HDDs. In practice, it may be necessary to add more equipment racks close to the original storage equipment.

In such situations, it makes more sense to boost storage by configuring a variety of devices that support those requirements. This is referred to as scaling out from the initial storage equipment, or what is also known as *horizontal scaling*.



Distributed file systems can be an important part of a scale-out arrangement, as they use multiple devices in a cohesive storage environment.

Advantages of Scale-out Architecture

The advantages of scale-out architecture include:

- **Better performance:** Horizontal scaling allows for more connection endpoints since the load will be shared by multiple machines, and this improves performance.
- **Easier scaling:** Horizontal scaling is much easier from a hardware perspective because all you need to do is add machines.

- **Less downtime and easier upgrades:** Scaling out means less downtime because you don't have to switch anything off to scale or make upgrades. Scaling out essentially allows you to upgrade or downgrade your hardware whenever you want as you can move all users, workloads, and data without any downtime. Scale-out systems can also auto-tune and self-heal, allowing clusters to easily accommodate all data demands.

Disadvantages of Scale-out Architecture

The disadvantages of horizontal scaling include:

- **Complexity:** It's always going to be harder to maintain multiple servers compared to a single server. Also, things like load balancing and virtualization may require adding software, and machine backups can also be more complex because you'll need to ensure nodes synchronize and communicate effectively.
- **Cost:** Scaling out can be more expensive than scaling up because adding new servers is far more expensive than upgrading old ones.

Scale up or scale out? How to decide

So, should you scale up or scale out your infrastructure? The decision tree below will help you more clearly answer this question.

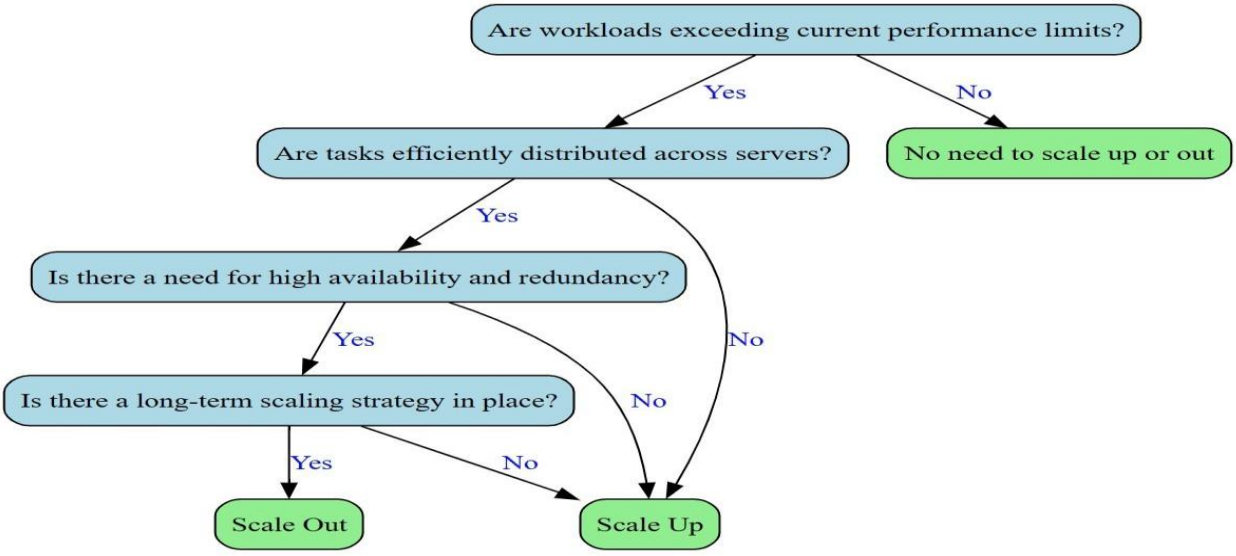


Figure A - Decision tree directing whether to scale up or scale out.

Bottom line: Scale up and scale out

Deciding between scaling up and scaling out largely depends on your organization's specific needs and circumstances. Vertical scaling is ideal for situations where a single system can meet the demand, like with high-performance databases.

However, this approach has its limits in terms of hardware capabilities and could lead to higher costs over time.

Conversely, horizontal scaling works best when the workload can be distributed efficiently across multiple servers. This is often preferred for handling web traffic surges or managing user-generated data on platforms like social media sites. Yet, this method can introduce complexities related to managing the distributed system.

In practice, many organizations use a hybrid approach, maximizing each server's power through scaling up, then expanding capacity through scaling out.

Ultimately, the choice between the two strategies should take into account your application's requirements, growth projections and budget. Remember, the goal is to align your scaling strategy with your business objectives for optimal performance.

One great option for scaling your storage is network-attached storage (NAS)

UNIT III

STORAGE NETWORKING TECHNOLOGIES AND VIRTUALIZATION

Block-Based Storage System, File-Based Storage System, Object-Based and Unified Storage. Fibre Channel SAN: Software-defined networking, FC SAN components and architecture, FC SAN topologies, link aggregation, and zoning, Virtualization in FC SAN environment. Internet Protocol SAN: iSCSI protocol, network components, and connectivity, Link aggregation, switch aggregation, and VLAN, FCIP protocol, 140 connectivity, and configuration. Fibre Channel over Ethernet SAN: Components of FCoE SAN, FCoE SAN connectivity, Converged Enhanced Ethernet, FCoE architecture.

➔ BLOCK-BASED STORAGE SYSTEM

- ***Block storage is for flexible, fast access***
- ***Block storage*** is a form of ***cloud storage*** that is used to store data, often on storage area networks (SANs).
- Data is stored in blocks, with each block stored separately based on the efficiency needs of the SAN.
- Each block is assigned a unique address, which is then used by a management application controlled by the server's operating system to retrieve and compile data into files upon request.
- Block storage offers efficiency due to the way blocks can be distributed across multiple systems and even configured to work with different operating systems.
- Block storage also offers an impressive level of flexibility because it can be accessed by different operating systems as mounted drive volumes and has the ability to use operating system–specific file systems (such as the New Technology File System (NTFS) for Windows and Virtual Machine File System (VMFS) for VMware).
- This makes using block storage quite similar to storing data on a hard drive within a server, except the data is stored in a remote location rather than on local hardware.

How block storage works?

- A block is a fixed-size amount of memory within storage media that's capable of storing a piece of data. The size of each block is determined by the management system.
- The block size is generally too small to fit an entire piece of data, and so the data for any particular file is broken up into numerous blocks for storage.
- Each block is given a unique identifier without any higher-level metadata; details such as data format, type, and ownership are not noted.
- The operating system allocates and distributes blocks across the storage network to balance efficiency and functionality.
- When a file is requested, the management application uses addresses to identify the necessary blocks and then compiles them into the complete file for use.

- By enabling storage across multiple environments, block storage separates data from the limitations of individual user environments. As a result, data can be retrieved through any number of paths to maximize efficiency, with high input/output operations per second (IOPS).
- The result is an approach that offers a higher level of efficiency than other cloud storage methods, making it ideal for high-performance applications or applications that require constant writing and retrieval.

Benefits of block storage

Block storage is a common and popular cloud storage choice because of its numerous benefits.

High efficiency: Block storage's high IOPS and low latency make it ideal for applications that demand high performance.

Compatibility: Block storage works across different operating systems and file systems, making it compatible for enterprises whatever their configuration and environment.

Flexibility: With block storage, horizontal scaling is extremely flexible. Cluster nodes can be added as needed, allowing for greater overall storage capability.

Large file efficiency: For large files, such as archives and video files, data must be completely overwritten when using file or object storage. With block storage, the management application identifies only the block targeted for change within the large file, increasing the efficiency of data updates.

Limitations of block storage

Like any technology platform, block storage comes with limitations despite its numerous benefits.

Greater cost: While block storage is easily scalable, it can also be expensive due to the cost of SANs. In addition, managing block storage requires more-specialized training for management and maintenance, increasing the overall expense.

Performance limitations: With block storage, metadata is built in and hierarchical, and it is defined by the file system. Because data is broken up into blocks, searching for a complete file requires the proper identification of all its pieces. This can create performance issues for operations accessing the metadata, particularly with folders featuring a large number of files. While the tipping point is usually about 10,000 files, some issues are seen with directories containing only 1,000 files.

Block storage use cases

As with object storage and other types of cloud storage, block storage works best in specific circumstances based on user needs and given parameters.

The following are just several of many effective block storage use cases:

Containers: Block storage supports the use of container platforms such as Kubernetes, creating a block volume that enables persistent storage for the entire container. This allows for the clean management and migration of containers as needed.

Email servers: Email servers can take advantage of block storage's flexibility and scalability. In fact, in the case of Microsoft Exchange, block storage is required due to the lack of support for network-attached storage.

Databases: Block storage is fast, efficient, flexible, and scalable, with support for redundant volumes. This allows it to support databases, particularly those that handle a heavy volume of queries and where latency must be minimized.
Disaster recovery: Block storage can be a redundant backup solution for nearline storage and quick restoration, with data swiftly moved from backup to production through easy access.

Need for *block storage :*

- Block storage continues to be an efficient and flexible cloud storage option for enterprises require high-performance workloads or need to manage large files. Learn more about how Oracle delivers block storage solutions with Oracle Cloud Infrastructure.

➔ FILE-BASED STORAGE SYSTEM

- File storage—also called file-level or file-based storage—is a hierarchical storage methodology used to organize and store data on a computer hard drive or on network-attached storage (NAS) device.
- In file storage, data is stored in files, the files are organized in folders, and the folders are organized under a hierarchy of directories and subdirectories.
- To locate a file, all you or your computer system need is the path—from directory to subdirectory to folder to file.
- Hierarchical file storage works well with easily organized amounts of structured data. But, as the number of files grows, the file retrieval process can become cumbersome and time-consuming. Scaling requires adding more hardware devices or continually replacing these with higher-capacity devices, both of which can get expensive.
- To some extent, you can mitigate these scaling and performance issues with cloud-based file storage services. These services allow multiple users to access and share the same file data located in off-site data centers (the cloud).
- You simply pay a monthly subscription fee to store your file data in the cloud, and you can easily scale-up capacity and specify your data performance and protection criteria. Moreover, you eliminate the expense of maintaining your own on-site hardware since this infrastructure is managed and maintained by the cloud service provider (CSP) in its data center.
- This is also known as Infrastructure-as-a-Service (IaaS).

File storage benefits

If your organization requires a centralized, easily accessible, and affordable way to store files and folders, file-level storage is a good approach. The benefits of file storage include the following:
Simplicity: File storage is the simplest, most familiar, and most straightforward approach to organizing files and folder on a computer's hard drive or NAS device. You simply name files, tag them with metadata, and store them in folders under a hierarchy of directories and subdirectories. It is not necessary to write applications or code to access your data.

File sharing: File storage is ideal for centralizing and sharing files on a Local Area Network (LAN). Files stored on a NAS device are easily accessible by any computer on the network that has the appropriate permission rights.

Common protocols: File storage uses common file-level protocols such as Server Message Block (SMB), Common Internet File System (CIFS), or Network File System (NFS). If you utilize a Windows or Linux operating system (or both), standard protocols like SMB/CIFS and NFS will allow you to read and write files to a Windows-based or Linux-based server over your Local Area Network (LAN).

Data protection: Storing files on a separate, LAN-connected storage device offers you a level of data protection should your network computer experience a failure. Cloud-based file storage services provide additional data protection and disaster recovery by replicating data files across multiple, geographically-dispersed data centers.

Affordability: File storage using a NAS device allows you to move files off of expensive computing hardware and onto a more affordable LAN-connected storage device. Moreover, if you choose to subscribe to a cloud file-storage service, you eliminate the expense of on-site hardware upgrades and the associated ongoing maintenance and operation costs.

File storage use cases

File storage is a good solution for a wide variety of data needs, including the following:

Local file sharing: If your data storage needs are generally consistent and straightforward, such as storing and sharing files with team members in the office, consider the simplicity of file-level storage.

Centralized file collaboration: If you upload, store, and share files in a centralized library—located on-site, off-site, or in the cloud—you can easily collaborate on files with internal and external users or with invited guests outside of your network.

Archiving/storage: You can cost-effectively archive files on NAS devices in a small data center environment or subscribe to a cloud-based file storage service to store and archive yourdata.

Backup/disaster recovery: You can store backups securely on separate, LAN-connected storage devices. Or you can subscribe to a cloud-based file storage service to replicate your data files across multiple, geographically-dispersed data centers and gain the additional data protection of distance and redundancy.

➔ OBJECT-BASED STORAGE SYSTEM

- Object storage, also known as object-based storage, is a computer data storage architecture designed to handle large amounts of unstructured data.
- Unlike other architectures, it designates data as distinct units, bundled with metadata and a unique identifier that can be used to locate and access each data unit.
- These units—or objects—can be stored on-premises, but are typically stored in the cloud, making them easily accessible from anywhere.
- Due to object storage's scale-out capabilities, there are few limits to its scalability, and it's less costly to store large data volumes than other options, such as block storage.

- Much of today's data is unstructured: email, media and audio files, web pages, sensor data, and other types of digital content that do not fit easily into traditional databases. As a result, finding efficient and affordable ways to store and manage it has become problematic.
- Increasingly, object storage has become the preferred method for storing static content, data arches, and backups.

Definition of Object storage

- Object storage is a data storage architecture for storing unstructured data, which sections data into units—objects—and stores them in a structurally flat data environment.
- Each object includes the data, metadata, and a unique identifier that applications can use for easy access and retrieval.

How does object storage work?

- With object storage, the data blocks of a file are kept together as an object, together with its relevant metadata and a custom identifier, and placed in a flat data environment known as a storage pool.
- When you want to access data, object storage systems will use the unique identifier and the metadata to find the object you need, such as an image or audio file.
- You can also customize metadata, allowing you to add more context that is useful for other purposes, such as retrieval for data analytics.
- You can locate and access objects using RESTful APIs, HTTP, and HTTPS to query object metadata. Since objects are stored in a global storage pool, it's fast and easy to locate the exact data you need. Plus, the flat environment enables you to scale quickly, even for petabyte or exabyte loads.
- Storage pools can be spread across multiple object storage devices and geographical locations, allowing for unlimited scale. You simply add more storage devices to the pool as your data grows.
- The benefits of object storage, like its elasticity and scalability, have made it an ideal fit for managing unstructured data in cloud infrastructure. So, what is object storage in the cloud? It's exactly what it sounds like—object-based storage as an on-demand cloud service.
- In fact, cloud object storage is the primary storage format for most major cloud service providers.

Benefits of object storage:

Massive scalability

You can easily scale out the flat architecture of object storage without suffering from the same limitations as file or block storage. Object storage size is essentially limitless, so data can scale to exabytes by simply adding new devices.

Reduced complexity

Object storage has no folders or directories, removing much of the complexity that comes with hierarchical systems. The lack of complex trees or partitions makes retrieving files easier as you don't need to know the exact location.

Searchability

Metadata is part of objects, making it easy to search through and navigate without the need of a separate application. It's also far more flexible and customizable. You can tag objects with attributes and information, such as consumption, cost, and policies for automated deletion, retention, and tiering.

Resiliency

Object storage can automatically replicate data and store it across multiple devices and geographical locations. This can help protect against outages, safeguard against data loss, and help support disaster recovery strategies.

Cost efficiency

Object storage was created with cost in mind, providing storage for large amounts of data at a lower price than file- and block-based systems. With object storage, you only pay for the capacity you need, allowing you to control costs even for large amounts of data.

➔ UNIFIED STORAGE :

- Also known as multiprotocol storage, unified storage allows multiple types of data to be stored in the same device.
- It combines block and file storage protocols, such as iSCSI, NFS, and SMB, into a single platform, making it easier for IT administrators to manage and maintain their storage infrastructure because they have it all in one place.
- With unified storage, users can access their data from different applications and platforms via a single interface, which helps streamline workflows and reduce storage complexity.

Unified Storage Architecture

- A unified storage architecture is the design and framework that underpins the functionality of unified storage systems.
- It uses a single storage pool to store data, which can be allocated dynamically to different storage tiers based on the data's usage.
- The architecture also includes features like data deduplication, compression, and encryption, which further enhance the efficiency and security of the storage system.

How a Unified Storage Architecture Works

- A unified storage architecture works by consolidating different types of storage into a single system. It provides a single point of management for all storage-related tasks, including provisioning, allocation, backup, and recovery.
- It also uses advanced features such as thin provisioning, snapshots, and cloning to reduce storage waste and improve efficiency.
- Furthermore, a unified storage architecture can scale horizontally and vertically to meet the growing demands of data-intensive applications and workloads.

Components of Unified Data Storage

- A unified data storage system contains several components, including storage controllers, storage arrays, network interfaces, and management software.

- The storage controllers manage the storage access protocols and data services, while the storage arrays contain the physical storage devices such as hard drives and solid-state drives.
- Network interfaces connect the storage system to the network, and management software provides a GUI or command-line interface for administrators to manage and monitor the storage environment.

Support for Multiple Storage Protocols

- One of the key benefits of unified storage is its support for multiple storage protocols. This allows users to access their data from a variety of platforms and applications, regardless of the underlying storage technology.
- For example, a user can access their files from their desktop PC, laptop, or mobile device, without worrying about the file format or location. Unified storage also supports multiple operating systems, including Windows, Linux, and Mac OS.

Benefits and Advantages of Unified Storage

- Unified storage offers several benefits and advantages to businesses and networks. It's simplified and cost-effective, for one.
- It also offers scalable and flexible architecture and improved data protection and security. Let's take a closer look at each of these benefits.

Simplified and Cost-effective

By consolidating different types of storage into a single platform, unified storage simplifies storage management and reduces operational costs. It eliminates the need for separate storage systems for different types of data, reducing the time and effort required to manage and maintain them.

Additionally, unified storage can help businesses save money on storage hardware and software licenses, as they no longer need to purchase separate systems for block and file storage.

Scalable and Flexible

A unified storage architecture is designed to scale both horizontally and vertically to meet the growing demands of data-intensive applications and workloads.

It uses tiered storage, thin provisioning, and other techniques to optimize the use of available storage resources, increasing the system's capacity and performance.

A unified storage architecture is also flexible enough to support different storage technologies, including hard disk drives, solid-state drives, and cloud storage.

Potential Downsides of Unified Storage

While unified storage offers many benefits, it also has potential downsides that businesses should consider. Two of the most significant downsides are performance and complexity issues and vendor lock-in.

Performance and Complexity Issues

Unified storage can be more challenging to manage and maintain than separate systems for block and file storage.

This complexity can lead to performance issues, especially when dealing with data-intensive applications and workloads.

Furthermore, unified storage may require additional resources, like network bandwidth and processing power, to handle the diverse storage workloads effectively.

Vendor Lock-in

Another potential downside of unified storage is that it can be challenging to switch vendors or migrate to different storage technologies once you have committed to a particular system.

This can result in higher costs and being locked in to specific hardware and software.

Unified Storage Vendors and Providers

There are several vendors and providers that claim to provide unified storage solutions, including NetApp, Dell, and Hewlett Packard. Each vendor offers a different set of features, performance, and pricing options.

However, historically these legacy storage systems have only offered unified storage via compromises and retrofits leveraging architectures built for the era of spinning disk. They lack native multi-protocol support for block and file on all-flash storage.

FlashArray is the first truly unified block and file platform of its kind. Not only do you get a global storage pool that can be used across block and file, but you also can expand it non-disruptively on the fly with unlimited file system sizes. FlashArray also offers high performance, scalability, and flexibility, making it an excellent choice for businesses and networks with demanding storage needs.

Block Storage vs. File Storage vs. Unified Storage

Block storage is a type of storage that manages data in large, fixed-sized blocks, typically used for databases, virtual machines, and backup data. File storage, on the other hand, organizes data into files and folders, typically used for documents, images, and video files. Unified storage combines both block and file storage protocols into a single platform, providing a more versatile and flexible storage solution.

Object storage vs. file storage vs. block storage

- Over time, the world's data storage needs have evolved with the introduction of the internet and an expanding list of data sources and types. Traditional file storage and block storage aren't well-suited to handle the enormous amount of data being generated, especially unstructured data that is not made to fit into structured data storage methods.

So, how does object storage compare to file storage and block storage?

File storage

File storage stores and organizes data into folders, similar to the physical files you might store in a paper filing system in an office. If you need information from a file, you'll need to know what room, cabinet, drawer, and folder contains that specific document. This same hierarchical storage structure is used for file storage, where files are named, tagged with metadata, and then placed in folders.

To locate a piece of data, you'll need to know the correct path to find it. Over time, searching and retrieving data files can become time-consuming as the number of files grows. While scalability is more limited, it is a simple way to store small amounts of just about any type of data and make it accessible to multiple users at once.

Block storage

Block storage improves on the performance of file storage, breaking files into separate blocks and storing them separately. A block-storage system will assign a unique identifier to each chunk of raw data, which can then be used to reassemble them into the complete file when you need to access it. Block storage doesn't require a single path to data, so you can store it wherever is most convenient and still retrieve it quickly when needed.

Block storage works well for organizations that work with large amounts of transactional data or mission-critical applications that need minimal delay and consistent performance. However, it can be expensive, offers no metadata capabilities, and requires an operating system to access blocks.

Object storage

Object storage, as discussed earlier, saves files in a flat data environment, or storage pool, as a self-contained object that contains all the data, a unique identifier, and detailed metadata that contains information about the data, permissions, policies, and other contingencies. Object storage works best for static storage, especially for unstructured data, where you write data once but may need to read it many times.

While object storage eliminates the need for directories, folders, and other complex hierarchical organization, it's not a good solution for dynamic data that is changing constantly as you'll need to rewrite the entire object to modify it. In some cases, file storage and block storage may still suit your needs depending on your speed and performance requirements.

➔ FIBRE CHANNEL SAN

- Fibre Channel is a high-speed network technology that runs on high-speed optical fiber cables (preferred for front-end SAN connectivity) and serial copper cables (preferred for back-end disk connectivity).
- The FC technology was created to meet the demand for increased speeds of data transfer among computers, servers, and mass storage subsystems.

➔ SOFTWARE DEFINED NETWORKING (SDN)

- SDN is an approach to networking that uses software controllers that can be driven by application programming interfaces (APIs) to communicate with hardware infrastructure to direct network traffic. Using software, it creates and operates a series of virtual overlay networks that work in conjunction with a physical underlay network.
- SDNs offer the potential to deliver application environments as code and minimize the hands-on time needed for managing the network.

Types of SDN

There are four primary types of software-defined networking (SDN):

· **Open SDN** – Open protocols are used to control the virtual and physical devices responsible for routing the data packets.

· **API SDN** – Through programming interfaces, often called southbound APIs, organizations control the flow of data to and from each device.

· **Overlay Model SDN** – It creates a virtual network above existing hardware, providing tunnels containing channels to data centers. This model then allocates bandwidth in each channel and assigns devices to each channel.

· **Hybrid Model SDN** – By combining SDN and traditional networking, the hybrid model assigns the optimal protocol for each type of traffic. Hybrid SDN is often used as an incremental approach to SDN.

SDN Architecture

The architecture of software-defined networking (SDN) consists of three main layers: the application layer, the control layer, and the infrastructure layer. Each layer has a specific role and interacts with the other layers to manage and control the network.

Infrastructure Layer: The infrastructure layer is the bottom layer of the SDN architecture, also known as the data plane. It consists of physical and virtual network devices such as switches, routers, and firewalls that are responsible for forwarding network traffic based on the instructions received from the control plane.

Control Layer: The control layer is the middle layer of the SDN architecture, also known as the control plane. It consists of a centralized controller that communicates with the infrastructure layer devices and is responsible for managing and configuring the network. The controller interacts with the devices in the infrastructure layer using protocols such as OpenFlow to program the forwarding behaviour of the switches and routers. The controller uses network policies and rules to make decisions about how traffic should be forwarded based on factors such as network topology, traffic patterns, and quality of service requirements.

Application Layer: The application layer is the top layer of the SDN architecture and is responsible for providing network services and applications to end-users. This layer consists of various network applications that interact with the control layer to manage the network.

Examples of applications that can be deployed in an SDN environment include network virtualization, traffic engineering, security, and monitoring. The application layer can be used to create customized network services that meet specific business needs.

The main benefit of the SDN architecture is its flexibility and ability to centralize control of the network. The separation of the control plane from the data plane enables network administrators to configure and manage the network more easily and in a more granular way, allowing for greater network agility and faster response times to changes in network traffic.

Advantages of SDN:

Software-defined networking (SDN) offers several advantages over traditional networking architectures, including:

- ***Centralized Network Control:*** One of the key benefits of SDN is that it centralizes the control of the network in a single controller, making it easier to manage and configure the network. This allows network administrators to define and enforce network

policies in a more granular way, resulting in better network security, performance, and reliability.

- ***Programmable Network:*** In an SDN environment, network devices are programmable and can be reconfigured on the fly to meet changing network requirements. This allows network administrators to quickly adapt the network to changing traffic patterns and demands, resulting in better network performance and efficiency.
- ***Cost Savings:*** With SDN, network administrators can use commodity hardware to build a network, reducing the cost of proprietary network hardware. Additionally, the centralization of network control can reduce the need for manual network management, leading to cost savings in labor and maintenance.
- ***Enhanced Network Security:*** The centralized control of the network in SDN makes it easier to detect and respond to security threats. The use of network policies and rules allows administrators to implement fine-grained security controls that can mitigate security risks.
- ***Scalability:*** SDN makes it easier to scale the network to meet changing traffic demands. With the ability to programmatically control the network, administrators can quickly adjust the network to handle more traffic without the need for manual intervention.
- ***Simplified Network Management:*** SDN can simplify network management by abstracting the underlying network hardware and presenting a logical view of the network to administrators. This makes it easier to manage and troubleshoot the network, resulting in better network uptime and reliability.

Disadvantages of SDN

While software-defined networking (SDN) has several advantages over traditional networking, there are also some potential disadvantages that organizations should be aware of. Here are some of the main disadvantages of SDN:

- ***Complexity:*** SDN can be more complex than traditional networking because it involves a more sophisticated set of technologies and requires specialized skills to manage. For example, the use of a centralized controller to manage the network requires a deep understanding of the SDN architecture and protocols.
- ***Dependency on the Controller:*** The centralized controller is a critical component of SDN, and if it fails, the entire network could go down. This means that organizations need to ensure that the controller is highly available and that they have a robust backup and disaster recovery plan in place.
- ***Compatibility:*** Some legacy network devices may not be compatible with SDN, which means that organizations may need to replace or upgrade these devices to take full advantage of the benefits of SDN.
- ***Security:*** While SDN can enhance network security, it can also introduce new security risks. For example, a single point of control could be an attractive target for attackers, and the programmability of the network could make it easier for attackers to manipulate traffic.
- ***Vendor Lock-In:*** SDN solutions from different vendors may not be interoperable, which could lead to vendor lock-in. This means that organizations may be limited in

their ability to switch to another vendor or integrate new solutions into their existing network.

- ***Performance:*** The centralized control of the network in SDN can introduce latency, which could impact network performance in certain situations. Additionally, the overhead of the SDN controller could impact the performance of the network as the network scales.

➔ COMPONENTS OF FC SAN

- A SAN consists of **three basic components: servers, network infrastructure, and storage.**
- These components can be further broken down into the following key elements: ***node ports, cabling, interconnecting devices (such as FC switches or hubs), storage arrays, and SAN management software.***

Node Ports

- In fibre channel, devices such as hosts, storage and tape libraries are all referred to as nodes. Each node is a source or destination of information for one or more nodes.
- Each node requires one or more ports to provide a physical interface for communicating with other nodes. These ports are integral components of an HBA and the storage front-end adapters.
- A port operates in full-duplex data transmission mode with a transmit (Tx) link and a receive (Rx) link (see Figure 6-3)

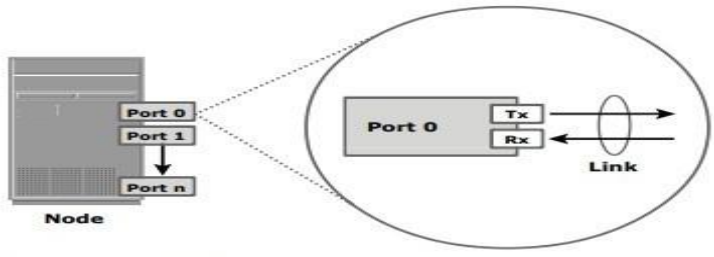


Figure 6-3: Nodes, ports, and links

Cabling

- SAN implementations use optical fiber cabling. Copper can be used for shorter distances for back-end connectivity, as it provides a better signal-to-noise ratio for distances up to 30 meters.
- Optical fiber cables carry data in the form of light.
- There are two types of optical cables, multi-mode and single-mode. Multi-mode fiber (MMF) cable carries multiple beams of light projected at different angles simultaneously onto the core of the cable (see Figure 6-4 (a)).
- Based on the bandwidth, multi-mode fibers are classified as OM1 (62.5µm), OM2 (50µm) and laser optimized OM3 (50µm). In an MMF transmission, multiple light beams traveling inside the cable tend to disperse and collide.
- This collision weakens the signal strength after it travels a certain distance — a process known as modal dispersion. An MMF cable is usually used for distances of up to 500 meters because of signal degradation (attenuation) due to modal dispersion.

Single-mode fiber (SMF) carries a single ray of light projected at the center of the core (see Figure 6-4 (b)).

- These cables are available in diameters of 7–11 microns; the most common size is 9 microns. In an SMF transmission, a single light beam travels in a straight line through the core of the fiber.
- The small core and the single light wave limits modal dispersion. Among all types of fibre cables, single-mode provides minimum signal attenuation over maximum distance (up to 10 km).
- A single-mode cable is used for long-distance cable runs, limited only by the power of the laser at the transmitter and sensitivity of the receiver

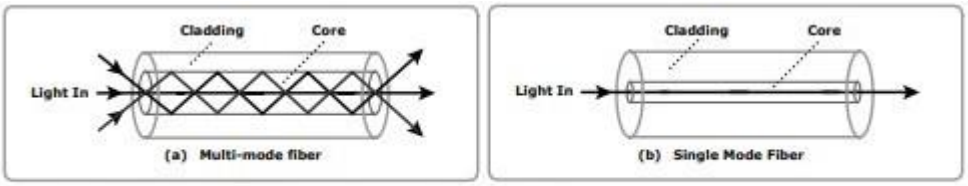


Figure 6-4: Multi-mode fiber and single-mode fiber

- MMFs are generally used within data centers for shorter distance runs, while SMFs are used for longer distances. MMF transceivers are less expensive as compared to SMF transceivers.
- A Standard connector (SC) (see Figure 6-5 (a)) and a Lucent connector (LC) (see Figure 6-5 (b)) are two commonly used connectors for fiber optic cables.
- An SC is used for data transmission speeds up to 1 Gb/s, whereas an LC is used for speeds up to 4 Gb/s. Figure 6-6 depicts a Lucent connector and a Standard connector.
- A Straight Tip (ST) is a fiber optic connector with a plug and a socket that is locked with a half-twisted bayonet lock (see Figure 6-5 (c)).
- In the early days of FC deployment, fiber optic cabling predominantly used ST connectors. This connector is often used with Fibre Channel patch panels

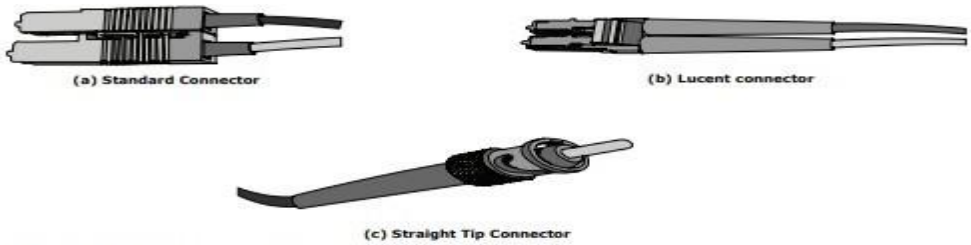


Figure 6-5: SC, LC, and ST connectors

- The Small Form-factor Pluggable (SFP) is an optical transceiver used in optical communication. The standard SFP+ transceivers support data rates up to 10 Gb/s.

Interconnect Devices

- Hubs, switches, and directors are the interconnect devices commonly used in SAN. Hubs are used as communication devices in FC-AL implementations. Hubs physically connect nodes in a logical loop or a physical star topology.
- All the nodes must share the bandwidth because data travels through all the connection points. Because of availability of low cost and high performance switches, hubs are no longer used in SANs.

- Switches are more intelligent than hubs and directly route data from one physical port to another.
- Therefore, nodes do not share the bandwidth. Instead, each node has a dedicated communication path, resulting in bandwidth aggregation
- Directors are larger than switches and are deployed for data center implementations. The function of directors is similar to that of FC switches, but directors have higher port count and fault tolerance capabilities.

Storage Arrays

- The fundamental purpose of a SAN is to provide host access to storage resources.
- The large storage capacities offered by modern storage arrays have been exploited in SAN environments for storage consolidation and centralization.
- SAN implementations complement the standard features of storage arrays by providing high availability and redundancy, improved performance, business continuity, and multiple host connectivity.

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. It provides key management functions, including mapping of storage devices, switches, and servers, monitoring and generating alerts for discovered devices, and logical partitioning of the SAN, called zoning.
- In addition, the software provides management of typical SAN components such as HBAs, storage components, and interconnecting devices.

➔ FC ARCHITECTURE

- The FC architecture represents true channel/network integration with standard interconnecting devices. Connections in a SAN are accomplished using FC.
- Traditionally, transmissions from host to storage devices are carried out over channel connections such as a parallel bus. Channel technologies provide high levels of performance with low protocol overheads.
- Such performance is due to the static nature of channels and the high level of hardware and software integration provided by the channel technologies.
- However, these technologies suffer from inherent limitations in terms of the number of devices that can be connected and the distance between these devices. Fibre Channel Protocol (FCP) is the implementation of serial SCSI-3 over an FC network. In the FCP architecture, all external and remote storage devices attached to the SAN appear as local devices to the host operating system.

The key advantages of FCP are as follows:

■Sustained transmission bandwidth over long distances.

■Support for a larger number of addressable devices over a network. Theoretically, FC can support over 15 million device addresses on a network.
■ Exhibits the characteristics of channel transport and provides speeds up to 8.5 Gb/s (8 GFC).

- The FC standard enables mapping several existing Upper Layer Protocols (ULPs) to FC frames for transmission, including SCSI, IP, High Performance Parallel Interface (HIPPI), Enterprise System Connection (ESCON), and Asynchronous Transfer Mode (ATM).

Fibre Channel Protocol Stack

- 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 6-13 illustrates the fibre channel protocol stack

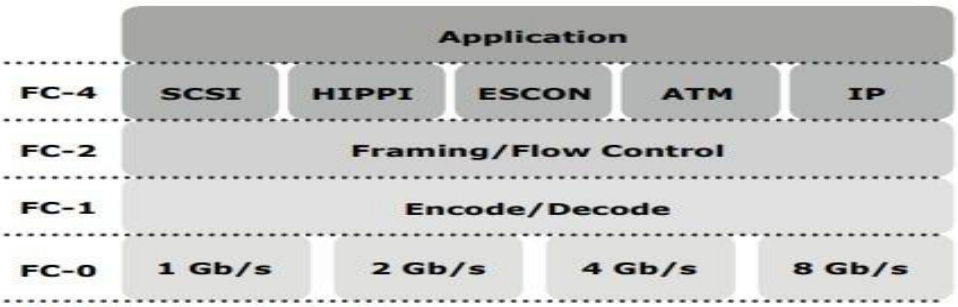


Figure 6-13: Fibre channel protocol stack

FC-4 Upper Layer Protocol

- 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. The FC standard defines several protocols that can operate on the FC-4 layer (see Figure 6-7).
- Some of the protocols include SCSI, HIPPI Framing Protocol, Enterprise Storage Connectivity (ESCON), ATM, and IP

FC-2 Transport Layer

- The FC-2 is the transport layer that contains the payload, addresses of the source and destination ports, and link control information.
- The FC-2 layer provides Fibre Channel addressing, structure, and organization of data (frames, sequences, and exchanges).
- It also defines fabric services, classes of service, flow control, and routing.

FC-1 Transmission Protocol

- This layer defines the transmission protocol that includes serial encoding and decoding rules, special characters used, and error control.

- 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.
- At the receiver node, the 10-bit character is passed to the FC-1 layer, which decodes the 10-bit character into the original 8-bit character.

FC-0 Physical Interface

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

Fibre Channel Addressing

- An FC address is dynamically assigned when a port logs on to the fabric. The FC address has a distinct format that varies according to the type of node port in the fabric. These ports can be an N_port and an NL_port in a public loop, or an NL_port in a private loop.
- The first field of the FC address of an N_port contains the domain ID of the switch (see Figure 6-14).
- This is an 8-bit field. Out of the possible 256 domain IDs, 239 are available for use; the remaining 17 addresses are reserved for specific services. For example, FFFFFC is reserved for the name server, and FFFFFE is reserved for the fabric login service.
- The maximum possible number of N_ports in a switched fabric is calculated as 239 domains × 256 areas × 256 ports = 15,663,104 Fibre Channel addresses

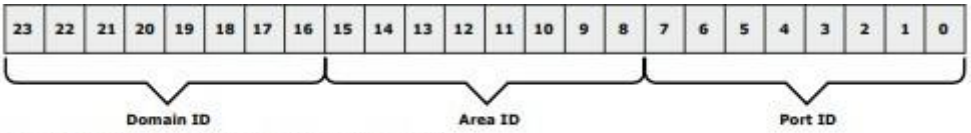


Figure 6-14: 24-bit FC address of N_port

- The area ID is used to identify a group of F_ports. An example of a group of F_ports would be a card on the switch with more than one port on it. The last field in the FC address identifies the F_port within the group.

FC Address of an NL_port

- The FC addressing scheme for an NL_port differs from other ports.
- The two upper bytes in the FC addresses of the NL_ports in a private loop are assigned zero values. However, when an arbitrated loop is connected to a fabric through an FL_port, it becomes a public loop.
- In this case, an NL_port supports a fabric login. The two upper bytes of this NL_port are then assigned a positive value, called a loop identifier, by the switch. The loop identifier is the same for all NL_ports on a given loop.
- Figure 6-15 illustrates the FC address of an NL_port in both a public loop and a private loop. The last field in the FC addresses of the NL_ports, in both public and

private loops, identifies the AL-PA. There are 127 allowable AL-PA addresses; one address is reserved for the FL_port on the switch

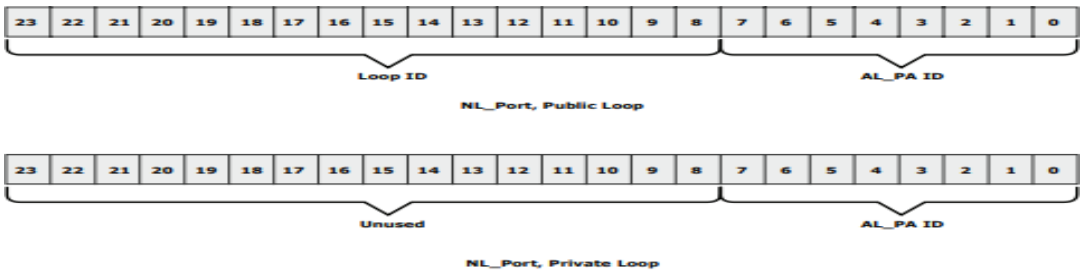


Figure 6-15: 24-bit FC address of NL_port

World Wide Names

- Each device in the FC environment is assigned a 64-bit unique identifier called the World Wide Name (WWN). The Fibre Channel environment uses two types of WWNs: World Wide Node Name (WWNN) and World Wide Port Name (WWPN). Unlike an FC address, which is assigned dynamically, a WWN is a static name for each device on an FC network.
- WWNs are similar to the Media Access Control (MAC) addresses used in IP networking. WWNs are burned into the hardware or assigned through software. Several configuration definitions in a SAN use WWN for identifying storage devices and HBAs.
- The name server in an FC environment keeps the association of WWNs to the dynamically created FC addresses for nodes. Figure 6-16 illustrates the WWN structure for an array and the HBA.

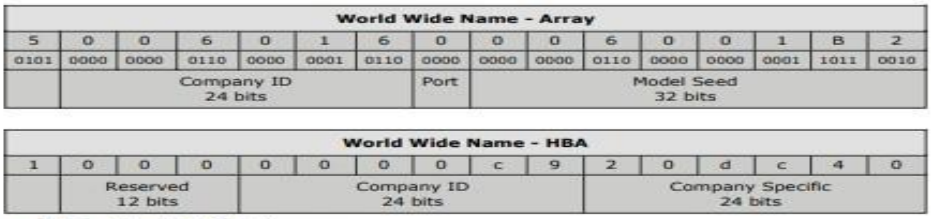


Figure 6-16: World Wide Names

FC Frame

- An FC frame (Figure 6-17) consists of five parts: start of frame (SOF), frame header, data field, cyclic redundancy check (CRC), and end of frame (EOF).
- The SOF and EOF act as delimiters.
- In addition to this role, the SOF is a flag that indicates whether the frame is the first frame in a sequence of frames. The frame header is 24 bytes long and contains addressing information for the frame.
- It includes the following information: Source ID (S_ID), Destination ID (D_ID), Sequence ID (SEQ_ID), Sequence Count (SEQ_CNT), Originating Exchange ID (OX_ID), and Responder Exchange ID (RX_ID), in addition to some control fields

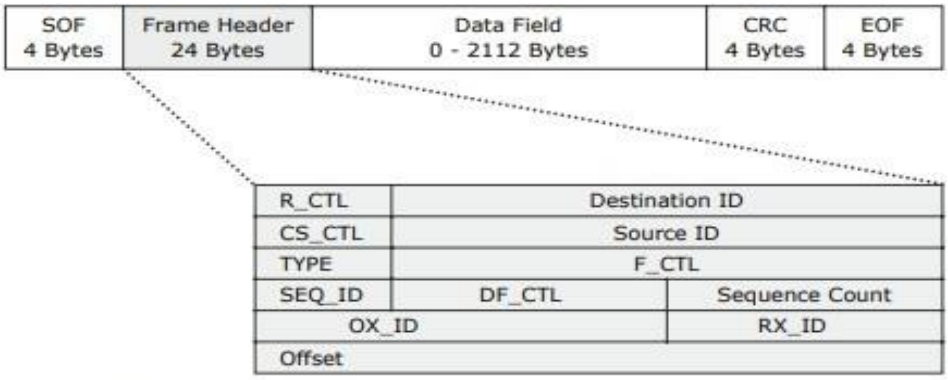


Figure 6-17: FC frame

- The S_ID and D_ID are standard FC addresses for the source port and the destination port, respectively. The SEQ_ID and OX_ID identify the frame as a component of a specific sequence and exchange, respectively.

- ***The frame header also defines the following fields:***
  ■ Routing Control (R_CTL): This field denotes whether the frame is a link control frame or a data frame. Link control frames are nondata frames that do not carry any payload. These frames are used for setup and messaging. In contrast, data frames carry the payload and are used for data transmission.
  ■ Class Specific Control (CS_CTL): This field specifies link speeds for class 1 and class 4 data transmission.
  ■ TYPE: This field describes the upper layer protocol (ULP) to be carried on the frame if it is a data frame. However, if it is a link control frame, this field is used to signal an event such as "fabric busy." For example, if the TYPE is 08, and the frame is a data frame, it means that the SCSI will be carried on an FC.
  ■ Data Field Control (DF_CTL): A 1-byte field that indicates the existence of any optional headers at the beginning of the data payload. It is a mechanism to extend header information into the payload.
  ■ Frame Control (F_CTL): A 3-byte field that contains control information related to frame content. For example, one of the bits in this field indicates whether this is the first sequence of the exchange

Structure and Organization of FC Data

- In an FC network, data transport is analogous to a conversation between two people, whereby a frame represents a word, a sequence represents a sentence, and an exchange represents a conversation.
  ■ **Exchange operation:**
  An exchange operation enables two N_ports to identify and manage a set of information units. This unit maps to a sequence. Sequences can be both unidirectional and bidirectional depending upon the type of data sequence exchanged between the initiator and the target.
  ■ **Sequence**:

A sequence refers to a contiguous set of frames that are sent from one port to another. A sequence corresponds to an information unit, as defined by the ULP.

■ **Frame:**

A frame is the fundamental unit of data transfer at Layer 2. Each frame can contain up to 2,112 bytes of payload.

Flow Control

- Flow control defines the pace of the flow of data frames during data transmission. FC technology uses two flow-control mechanisms: buffer-to-buffer credit (BB_Credit) and end-to-end credit (EE_Credit).

BB_Credit

- FC uses the BB_Credit mechanism for hardware-based flow control.
- BB_Credit controls the maximum number of frames that can be present over the link at any given point in time. In a switched fabric, BB_Credit management may take place between any two FC ports.
- The transmitting port maintains a count of free receiver buffers and continues to send frames if the count is greater than 0. The BB_Credit mechanism provides frame acknowledgment through the Receiver Ready (R_RDY) primitive.

EE_Credit

- The function of end-to-end credit, known as EE_Credit, is similar to that of BB_ Credit.
- When an initiator and a target establish themselves as nodes communicating with each other, they exchange the EE_Credit parameters (part of Port Login).
- The EE_Credit mechanism affects the flow control for class 1 and class 2 traffic only

Classes of Service

- The FC standards define different classes of service to meet the requirements of a wide range of applications.
- The table below shows three classes of services and their features (Table 6-1)

Table 6-1: FC Class of Services

	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 acknowl-edgement	Acknowledged	Acknowledged	Not acknowledged
Multiplexing	No	Yes	Yes
Bandwidth utilization	Poor	Moderate	High

- Another class of services is class F, which is intended for use by the switches communicating through ISLs. Class F is similar to Class 2, and it provides notification of nondelivery of frames.

➔ FC TOPOLOGIES :

- Fabric design follows standard topologies to connect devices.
- Core-edge fabric is one of the popular topology designs.
- ***Variations of core-edge fabric and mesh topologies*** are most commonly deployed in SAN implementations.

Core-Edge Fabric

- In the core-edge fabric topology, ***there are two types of switch tiers in this fabric.*** The edge tier usually comprises switches and offers an inexpensive approach to adding more hosts in a fabric.
- The tier at the edge fans out from the tier at the core. The nodes on the edge can communicate with each other.
- The core tier usually comprises enterprise directors that ensure high fabric availability. Additionally all traffic has to either traverse through or terminate at this tier. In a two-tier configuration, all storage devices are connected to the core tier, facilitating fan-out.
- The host-to-storage traffic has to traverse one and two ISLs in a two-tier and three-tier configuration, respectively.
- Hosts used for mission-critical applications can be connected directly to the core tier and consequently avoid traveling through the ISLs to process I/O requests from these hosts.
- The core-edge fabric topology increases connectivity within the SAN while conserving overall port utilization. If expansion is required, an additional edge switch can be connected to the core.
- This topology can have different variations. In a single-core topology, all hosts are connected to the edge tier and all storage is connected to the core tier.
- Figure 6-21 depicts the core and edge switches in a single-core topology.

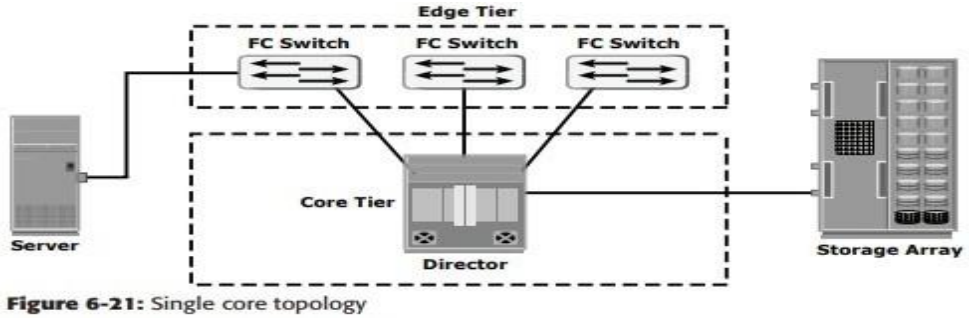


Figure 6-21: Single core topology

- A dual-core topology can be expanded to include more core switches.
- However, to maintain the topology, it is essential that new ISLs are created to connect each edge switch to the new core switch that is added.
- Figure 6-22 illustrates the core and edge switches in a dual-core topology.

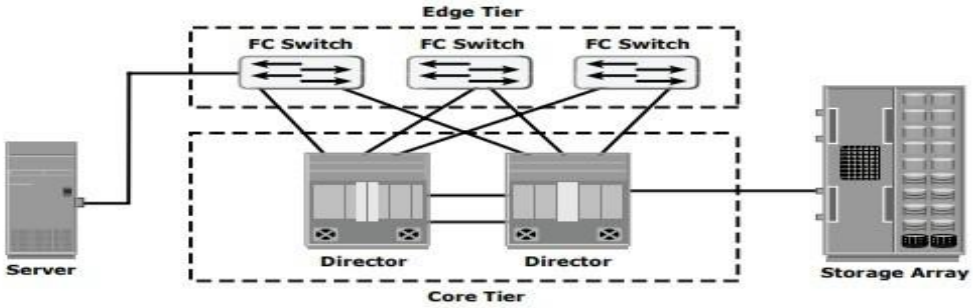


Figure 6-22: Dual-core topology

Benefits and Limitations of Core-Edge Fabric

- The core-edge fabric provides one-hop storage access to all storage in the system. Because traffic travels in a deterministic pattern (from the edge to the core), a core-edge provides easier calculation of ISL loading and traffic patterns.
- Because each tier's switch is used for either storage or hosts, one can easily identify which resources are approaching their capacity, making it easier to develop a set of rules for scaling and apportioning.
- A well-defined, easily reproducible building-block approach makes rolling out new fabrics easier. Core-edge fabrics can be scaled to larger environments by linking core switches, adding more core switches, or adding more edge switches.
- This method can be used to extend the existing simple core-edge model or to expand the fabric into a compound or complex core-edge model.
- However, the core-edge fabric may lead to some performance-related problems because scaling a core-edge topology involves increasing the number of ISLs in the fabric.
- As more edge switches are added, the domain count in the fabric increases. A common best practice is to keep the number of host-to-storage hops unchanged, at one hop, in a core-edge.
- Hop count represents the total number of devices a given piece of data (packet) passes through. Generally a large hop count means greater the transmission delay between data traverse from its source to destination.
- As the number of cores increases, it may be prohibitive to continue to maintain ISLs from each core to each edge switch. When this happens, the fabric design can be changed to a compound or complex core-edge design.

Mesh Topology

- In a mesh topology, each switch is directly connected to other switches by using ISLs. This topology promotes enhanced connectivity within the SAN.
- When the number of ports on a network increases, the number of nodes that can participate and communicate also increases.
- A mesh topology may be one of the two types: full mesh or partial mesh. In a full mesh, every switch is connected to every other switch in the topology. Full mesh topology may be appropriate when the number of switches involved is small.
- A typical deployment would involve up to four switches or directors, with each of them servicing highly localized host-to-storage traffic.

- In a full mesh topology, a maximum of one ISL or hop is required for host-to-storage traffic. In a partial mesh topology, several hops or ISLs may be required for the traffic to reach its destination.
- Hosts and storage can be located anywhere in the fabric, and storage can be localized to a director or a switch in both mesh topologies.
- A full mesh topology with a symmetric design results in an even number of switches, whereas a partial mesh has an asymmetric design and may result in an odd number of switches.
- Figure 6-23 depicts both a full mesh and a partial mesh topology.

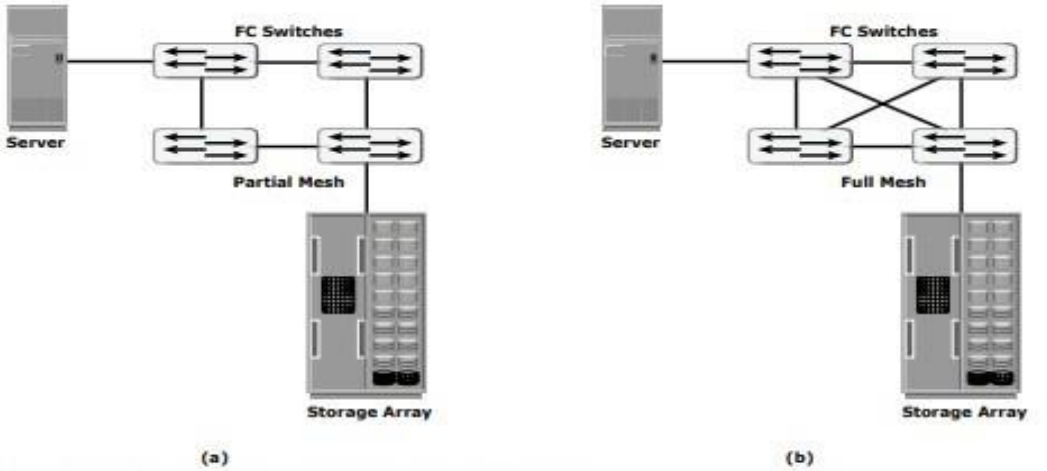


Figure 6-23: Partial mesh and full mesh topologies

➔ ZONING

- Zoning is an FC switch function that enables nodes within the fabric to be logically segmented into groups that can communicate with each other (see Figure 6-18).
- When a device (host or storage array) logs onto a fabric, it is registered with the name server.When a port logs onto the fabric, it goes through a device discovery process with other devices registered in the name server.
- The zoning function controls this process by allowing only the members in the same zone to establish these link-level services.

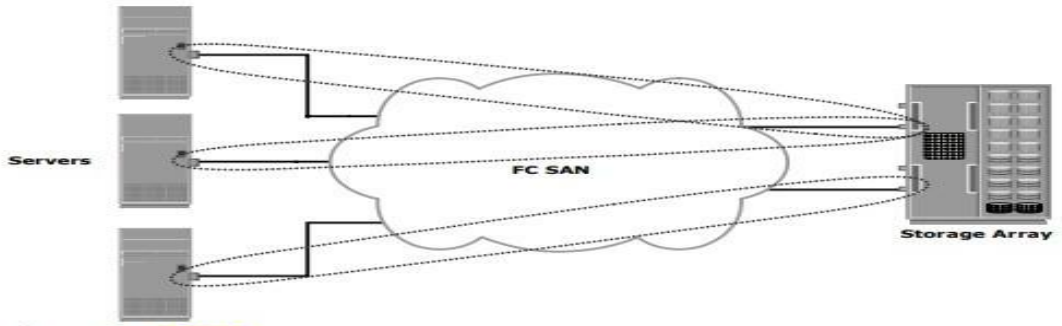


Figure 6-18: Zoning

- Multiple zone sets may be defined in a fabric, but only one zone set can be active at a time. A zone set is a set of zones and a zone is a set of members. A member may be in multiple zones. Members, zones, and zone sets form the hierarchy defined in the zoning process (see Figure 6-19).
- Members are nodes within the SAN that can be included in a zone. Zones comprise a set of members that have access to one another. A port or a node can be a member of multiple zones.
- Zone sets comprise a group of zones that can be activated or deactivated as a single entity in a fabric. Only one zone set per fabric can be active at a time.
- Zone sets are also referred to as zone configurations

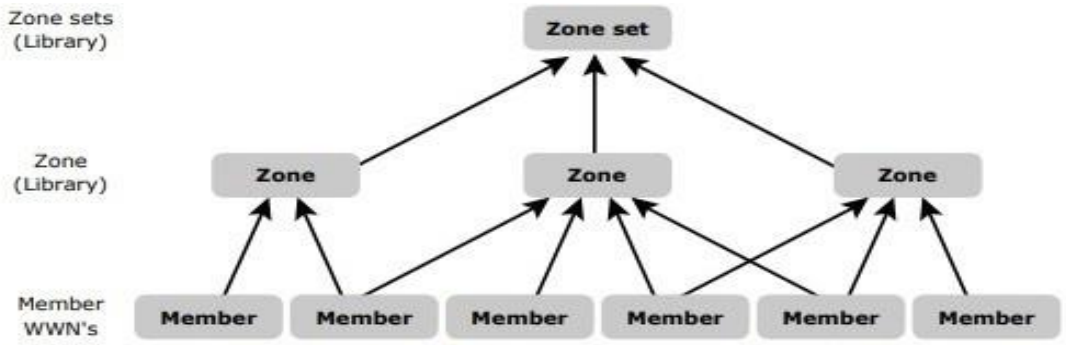


Figure 6-19: Members, zones, and zone sets

Types of Zoning

- ***Zoning can be categorized into three types:***

■ **Port zoning:** It uses the FC addresses of the physical ports to define zones.
In port zoning, access to data is determined by the physical switch port to which a node is connected.
The FC address is dynamically assigned when the port logs on to the fabric.
Therefore, any change in the fabric configuration affects zoning. Port zoning is also called *hard zoning*.
Although this method is secure, it requires updating of zoning configuration information in the event of fabric reconfiguration.

■ **WWN zoning:** It uses World Wide Names to define zones. WWN zoning is also referred to as soft zoning. A major advantage of WWN zoning is its flexibility. It allows the SAN to be recabled without reconfiguring the zone information. This is possible because the WWN is static to the node port.

■ **Mixed zoning**: It combines the qualities of both WWN zoning and port zoning. Using mixed zoning enables a specific port to be tied to the WWN of a node.

Figure 6-20 shows the three types of zoning on an FC network.

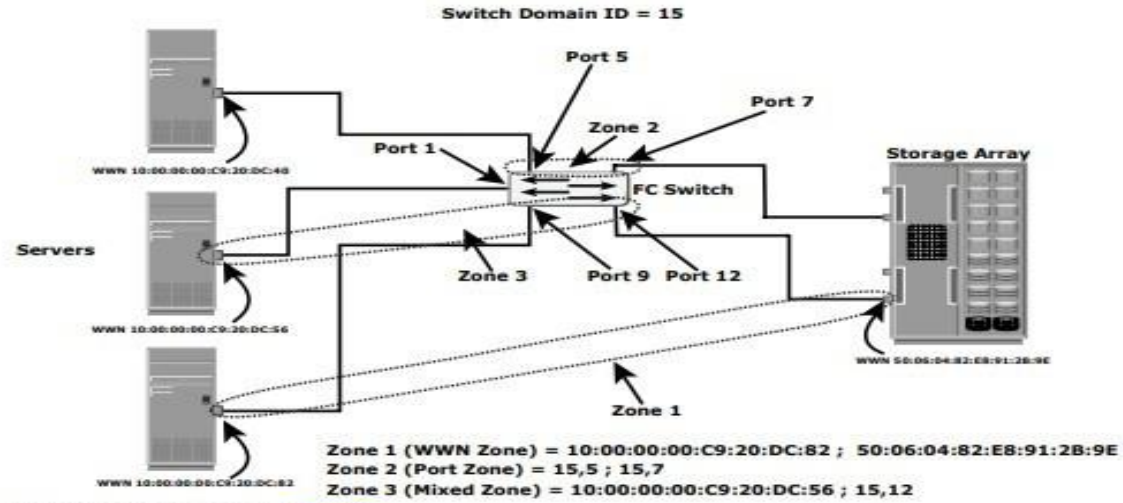


Figure 6-20: Types of zoning

- Zoning is used in conjunction with LUN masking for controlling server access to storage. However, these are two different activities.
- Zoning takes place at the fabric level and LUN masking is done at the array level

➔ FC SAN VIRTUALIZATION

- For SAN virtualization, the available virtualization features in the IBM Storage portfolio is described.
- These features enable the SAN infrastructure to support the requirements of scalability and consolidation, combining them with a lower TCO and a higher return on investment (ROI):
    - IBM b-type Virtual Fabrics
    - CISCO Virtual SAN (VSAN)
    - N_Port ID Virtualization (NPIV) support for virtual nodes

IBM b-type Virtual Fabrics

- The Virtual Fabric of the IBM b-type switches is a licensed feature that enables the logical partitioning of SAN switches. When Virtual Fabric is enabled, a default logical switch that uses all of the ports is formed.
- This default logical switch can be then divided into multiple logical switches by grouping them together at a port level. Figure 6-6 shows the flow of Virtual Fabric creation

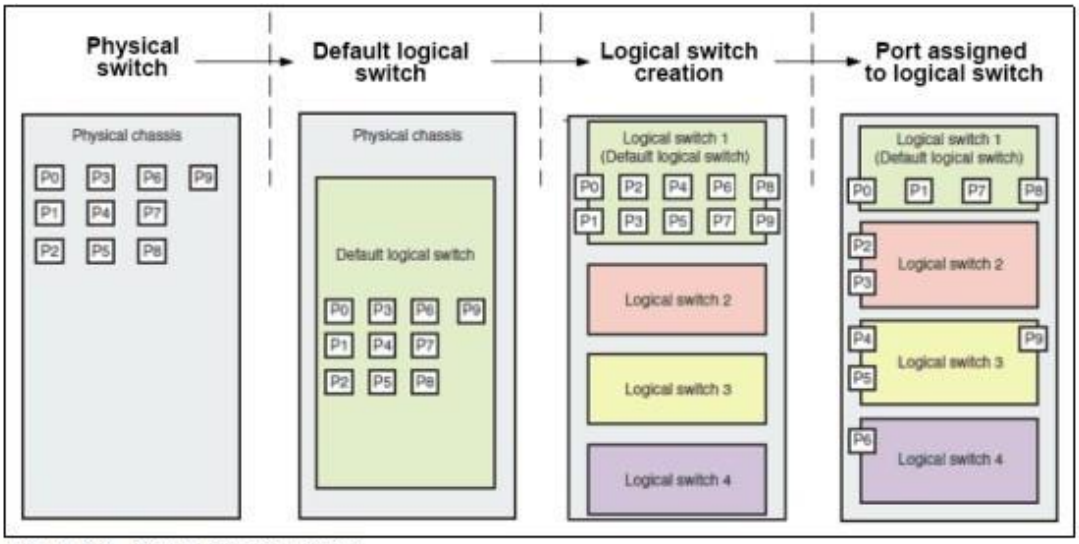


Figure 6-6 Virtual Fabric creation

- Logical fabric When the fabric is formed with at least one logical switch, the fabric is called a logical fabric.
- Two methods of fabric connectivity are available for logical fabrics:
  - ❖ A logical fabric is connected with a dedicated inter-switch link (ISL) to another switch or a logical switch.
    Figure 6-7 shows a logical fabric that is formed between logical switches through a dedicated ISL for logical switches.

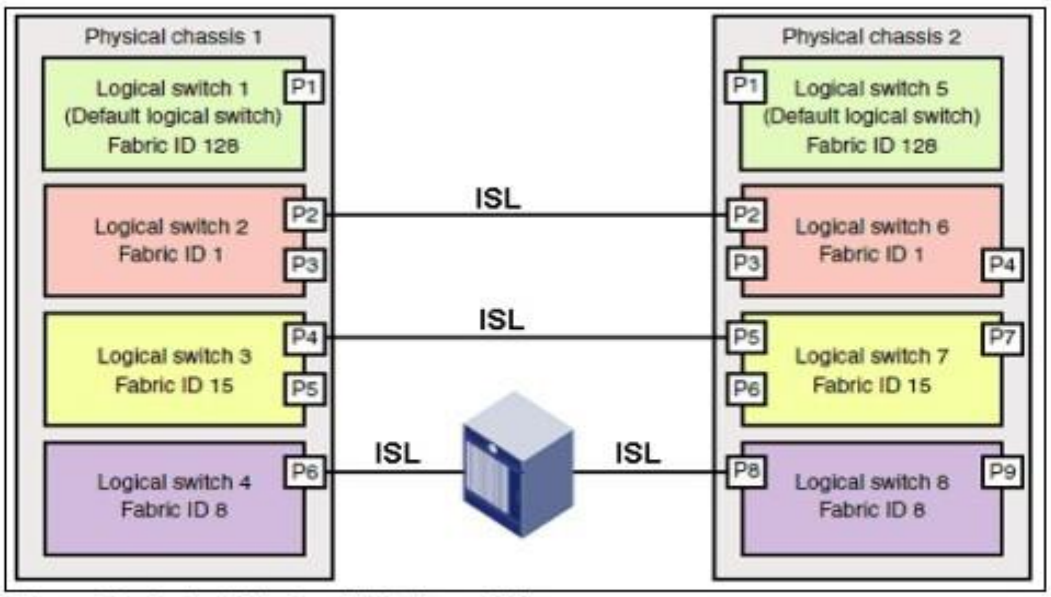


Figure 6-7 Logical fabrics with dedicated ISL

  - ❖ Logical fabrics are connected by using a shared ISL, which is called an extended ISL (XISL), from a base logical switch. In this case, the separate logical switch is configured as a base switch.
    This separate logical switch is used only for XISL connectivity and not for device connectivity.

Figure 6-8 shows a logical fabric that is formed through the XISL in the base switch

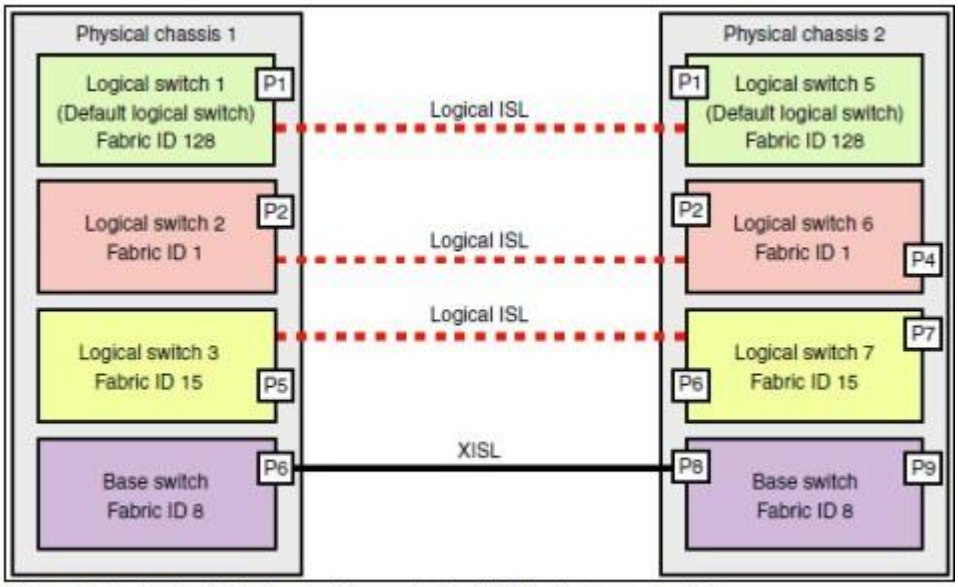


Figure 6-8 Logical ISL formed through the XISL in the base switch

- Cisco virtual storage area network Cisco virtual storage area network (VSAN) is a feature that enables the logical partition of SAN switches. A VSAN provides the flexibility to partition, for example, a dedicated VSAN for disk and tape.
- Or, a VSAN can provide the flexibility to maintain production and test devices in separate VSANs on the same chassis.
- Also, the VSAN can scale across the chassis, which allows it to overcome the fixed port numbers on the chassis.
- Virtual storage area network in a single storage area network switch With VSAN, you can consolidate small fabrics into the same chassis.
- This consolidation can also enable more security by the logical separation of the chassis into two individual VSANs.
- Figure 6-9 shows a single chassis that is divided into two logical VSANs.

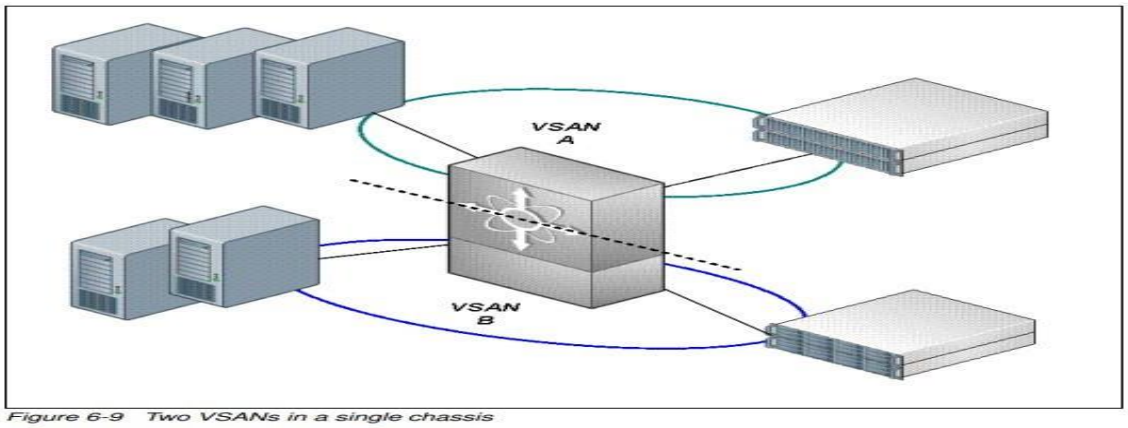


Figure 6-9 Two VSANs in a single chassis

- Virtual storage area network across multiple chassis In multiple chassis, the virtual storage area network (VSAN) can be formed with devices in one chassis to devices in another switch chassis through the extended inter-switch link (XISL).

- *Figure 6-10 shows the VSAN across chassis with an enhanced inter-switch link (EISL) for VSAN communication.*

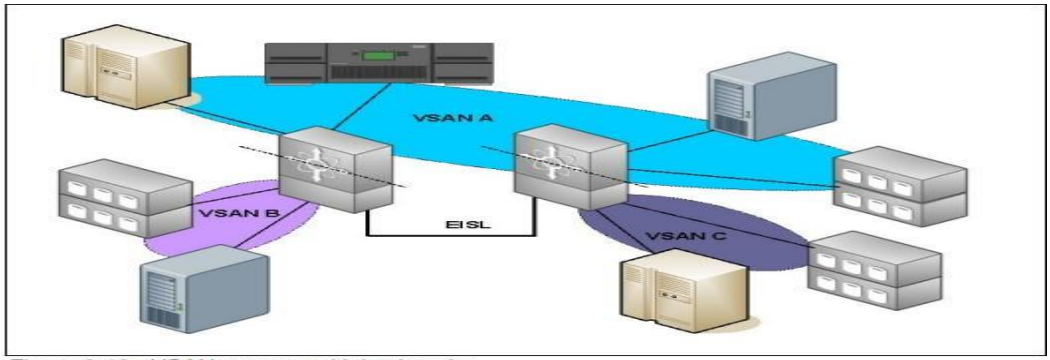


Figure 6-10 VSAN across multiple chassis

- N_Port ID Virtualization Server virtualization with blade servers provides enhanced scalability of servers. This scalability is supported equally in the SAN with N_Port ID Virtualization (NPIV).
- NPIV allows SAN switches to have one port that is shared by many virtual nodes, therefore, supporting a single HBA with many virtual nodes.
- *Figure 6-11 shows sharing a single HBA by multiple virtual nodes. In this case, the same HBA is defined with multiple virtual worldwide node names (WWNNs) and worldwide port names (WWPNs).*

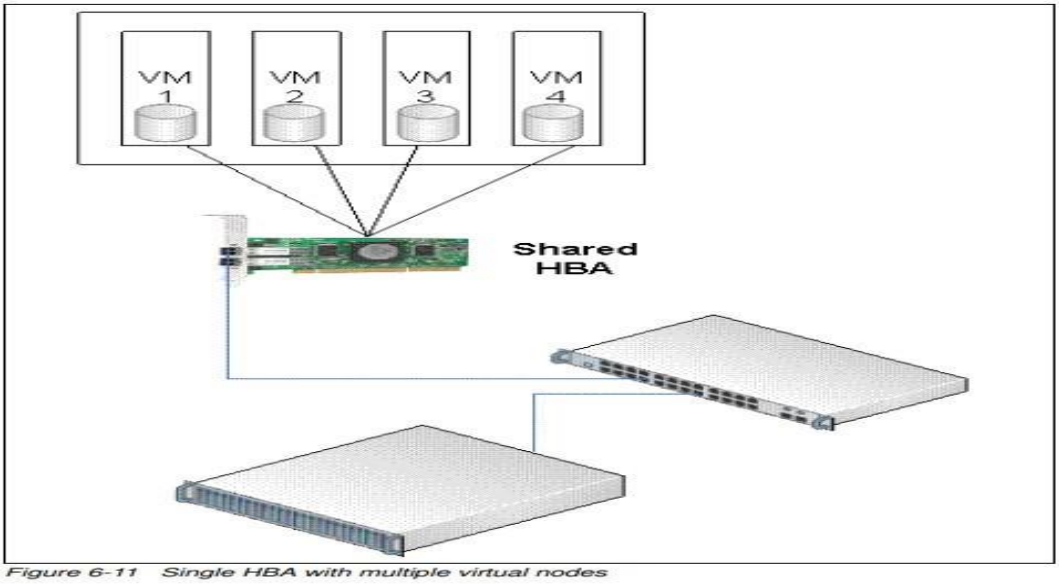


Figure 6-11 Single HBA with multiple virtual nodes

- NPIV mode of blade server switch modules On blade servers, when they are enabled with the NPIV mode, the FC switch modules that connect to an external SAN switch for access to storage act as an HBA N_port (instead of a switch E_port).
- The back-end ports are F_ports that connect to server blade modules.

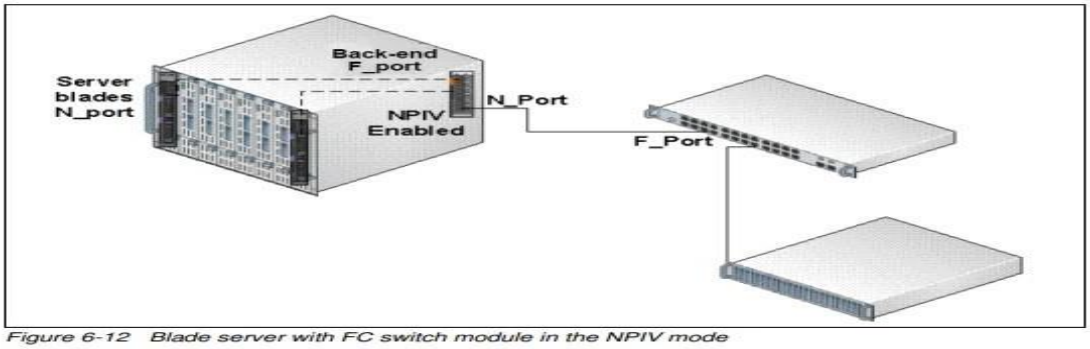


Figure 6-12 Blade server with FC switch module in the NPIV mode

- With the NPIV mode, we can overcome the interoperability issues of merging external switches that might come from separate vendors to the blade server switch module. Also, management is easier because the blade switch module becomes a node in the fabric.
- And, we can overcome the scalability limitations of many switch domains for a switch module in blade servers.

➔ INTERNET PROTOCOL SAN (IP SAN)

- IP offers easier management and better interoperability. When block I/O is run over IP, the existing network infrastructure can be leveraged, which is more economical than investing in new SAN hardware and software.
- Many long-distance, disaster recovery (DR) solutions are already leveraging IP-based networks. In addition, many robust and mature security options are now available for IP networks.
- With the advent of block storage technology that leverages IP networks (the result is often referred to as IP SAN), organizations can extend the geographical reach of their storage infrastructure.
- IP SAN technologies can be used in a variety of situations.
- Figure 8-1 illustrates the co-existence of FC and IP storage technologies in an organization where mission-critical applications are serviced through FC, and businesscritical applications and remote office applications make use of IP SAN.
- Disaster recovery solutions can also be implemented using both of these technologies.
- Two primary protocols that leverage IP as the transport mechanism are iSCSI and Fibre Channel over IP (FCIP).

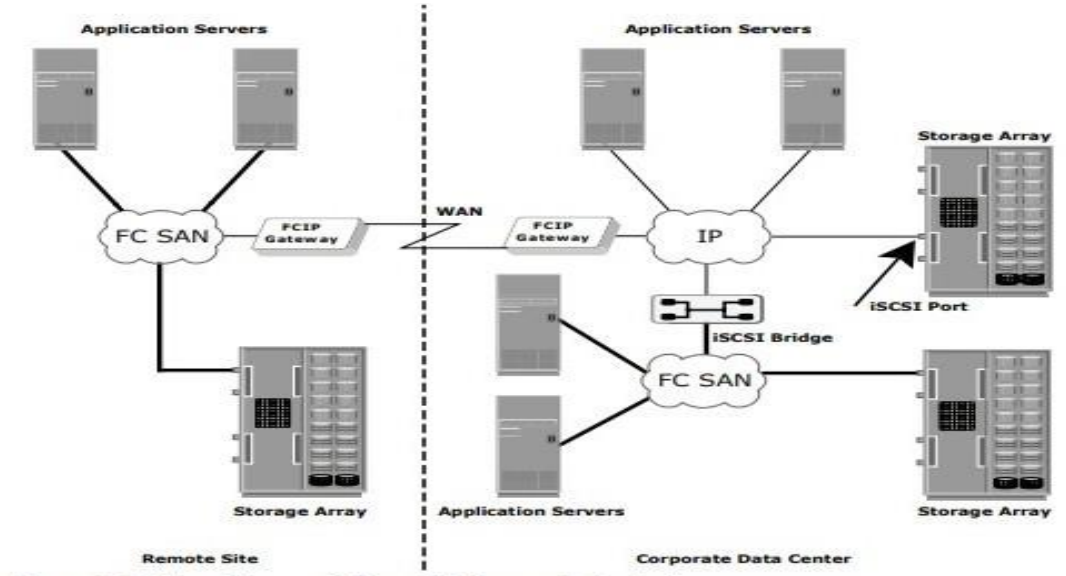


Figure 8-1: Co-existance of FC and IP storage technologies

- iSCSI is the host-based encapsulation of SCSI I/O over IP using an Ethernet NIC card or an iSCSI HBA in the host.
- As illustrated in Figure 8-2 (a), IP traffic is routed over a network either to a gateway device that extracts the SCSI I/O from the IP packets or to an iSCSI storage array.
- The gateway can then send the SCSI I/O to an FC-based external storage array, whereas an iSCSI storage array can handle the extraction and I/O natively. FCIP uses a pair of bridges (FCIP gateways) communicating over TCP/IP as the transport protocol.
- FCIP is used to extend FC networks over distances and/or an existing IP-based infrastructure, as illustrated in Figure 8-2 (b).
- Today, iSCSI is widely adopted for connecting servers to storage because it is relatively inexpensive and easy to implement, especially in environments where an FC SAN does not exist.
- FCIP is extensively used in disaster-recovery implementations, where data is duplicated on disk or tape to an alternate site.

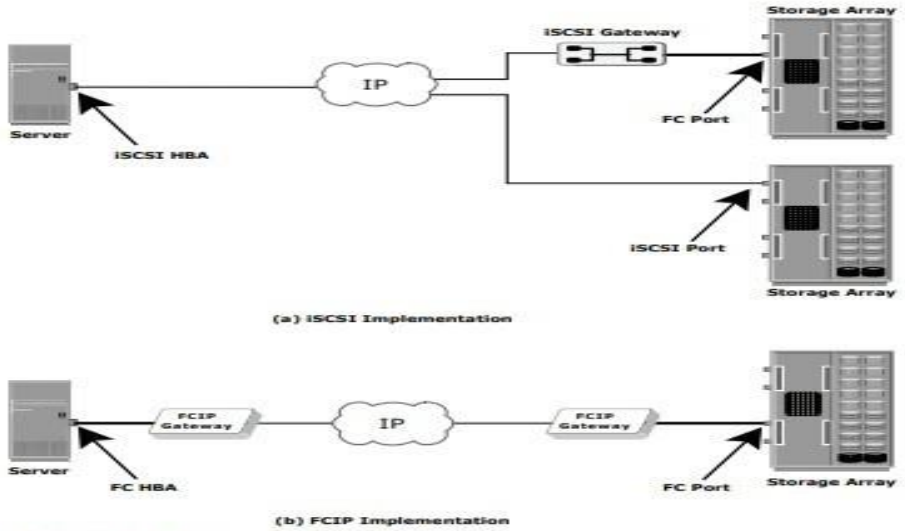


Figure 8-2: iSCSI and FCIP implementation

➔ iSCSI

- iSCSI is an IP-based protocol that establishes and manages connections between storage, hosts, and bridging devices over IP. iSCSI carries block-level data over IP-based networks, including Ethernet networks and the Internet.
- iSCSI is built on the SCSI protocol by encapsulating SCSI commands and data in order to allow these encapsulated commands and data blocks to be transported using TCP/IP packets.

➔ Components of iSCSI

- Host (initiators), targets, and an IP-based network are the principal iSCSI components. The simplest iSCSI implementation does not require any FC components. If an iSCSI-capable storage array is deployed, a host itself can act as an iSCSI initiator, and directly communicate with the storage over an IP network.
- However, in complex implementations that use an existing FC array for iSCSI connectivity, iSCSI gateways or routers are used to connect the existing FC SAN. These devices perform protocol translation from IP packets to FC packets and vice-versa, thereby bridging connectivity between the IP and FC environments.

➔ iSCSI Host Connectivity

- iSCSI host connectivity requires a hardware component, such as a NIC with a software component (iSCSI initiator) or an iSCSI HBA. In order to use the iSCSI protocol, a software initiator or a translator must be installed to route the SCSI commands to the TCP/IP stack.
- A standard NIC, a TCP/IP offload engine (TOE) NIC card, and an iSCSI HBA are the three physical iSCSI connectivity options. A standard NIC is the simplest and least expensive connectivity option.
- It is easy to implement because most servers come with at least one, and in many cases two, embedded NICs. It requires only a software initiator for iSCSI functionality. However, the NIC provides no external processing power, which places additional overhead on the host CPU because it is required to perform all the TCP/IP and iSCSI processing.
- If a standard NIC is used in heavy I/O load situations, the host CPU may become a bottleneck. TOE NIC help alleviate this burden. A TOE NIC offloads the TCP management functions from the host and leaves iSCSI functionality to the host processor.
- The host passes the iSCSI information to the TOE card and the TOE card sends the information to the destination using TCP/IP. Although this solution improves performance, the iSCSI functionality is still handled by a software initiator, requiring host CPU cycles.
- An iSCSI HBA is capable of providing performance benefits, as it offloads the entire iSCSI and TCP/IP protocol stack from the host processor.

- Use of an iSCSI HBA is also the simplest way for implementing a boot from SAN environment via iSCSI. If there is no iSCSI HBA, modifications have to be made to the basic operating system to boot a host from the storage devices because the NIC needs to obtain an IP address before the operating system loads.
- The functionality of an iSCSI HBA is very similar to the functionality of an FC HBA, but it is the most expensive option.
- A fault-tolerant host connectivity solution can be implemented using hostbased multipathing software (e.g., EMC PowerPath) regardless of the type of physical connectivity. Multiple NICs can also be combined via link aggregation technologies to provide failover or load balancing.
- Complex solutions may also include the use of vendor-specific storage-array software that enables the iSCSI host to connect to multiple ports on the array with multiple NICs or HBAs.

Topologies for iSCSI Connectivity

- The topologies used to implement iSCSI can be categorized into two classes: native and bridged. Native topologies do not have any FC components; they perform all communication over IP.
- The initiators may be either directly attached to targets or connected using standard IP routers and switches.
- Bridged topologies enable the co-existence of FC with IP by providing iSCSI-to-FC bridging functionality.
- For example, the initiators can exist in an IP environment while the storage remains in an FC SAN.

Native iSCSI Connectivity

- If an iSCSI-enabled array is deployed, FC components are not needed for iSCSI connectivity in the native topology.
- In the example shown in Figure 8-3 (a), the array has one or more Ethernet NICs that are connected to a standard Ethernet switch and configured with an IP address and listening port.
- Once a client/ initiator is configured with the appropriate target information, it connects to the array and requests a list of available LUNs.
- A single array port can service multiple hosts or initiators as long as the array can handle the amount of storage traffic that the hosts generate.
- Many arrays provide more than one interface so that they can be configured in a highly available design or have multiple targets configured on the initiator. Some NAS devices are also capable of functioning as iSCSI targets, enabling file-level and block-level access to centralized storage.
- This offers additional storage options for environments with integrated NAS devices or environments that don’t have an iSCSI/FC bridge.

Bridged iSCSI Connectivity

- A bridged iSCSI implementation includes FC components in its configuration.

- Figure 8-3 (b) illustrates an existing FC storage array used to service hosts connected through iSCSI.
- The array does not have any native iSCSI capabilities—that is, it does not have any Ethernet ports.
- Therefore, an external device, called a bridge, router, gateway, or a multi-protocol router, must be used to bridge the communication from the IP network to the FC SAN.
- These devices can be a stand-alone unit, or in many cases are integrated with an existing FC switch. In this configuration, the bridge device has Ethernet ports connected to the IP network, and FC ports connected to the storage.
- These ports are assigned IP addresses, similar to the ports on an iSCSI-enabled array. The iSCSI initiator/host is configured with the bridge's IP address as its target destination.
- The bridge is also configured with an FC initiator or multiple initiators. These are called virtual initiators because there is no physical device, such as an HBA, to generate the initiator record

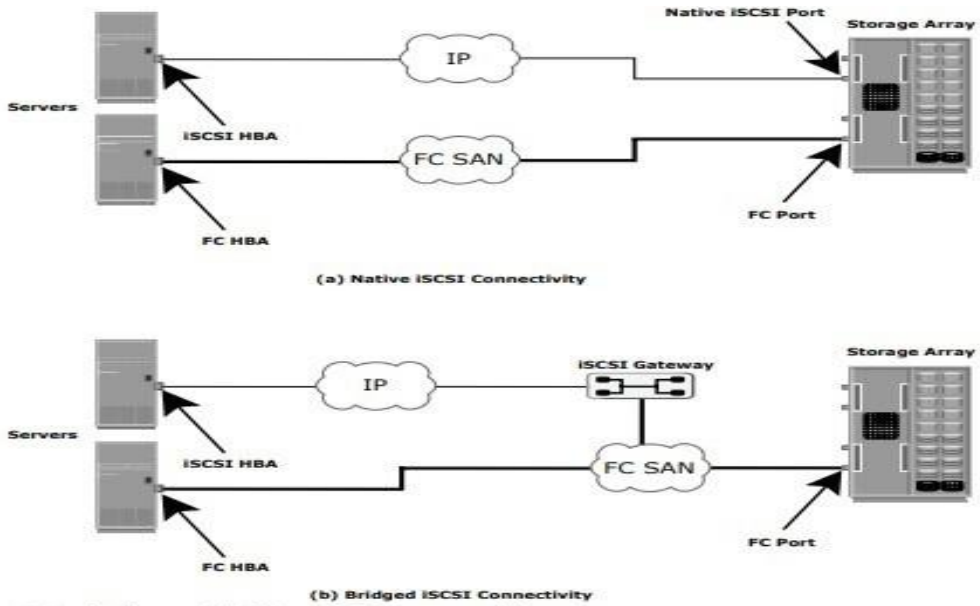


Figure 8-3: Native and bridged iSCSI connectivity

Combining FCP and Native iSCSI Connectivity

- A combination topology can also be implemented.
- In this case, a storage array capable of connecting the FC and iSCSI hosts without the need for external bridging devices is needed (see Figure 8-3 [a]).
- These solutions reduce complexity, as they remove the need for configuring bridges.
- However, additional processing requirements are placed on the storage array because it has to accommodate the iSCSI traffic along with the standard FC traffic

➔ iSCSI Protocol Stack

- The architecture of iSCSI is based on the client/server model.
- Figure 8-4 displays a model of the iSCSI protocol layers and depicts the encapsulation order of SCSI commands for their delivery through a physical carrier.

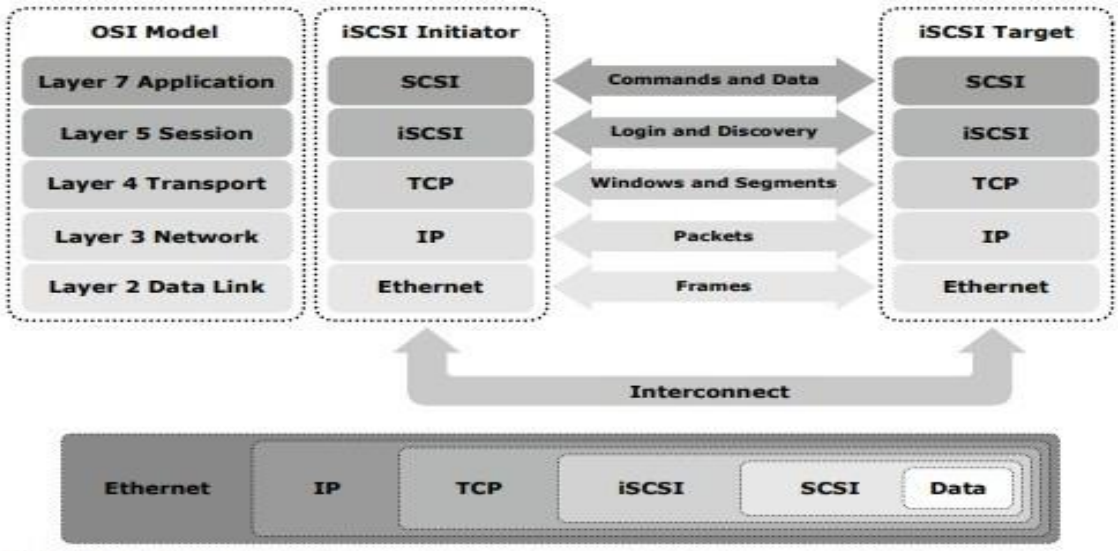


Figure 8-4: iSCSI protocol stack

- SCSI is the command protocol that works at the application layer of the 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 initiators and targets.
- iSCSI is the session-layer protocol that initiates a reliable session between a device that recognizes 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 service.
- TCP is used to control 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 for each hop through a separate physical network.

➔ LINK AGGREGATION

- Link aggregation combines multiple physical links to operate as a single larger logical link.
- The member links no longer function as independent physical connections, but as members of the larger logical link (Figure 4-9).

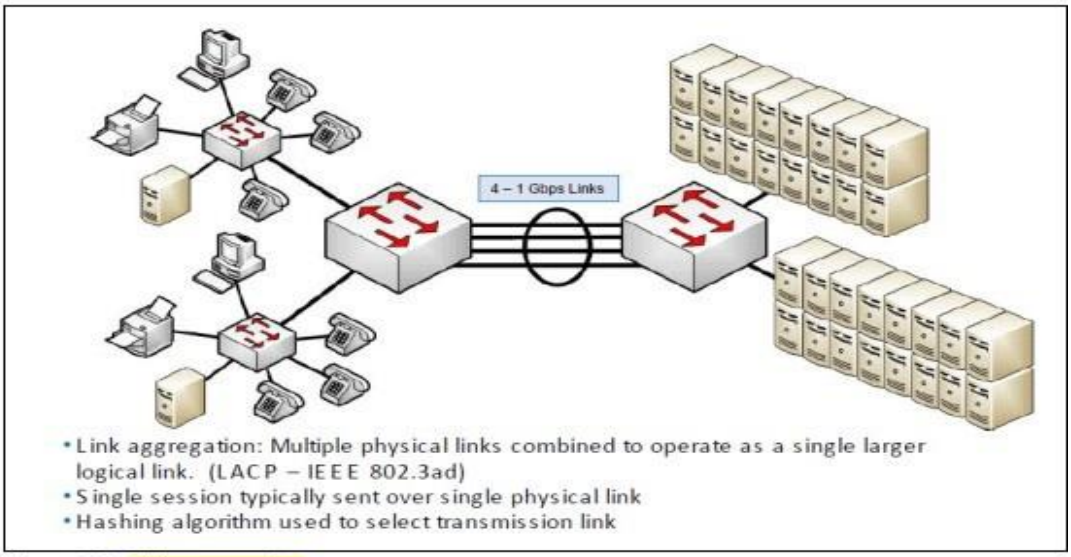


Figure 4-9 Link aggregation

- Link aggregation provides greater bandwidth between the devices at each end of the aggregated link.
- Another advantage of link aggregation is increased availability because the aggregated link is composed of multiple member links.
- If one member link fails, the aggregated link continues to carry traffic over the remaining member links. Each of the devices that is interconnected by the aggregated link uses a hashing algorithm to determine on which of the member links the frames will be transmitted.
- The hashing algorithm might use various information in the frame to make the decision.
- This algorithm might include a source MAC, destination MAC, source IP, destination IP, and more. It might also include a combination of these values.

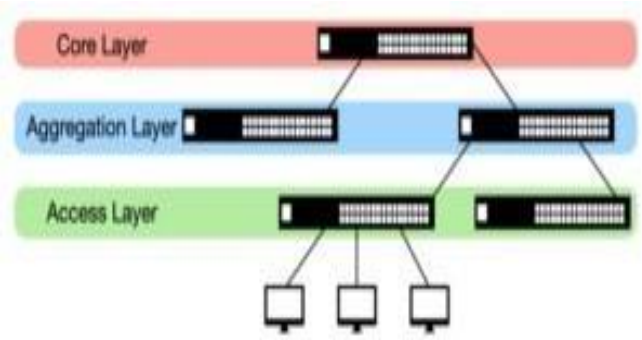
➔ SWITCH AGGREGATION:

- An aggregation switch is a networking device that allows multiple network connections to be bundled together into a single link. This enables increased bandwidth and better network performance.
- Typically, aggregation switches use link aggregation protocols, such as Link Aggregation Control Protocol (LACP) and Ethernet Aggregation to combine multiple links into a single, logical connection.
- Therefore, they can offer great flexibility and scalability, allowing for quick and easy network expansion or reconfiguration.
- In most cases, aggregation switches are used in networks with high-traffic levels or large numbers of users, as they can efficiently distribute data across multiple links.

Role of the Aggregation Switch in the Network

- The aggregation switch is located in the middle of the network architecture, which is equivalent to a middle-level manager of a company.

- It needs to be responsible for managing the data from the lower layer (the access layer switch), and at the same time, it also reports data to the upper layer (the core layer switch).
- Usually, when the aggregation switch receives data from the access switch, it will perform local routing, filtering, traffic balancing, and QoS priority management. Then it will process the security mechanism, IP address translation, and multicast management of the data.
- Finally, it will forward the data to the core layer switch or perform local routing processing according to the processing result to ensure the normal operation of the core layer.
- It can be seen from the above that the aggregation switch has functions such as source address, destination address filtering, real-time policy, security, network isolation, and segmentation.
- Compared with access switches, aggregation switches have better performance and higher switching speeds.



The aggregation switch is located in the middle of the network architecture

- However, in practical applications, some network architectures only have access switches and core switches without aggregation switches.
- The reason is that the network is small, simple, and has a short transmission distance. Users do not deploy aggregation switches to reduce network costs and maintenance burden.
- However, if the number of network users exceeds 200, and the number of users will continue to grow in the future, it is recommended to deploy aggregation switches.

Aggregation Switches vs Access Switches: What's the Difference?

The main distinction between access switches and aggregation switches is their level of operation and performance.

Operational Level. The access switch is located in the network where users can directly connect to or access the network. As for the aggregation switch, it is used to reduce the load on the core layer equipment, and it performs uploading and distributing as well as other functions such as policy implementation, security, and working group access.

Features. Aggregation switches require more performance than access layer switches to handle all traffic from access layer devices, fewer interfaces, and faster switching rates. And the access switch primarily provides adequate bandwidth for access layer access and includes

user management functions such as address authentication, user authentication, and user information collection.

Things to Consider When Selecting Aggregation Switches

Backplane Bandwidth and Packet Forwarding Rate

If the backplane bandwidth and packet forwarding rate are limited, the switch's data processing capability will be compromised, resulting in congestion.

As a result, when selecting an aggregation switch, it is sufficient to select the appropriate one based on the actual needs in order to avoid resource waste.

Port Type and Port Number

Data from several access switches must be combined by the aggregation switch before being forwarded to the core switch. The kind and quantity of uplink ports on the network's access switches must be taken into account while choosing the aggregation switch.

When choosing an aggregation switch, it is best to take the network's scale into account. As the network upgrades and expands, the company should select an enterprise-level switch with scalable ports as the aggregation switch.

Port Speed

The uplink and downlink should be considered when determining the aggregation switch port rate. The speeds of the ports can be the same or different.

For instance, when a 10G aggregation switch needs to be interconnected with a 10G access switch, a 10G downlink port must be selected.

Functional Management

Link Aggregation. High-bandwidth aggregation links connecting to core switches are required for aggregation switches. Therefore, link aggregation must be supported by aggregation switches in order to ensure that the access layer has enough bandwidth and that it can continue to function even if one of the links is cut.

Quality of Service (QoS). To assure the quality of service for a certain type of traffic, the QoS priority policy might give it a priority during transmission. The performance and quality of audio and video communications cannot be guaranteed during network transmission unless you choose an enterprise-level switch that supports QoS as an aggregation switch when you make your purchase.

Security Strategy. The aggregation switch can select an enterprise-level switch that supports security controls to stop unauthorized access and malicious information from entering the network. The ACL (Access Control List) can specify the kinds of traffic communication that are permitted, effectively stop some forms of traffic from being transmitted, and maintain network security.

Redundancy

The network's safety is guaranteed by redundancy capability. Power redundancy is crucial for aggregation switches because it allows them to continue to function even if one of their power supplies fails or needs to be replaced, preventing any disruption to the network's regular operations.

➔ VIRTUAL LOCAL AREA NETWORK (VLAN)

- A virtual local area network (VLAN) is a networking concept in which a network is logically divided into smaller virtual LANs.
- The Layer 2 traffic in one VLAN is logically isolated from other VLANs (Figure 4-5)

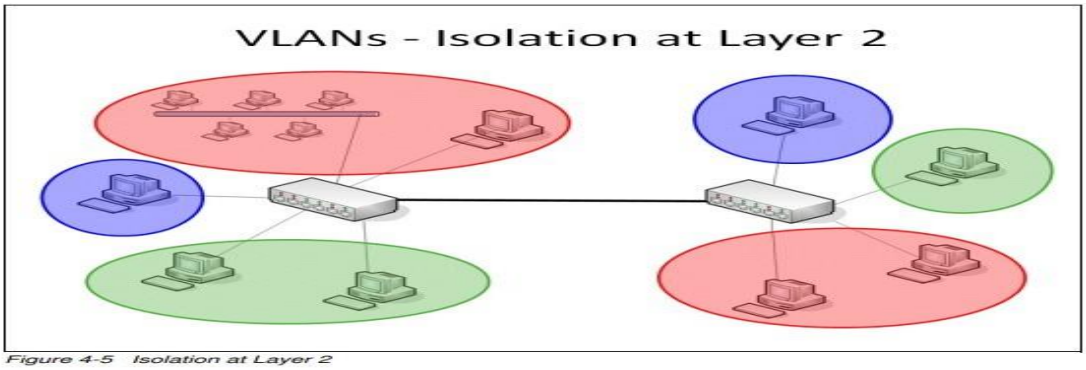


Figure 4-5 Isolation at Layer 2

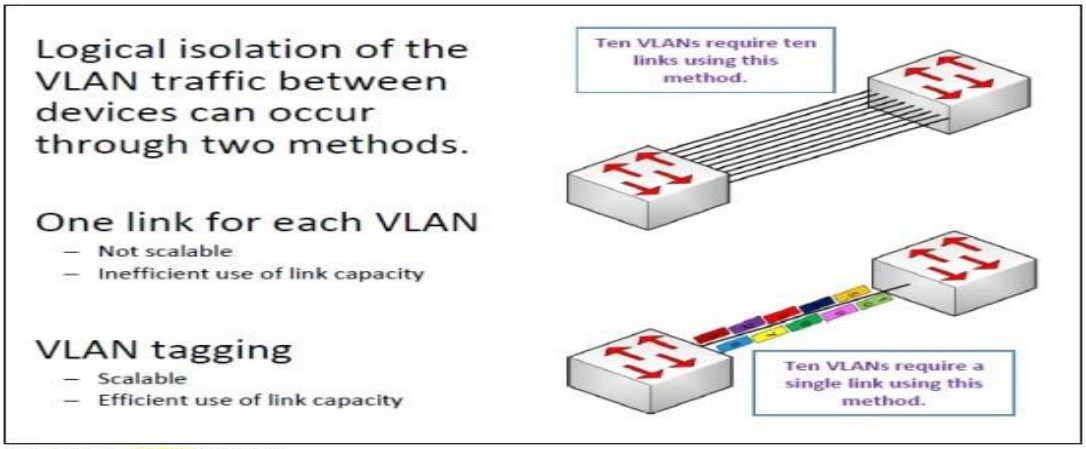


Figure 4-6 VLAN tagging

- The first method uses a single link for each VLAN. This method does not scale well because it uses many ports in networks that have multiple VLANs and multiple switches.
- Also, this method does not use link capacity efficiently when traffic in the VLANs is not uniform.
- The second method is VLAN tagging over a single link in which each frame in tagged with its VLAN ID. This method is highly scalable because only a single link is required to provide connectivity to many VLANs.
- This configuration provides for better utilization of the link capacity when VLAN traffic is not uniform.
- The protocol for VLAN tagging of frames in a LAN environment is defined by the IEEE 802.1p/q standard (priority tagging and VLAN identifier tagging).
- Inter-switch link (ISL): ISL is another protocol for providing the VLAN tagging function in a network. This protocol is not compatible with the IEEE 802.1p/q standard.

Tagged frames

- The IEEE 802.1p/q standard provides a methodology for information, such as VLAN membership and priority, that is added to the frame (Figure 4-7).

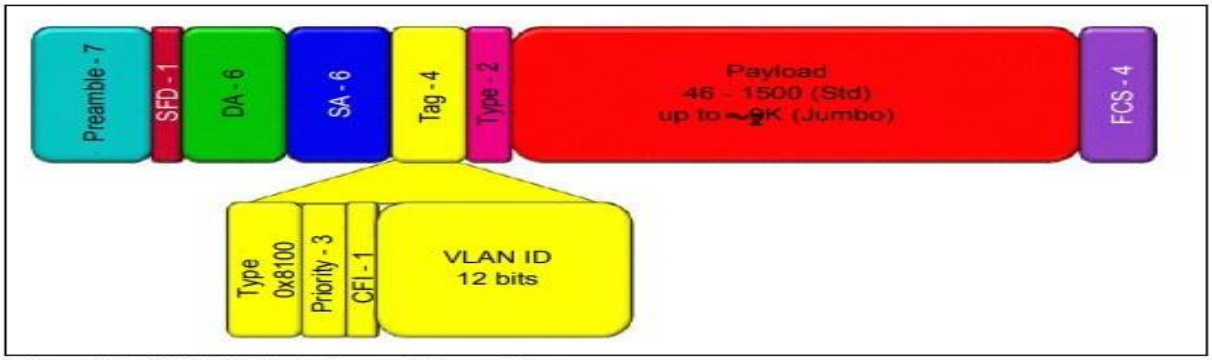


Figure 4-7 IEEE 802.1p/q tagged Ethernet frame

- The standard provides an additional 4 bytes of information to be added to each Ethernet frame. A frame that includes this extra information is known as a tagged frame.
- The 4-byte tag has four component fields:
  - ✓ The type field is 2 bytes and has the hexadecimal value of x8100 to identify the frame as an 802.1p/q tagged frame.
  - ✓ The priority field is 3 bits and allows a priority value of eight different values to be included in the tag. This field has the "P" portion of the 802.1p/q standard.
  - ✓ The Canonical Format Indicator field is 1 bit and identifies when the contents of the payload field are in canonical format.
  - ✓ The VLAN ID field is 12 bits and identifies the VLAN that the frame is a member of, with 4,096 different VLANs that are possible.

➔ FCIP PROTOCOL

- Organizations are now looking for new ways to transport data throughout the enterprise, locally over the SAN as well as over longer distances, to ensure that data reaches all the users who need it.
- One of the best ways to achieve this goal is to interconnect geographically dispersed SANs through reliable, high-speed links.
- This approach involves transporting FC block data over the existing IP infrastructure used throughout the enterprise.
- The FCIP standard has rapidly gained acceptance as a manageable, costeffective way to blend the best of two worlds: FC block-data storage and the proven, widely deployed IP infrastructure.
- FCIP is a tunneling protocol that enables distributed FC SAN islands to be transparently interconnected over existing IP-based local, metropolitan, and wide-area networks.
- As a result, organizations now have a better way to protect, store, and move their data while leveraging investments in existing technology. FCIP uses TCP/IP as its underlying protocol.
- In FCIP, the FC frames are encapsulated onto the IP payload, as shown in Figure 8-9. FCIP does not manipulate FC frames (translating FC IDs for transmission).

- When SAN islands are connected using FCIP, each interconnection is called an FCIP link.
- A successful FCIP link between two SAN islands results in a fully merged FC fabric.

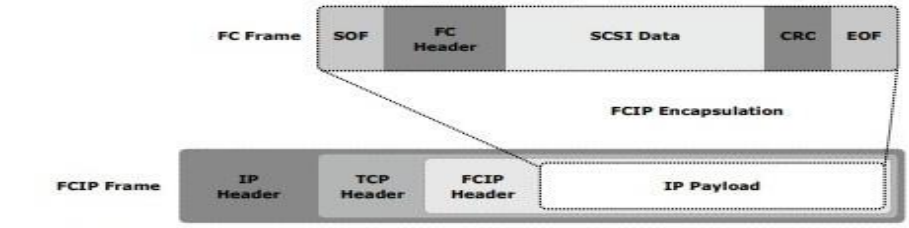


Figure 8-9: FCIP encapsulation

➔ FCIP Topology (FCIP CONNECTIVITY AND CONFIGURATION)

- An FCIP environment functions as if it is a single cohesive SAN environment. Before geographically dispersed SANs are merged, a fully functional layer 2 network exists on the SANs.
- This layer 2 network is a standard SAN fabric.
- These physically independent fabrics are merged into a single fabric with an IP link between them. An FCIP gateway router is connected to each fabric via a standard FC connection (see Figure 8-10).
- The fabric treats these routers like layer 2 fabric switches. The other port on the router is connected to an IP network and an IP address is assigned to that port. This is similar to the method of assigning an IP address to an iSCSI port on a gateway.
- Once IP connectivity is established, the two independent fabrics are merged into a single fabric.
- When merging the two fabrics, all the switches and routers must have unique domain IDs, and the fabrics must contain unique zone set names. Failure to ensure these requirements will result in a segmented fabric.
- The FC addresses on each side of the link are exposed to the other side, and zoning or masking can be done to any entity in the new environment.

•

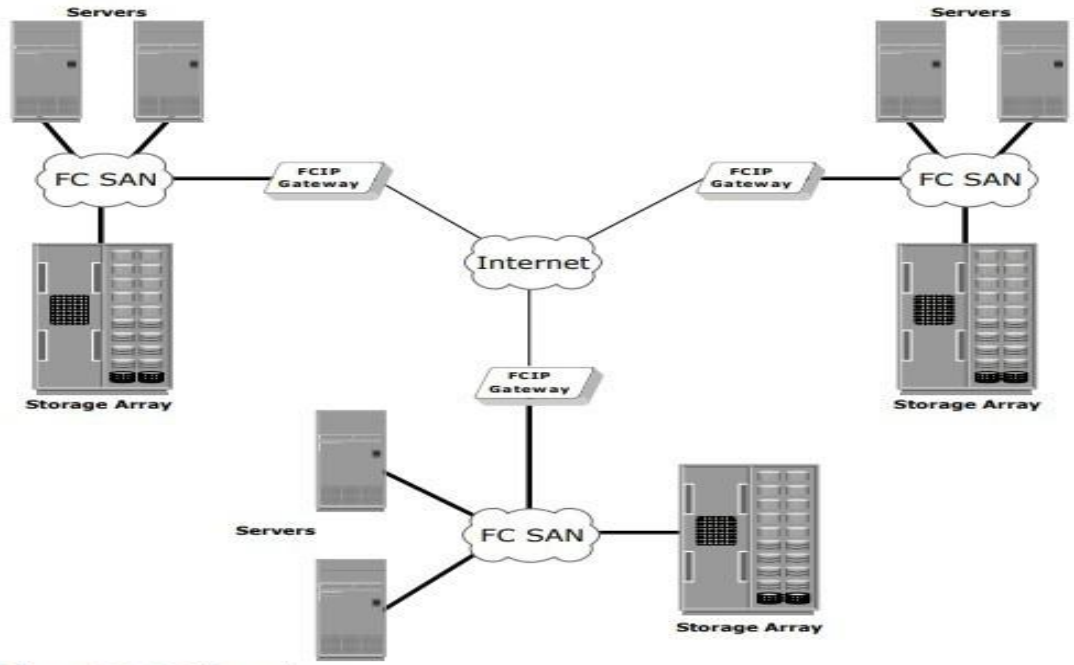


Figure 8-10: FCIP topology

FCIP Performance and Security

- Performance, reliability, and security should always be taken into consideration when implementing storage solutions.
- The implementation of FCIP is also subject to the same consideration. From the perspective of performance, multiple paths to multiple FCIP gateways from different switches in the layer 2 fabric eliminates single points of failure and provides increased bandwidth.
- In a scenario of extended distance, the IP network may be a bottleneck if sufficient bandwidth is not available.
- In addition, because FCIP creates a unified fabric, disruption in the underlying IP network can cause instabilities in the SAN environment. These include a segmented fabric, excessive RSCNs, and host timeouts.
- The vendors of FC switches have recognized some of the drawbacks related to FCIP and have implemented features to provide additional stability, such as the capability to segregate FCIP traffic into a separate virtual fabric.
- Security is also a consideration in an FCIP solution because the data is transmitted over public IP channels. Various security options are available to protect the data based on the router's support.
- IPSec is one such security measure that can be implemented in the FCIP environment.

➔ FCOE (FIBRE CHANNEL OVER ETHERNET)

- FCoE (Fibre Channel over Ethernet) is a storage protocol that enables Fibre Channel (FC) communications to run directly over Ethernet.

- FCoE makes it possible to move Fibre Channel traffic across existing high-speed Ethernet infrastructure and converges storage and IP protocols onto a single cable transport and interface.
- The goal of FCoE is to consolidate I/O (input/output) and reduce switch complexity, as well as to cut back on cable and interface card counts.
- Adoption of FCoE has been slow, however, due to a scarcity of end-to-end FCoE devices and a reluctance on the part of many organizations to change the way they implement and manage their networks.
- Traditionally, organizations have used Ethernet for Transmission Control Protocol/Internet Protocol (TCP/IP) networks and FC for storage networks.
- Fibre Channel supports high-speed data connections between computing devices that interconnect servers with shared storage devices and between storage controllers and drives.
- FCoE shares Fibre Channel and Ethernet traffic on the same physical cable or lets organizations separate Fibre Channel and Ethernet traffic on the same hardware.
- FCoE uses a lossless Ethernet fabric and its own frame format.
- It retains Fibre Channel's device communications but substitutes high-speed Ethernet links for Fibre Channel links between devices.

➔ FCOE SAN COMPONENTS

The key FCoE SAN components are:

- ✓ Network adapters such as Converged Network Adapter (CNA) and software FCoE adapter
- ✓ Cables such as copper cables and fiber optical cables
- ✓ FCoE switch

Converged Network Adapter (CNA)

- The CNA is a physical adapter that provides the functionality of both a standard NIC and an FC HBA in a single device.
- It consolidates both FC traffic and regular Ethernet traffic on a common Ethernet infrastructure.
- FC traffic onto Ethernet frames and forwarding them to FCoE switches over CEE links.
- They eliminate the need to deploy separate adapters and cables for FC and Ethernet communications, thereby reducing the required number of network adapters and switch ports.
- A CNA offloads the FCoE protocol processing task from the compute system, thereby freeing the CPU resources of the compute system for application processing.
- It contains separate modules for 10 Gigabit Ethernet (GE), FC, and FCoE Application Specific Integrated Circuits (ASICs).

Software FCoE Adapter

- Instead of a CNA, a software FCoE adapter may also be used. A software FCoE adapter is OS or hypervisor kernel-resident software that performs FCoE processing.

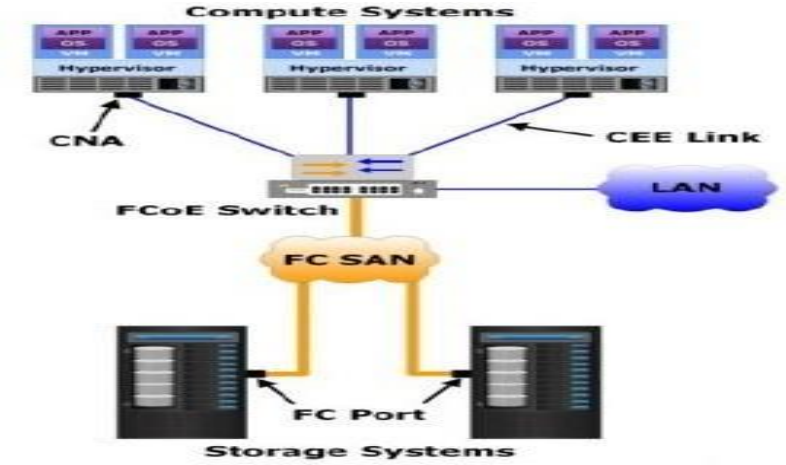
- The FCoE processing consumes hosts CPU cycles.
- With software FCoE adapters, the OS or hypervisor implements FC protocol in software that handles SCSI to FC processing.
- The software FCoE adapter performs FC to Ethernet encapsulation. Both FCoE traffic (Ethernet traffic that carries FC data) and regular Ethernet traffic are transferred through supported NICs on the hosts.

FCOE Switch

- An FCoE switch has both Ethernet switch and FC switch functionalities. It has a Fibre Channel Forwarder (FCF), an Ethernet Bridge, and a set of ports that can be used for FC and Ethernet connectivity.
- FCF handles FCoE login requests, applies zoning, and provides the fabric services typically associated with an FC switch.
- It also encapsulates the FC frames received from the FC port into the Ethernet frames and decapsulates the Ethernet frames received from the Ethernet Bridge to the FC frames.
- Upon receiving the incoming Ethernet traffic, the FCoE switch inspects the Ethertype of the incoming frames and uses that to determine their destination.
- If the Ethertype of the frame is FCoE, the switch recognizes that the frame contains an FC payload and then forwards it to the FCF.
- From there, the FC frame is extracted from the Ethernet frame and transmitted to the FC SAN over the FC ports.
- If the Ethertype is not FCoE, the switch handles the traffic as usual Ethernet traffic and forwards it over the Ethernet ports.

➔ CONVERGED ENHANCED ETHERNET (CEE) (or) (FCoE SAN CONNECTIVITY)

- FCoE SAN is a Converged Enhanced Ethernet (CEE) network that is capable of transporting FC data along with regular Ethernet traffic over high speed (such as 10 Gbps or higher) Ethernet links.



- It uses FCoE protocol that encapsulates FC frames into Ethernet frames. FCoE protocol is defined by the T11 standards committee.

- FCoE is based on an enhanced Ethernet standard that supports Data Center Bridging (DCB) functionalities (also called CEE functionalities). DCB ensures lossless transmission of FC traffic over Ethernet.
- FCoE SAN provides the flexibility to deploy the same network components for transferring both server-to-server traffic and FC storage traffic. This helps to mitigate the complexity of managing multiple discrete network infrastructures. FCoE SAN uses multi-functional network adapters and switches.
- Therefore, FCoE reduces the number of network adapters, cables, and switches, along with power and space consumption required in a data center.

Some of the CEE enhancements to Ethernet include:

Priority Flow Control: Focused on developing a standard mechanism that can control the flow for each traffic class of service independently. The idea is to ensure zero loss when a traffic class gets congested in data center bridging networks.

Data Center Bridging exchange: Focused on developing a standard mechanism that can ensure interoperability.

Priority-Based Packet Scheduling: Used to develop a standard mechanism to set scheduling priorities for a set of traffic classes.

Some of the advantages of CEE convergence include:

- CEE enhances the network-attached storage and Internet small computer interface by offering traffic differentiation at the link layer.
- Fiber channel over CEE enables new servers in the data center to use a single link for both Ethernet and fiber channel communications, thereby reducing cable costs.
- CEE technology can be used to converge a variety of applications such as local area networks, storage area networks and high-performance computing.

➔ FCoE ARCHITECTURE

- Fibre Channel over Ethernet (FCoE) is a method of supporting converged Fibre Channel (FC) and Ethernet traffic on a data center bridging (DCB) network.
- FCoE encapsulates unmodified FC frames in Ethernet to transport the FC frames over a physical Ethernet network.
- An FCoE frame is the same as any other Ethernet frame because the Ethernet encapsulation provides the header information needed to forward the frames. However, to achieve the lossless behavior that FC transport requires, the Ethernet network must conform to DCB standards.
- DCB standards create an environment over which FCoE can transport native FC traffic encapsulated in Ethernet while preserving the mandatory *class of service* (CoS) and other characteristics that FC traffic requires.
- Supporting FCoE in a DCB network requires that the FCoE devices in the Ethernet network and the FC switches at the edge of the SAN network handle both Ethernet and native FC traffic. To handle Ethernet traffic, an FC switch does one of two things:
  - ✓ Incorporates FCoE interfaces.

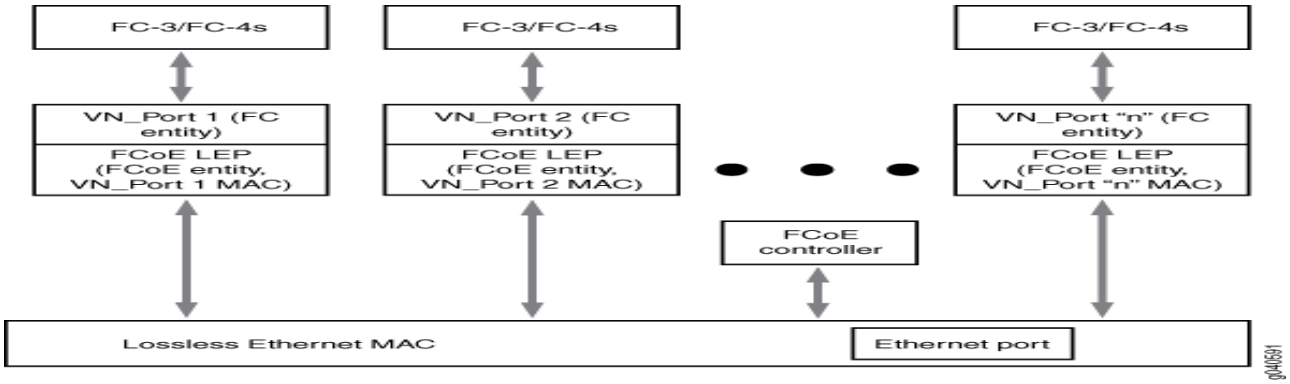
- ✓ Uses an FCoE-FC gateway such as a QFX3500 switch to de-encapsulate FCoE traffic from FCoE devices into native FC and to encapsulate native FC traffic from the FC switch into FCoE and forward it to FCoE devices through the Ethernet network.

FCoE Devices

- Each FCoE device has a converged network adapter (CNA) that combines the functions of an FC host bus adapter (HBA) and a lossless Ethernet network interface card (NIC) with 10-Gbps Ethernet ports.
- The portion of the CNA that handles FCoE traffic is called an FCoE Node (ENode). An ENode combines FCoE termination functions and the client part of the FC stack on the CNA.
- ENodes present virtual FC interfaces to FC switches in the form of virtual N_Ports (VN_Ports). A VN_Port is an endpoint in a virtual point-to-point connection called a virtual link.
- The other endpoint of the virtual link is an FC switch (or FCF) port. A VN_Port emulates a native FC N_Port and performs similar functions: handling the creation, detection, and flow of messages to and from the FC switch.
- A single ENode can host multiple VN_Ports. Each VN_Port has a separate, unique virtual link with a FC switch.
- ENodes contain at least one lossless Ethernet media access controller (MAC). Each Ethernet MAC is paired with an FCoE controller. The lossless Ethernet MAC is a full-duplex Ethernet MAC that implements Ethernet extensions to avoid frame loss due to congestion and supports frames of at least 2500 bytes.
- The FCoE controller instantiates and terminates VN_Port instances dynamically as they are needed for FCoE sessions. Each VN_Port instance has a unique virtual link to an FC switch.
- Nodes also contain one FCoE link end point (LEP) for each VN_Port connection. An FCoE LEP is a virtual FC interface mapped onto the physical Ethernet interface.
- An FCoE LEP:
  - ✓ Transmits and receives FCoE frames on the virtual link.
  - ✓ Handles FC frame encapsulation for traffic going from the server to the FC switch.
  - ✓ Performs frame de-encapsulation of traffic received from the FC switch.

Figure 1 shows a block diagram of the major ENode components.

ENodeComponents



FCoE Frames

- The FCoE protocol specification replaces the FC0 and FC1 layers of the FC stack with Ethernet, but retains the FC frame header. Retaining the FC frame header enables the FC frame to pass directly to a native FC SAN after de-encapsulation.
- The FCoE header carries the FC start of file (SOF) bits and end of file (EOF) bits in an encoded format. FCoE supports two frame types, control frames and data frames. FCoE Initialization Protocol (FIP) carries all of the discovery and fabric login frames.
- FIP control frames handle FCoE device discovery, initializing communication, and maintaining communication.
- They do not carry a data payload. FIP has its own EtherType (0x8914) to distinguish FIP traffic from FCoE traffic and other Ethernet traffic.
- To establish communication, the ENode uses the globally unique MAC address assigned to it by the CNA manufacturer.
- After FIP establishes a connection between FCoE devices, the FCoE data frames handle the transport of the FC frames encapsulated in Ethernet.
- FCoE also has its own EtherType (0x8906) to distinguish FCoE frames from other Ethernet traffic and ensure the in-order frame handling that FC requires. FCoE frames include:
    - ✓ 2112 bytes FC payload
    - ✓ 24 bytes FC header
    - ✓ 14 bytes standard Ethernet header
    - ✓ 14 bytes FCoE header
    - ✓ 8 bytes cyclic redundancy check (CRC) plus EOF
    - ✓ 4 bytes VLAN header
    - ✓ 4 bytes frame check sequence (FCS)
- The payload, headers, and checks add up to 2180 bytes. Therefore, interfaces that carry FCoE traffic should have a configured maximum transmission unit (MTU) of 2180 or larger. An MTU size of 2180 bytes is the minimum size; some network administrators prefer an MTU of 2240 or 2500 bytes.

Virtual Links

- Native FC uses point-to-point physical links between FC devices. In FCoE, virtual links replace the physical links.

- A virtual link emulates a point-to-point link between two FCoE device endpoints, such as a server VN_Port and an FC switch (or FCF) VF_Port.
- Each FCoE interface can support multiple virtual links.
- The MAC addresses of the FCoE endpoints (the VN_Port and the VF_Port) uniquely identify each virtual link and allow traffic for multiple virtual links to share the same physical link while maintaining data separation and security.
- A virtual link exists in one FCoE VLAN and cannot belong to more than one VLAN. Although the FC switch and the FCoE device detect a virtual link as a point-to-point connection, virtual links do not need to be direct connections between a VF_Port and a VN_Port.
- A virtual link can traverse one or more transit switches, also known as passthrough switches.
- A transit switch can transparently aggregate virtual links while still appearing and functioning as a point-to-point connection to the FCoE devices. However, a virtual link must remain within a single Layer 2 domain.

FCoE VLANs

- All FCoE traffic must travel in a VLAN dedicated to transporting only FCoE traffic. Only FCoE interfaces should be members of an FCoE VLAN. Ethernet traffic that is not FCoE or FIP traffic must travel in a different VLAN.
- FCoE traffic cannot use a standard LAG because traffic might be hashed to different physical LAG links on different transmissions. This breaks the (virtual) point-to-point link that Fibre Channel traffic requires.
- If you configure a standard LAG interface for FCoE traffic, FCoE traffic might be rejected by the FC SAN.

UNIT IV
BACKUP, ARCHIVE AND REPLICATION

Introduction to Business Continuity, Backup architecture, Backup targets and methods, Data deduplication, Cloud-based and mobile device backup, Data archive, Uses of replication and its characteristics, Compute based, storage-based, and network-based replication, Data migration, Disaster Recovery as a Service (DRaaS).

➔ INTRODUCTION TO BUSINESS CONTINUITY :

- Continuous access to information is a must for the smooth functioning of business operations today, as the cost of business disruption could be catastrophic.
- There are many threats to information availability, such as natural disasters (e.g., flood, fire, earthquake), unplanned occurrences (e.g., cybercrime, human error, network and com- puter failure), and planned occurrences (e.g., upgrades, backup, restore) that result in the inaccessibility of information.
- It is critical for businesses to define appropriate plans that can help them overcome these crises. *Business continuity is an important process to define and implement these plans.*

Business continuity (BC) **is an integrated and enterprisewide process that includes all activities (internal and external to IT) that a business must perform to mitigate the impact of planned and unplanned downtime**.

BC entails preparing for, responding to, and recovering from a system outage that adversely affects business operations. It involves proactive measures, such as business impact analysis and risk assessments, data protection, and security, and reactive countermeasures, such as disaster recovery and restart, to be invoked in the event of a failure. The goal of a business continuity solution is to ensure the “information availability” required to conduct vital business operations.

INFORMATION AVAILABILITY

➢ *Information availability (IA)* refers to the ability of the infrastructure to function according to business expectations during its specified time of operation. Information availability ensures that people (employees, customers, suppliers, and partners) can access information whenever they need it.

Information availability can be defined with the help of reliability, accessibility and timeliness.

Reliability: This reflects a component's ability to function without failure, under stated conditions, for a specified amount of time.

Accessibility: This is the state within which the required information is accessible at the right place, to the right user. The period of time during which the system is in an accessible state is termed *system uptime;* when it is not accessible it is termed *system downtime.*

Timeliness: Defines the exact moment or the time window (a particular time of the day, week, month, and/or year as specified) during which information must be accessible.

For example, if online access to an application is required between 8:00 AM and 10:00 PM each day, any disruptions to data availability outside of this time slot are not considered to affect timeliness.

Causes of Information Unavailability

- Various planned and unplanned incidents result in data unavailability.
  - ✓ *Planned outages* include installation/integration/maintenance of new hardware, soft- ware upgrades or patches, taking backups, application and data restores,facility operations (renovation and construction), and refresh/migration of the testing to the production environment.
  - ✓ *Unplanned outages* include failure caused by database corruption, component failure, and human errors.
- Another type of incident that may cause data unavailability is natural or man-made disasters such as flood, fire, earthquake, and contamination.
- As illustrated in Figure 11-1, the majority of outages are planned. Planned outages are expected and scheduled, but still cause data to be unavailable.
  Statistically, less than 1 percent is likely to be the result of an unforeseen disaster.

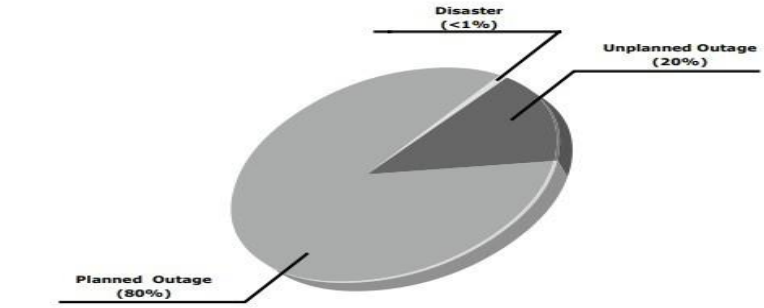


Figure 11-1: Disruptors of data availability

Measuring Information Availability

- Information availability relies on the availability of the hardware and software components of a data center. Failure of these components might disrupt informa- tion 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 action, such as a manual reboot, a repair, or replacement of the failed component(s).
- Repair involves restoring a component to a condition that enables it to perform a required function within a specified time by using procedures and resources.
- 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 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.

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 identified and that the required spares and personnel are available.

MTTR includes the time required to do the following: detect the fault, mobilize the maintenance team, diagnose the fault, obtain the spare parts, repair, test, and resume normal operations.

- **IA is the fraction of a time period that a system is in a condition to perform its intended function upon demand. It can be expressed in terms of system uptime and downtime and measured as the amount or percentage of system uptime:**

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

In terms of MTBF and MTTR, IA could also be expressed as

IA = MTBF / (MTBF + MTTR)

Table 11-1 lists the approximate amount of downtime allowed for a service to achieve certain levels of 9s availability.

For example, a service that is said to be "five 9s available" is available for 99.999 percent of the scheduled time in a year (24 × 7 × 365).

Table 11-1: Availability Percentage and Allowable Downtime

UpTIme (%)	DownTIme (%)	DownTIme per Year	DownTIme per week
98	2	7.3 days	3 hr 22 minutes
99	1	3.65 days	1 hr 41 minutes
99.8	0.2	17 hr 31 minutes	20 minutes 10 sec
99.9	0.1	8 hr 45 minutes	10 minutes 5 sec
99.99	0.01	52.5 minutes	1 minute
99.999	0.001	5.25 minutes	6 sec
99.9999	0.0001	31.5 sec	0.6 sec

Consequences of Downtime

- Data unavailability, or downtime, results in loss of productivity, loss of revenue, poor financial performance, and damages to reputation.
- *Loss of produc tivity* reduces the output per unit of labor, equipment, and capital.
- *Loss of revenue* includes direct loss, compensatory payments, future revenue losses, billing losses, and investment losses.
- *Poor financial performance* affects revenue recognition, cash flow, discounts, payment guarantees, credit rating, and stock price.

An important metric, *average cost of downtime per hour*, provides a key estimate in determining the appropriate BC solutions.

It is calculated as follows:

Average cost of downtime per hour = average productivity loss per hour + average revenue loss per hour

Where:

Productivity loss per hour = (total salaries and benefits of all employees per week) / (average number of working hours per week)

Average revenue loss per hour = (total revenue of an organization per week) / (average number of hours per week that an organization is open for business)

Common terms of BC

- **Disaster recovery:** This is the coordinated process of restoring systems, data, and the infrastructure required to support key ongoing business operations in the event of a disaster.
- **Disaster restart:** This is the process of restarting business operations with mirrored consistent copies of data and applications.
- **Recovery-Point Objective (RPO):** This is the point in time to which sys tems and data must be recovered after an outage. It defines the amount of data loss that a business can endure.
  - For example, if the RPO is six hours, backups or replicas must be made at least once in 6 hours.

    Figure 11-2 shows various RPOs and their corresponding ideal recovery strategies. For example:

    RPO of 24 hours: This ensures that backups are created on an offsite tape drive every midnight.

    RPO of 1 hour: This ships database logs to the remote site every hour.

    RPO of zero: This mirrors mission-critical data synchronously to a remote site.
- **Recovery-Time Objective (RTO):** The 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.

  For example, if the RTO is two hours, then use a disk backup because it enables a faster restore than a tape backup.

  Some examples of RTOs and the recovery strategies to ensure data availability are

listed below

- **RTO of 72 hours:** Restore from backup tapes at a cold site.
- **RTO of 12 hours:** Restore from tapes at a hot site.
- **RTO of 4 hours:** Use a data vault to a hot site

BC PLANNING LIFECYCLE

- BC planning must follow a disciplined approach like any other planning process. Organizations today dedicate specialized resources to develop and main tain BC plans.
- The BC planning life cycle includes five stages (see Figure 11-3):

1. Establishing objectives
2. Analyzing
3. Designing and developing
4. Implementing
5. Training, testing, assessing, and maintaining

Figure 11-3: 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, infra- structure 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 modi- fication 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.

➔ BACKUP PROCESS (BACKUP ARCHITECTURE)

- A backup system uses 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 process and backup metadata. The backup server depends on backup clients to gather the data to be backed up.
- The backup clients can be local to the server or they can reside on another server, presumably to back up the data visible to that server. The backup server receives backup metadata from the backup clients to perform its activities.
- Figure 12-4 illustrates the backup process.
- The storage node is responsible for writing data to the backup device (in a backup environment, a storage node is a host that controls backup devices). Typically, the storage node is integrated with the backup server and both are hosted on the same physical platform.
- A backup device is attached directly to the storage node's host platform. 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.
- The backup process is based on the policies defined on the backup server, such as the time of day or completion of an event. The backup server then initiates the process by sending a request to a backup client (backups can also be initiated by a client). This request instructs the backup client to send its metadata to the backup server, and the data to be backed up to the appropriate storage node. On receiving this request, the backup client sends the metadata to the backup server.
- The backup server writes this metadata on its metadata catalog. The backup client also sends the data to the storage node, and the storage node writes the data to the storage device.
- After all the data is backed up, the storage node closes the connection to the backup device. The backup server writes backup completion status to the metadata catalog.

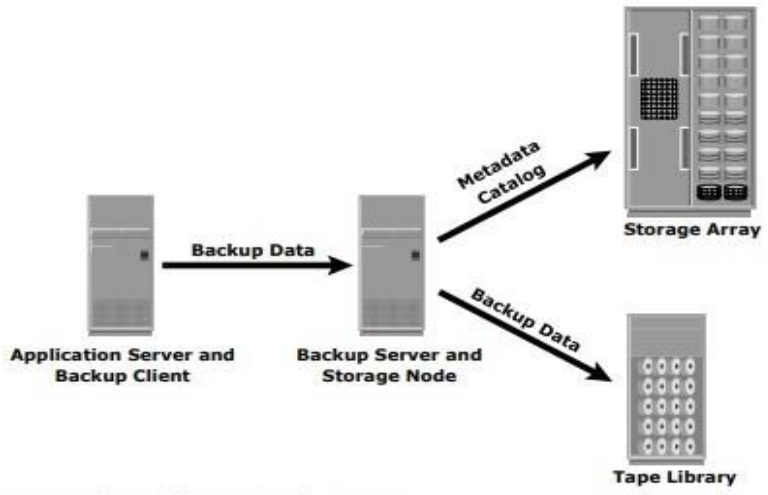


Figure 12-4: Backup architecture and process

- Backup software also provides extensive reporting capabilities based on the backup catalog and the log files. These reports can include information such as the amount of data backed up, the

number of completed backups, the number of incomplete backups, and the types of errors that may have occurred. Reports can be customized depending on the specific backup software used.

➔ 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.
- The backup of online production data becomes more challenging because data is actively being used and changed. An open file is locked by the operating system and is not copied during the backup process until the user closes it.
- The backup application can back up open files by retrying the operation on files that were opened earlier in the backup process. During the backup process, it may be possible that files opened earlier will be closed and a retry will be successful.
- The maximum number of retries can be configured depending on the backup application. However, this method is not considered robust because in some environments certain files are always open.
- In such situations, the backup application provides open file agents. These agents interact directly with the operating system and enable the creation of consistent copies of open files. In some environments, the use of open file agents is not enough.
- For example, a database is composed of many files of varying sizes, occupying several file systems. To ensure a consistent database backup, all files need to be backed up in the same state. That does not necessarily mean that all files need to be backed up at the same time, but they all must be synchronized so that the database can be restored with consistency.
- Consistent backups of databases can also be done by using a cold backup. This requires the database to remain inactive during the backup. Of course, *the disadvantage of a cold backup is that the database is inaccessible to users during the backup process.*
- Hot backup is used in situations where it is not possible to shut down the database. This is facilitated by database backup agents that can perform a backup while the database is active. *The disadvantage associated with a hot backup is that the agents usually affect overall application performance.*
- 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.

- A pointer-based PIT copy consumes only a fraction of the storage space and can be created very quickly. A pointer-based PIT copy is implemented in a disk-based solution whereby a virtual LUN is created and holds pointers to the data stored on the production LUN or save location.
- In this method of backup, the database is stopped or frozen momentarily while the PIT copy is created. The PIT copy is then mounted on a secondary server and the backup occurs on the primary server.
- To ensure consistency, it is not enough to back up only production data for recovery. Certain attributes and properties attached to a file, such as permissions, owner, and other metadata, also need to be backed up.
- These attributes are as important as the data itself and must be backed up for consistency. Backup of boot sector and partition layout information is also critical for successful recovery.
- In a disaster recovery environment, bare-metal recovery (BMR) refers to a backup in 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 first, before starting the recovery of data files. Some BMR technologies can recover a server onto dissimilar hardware.

➔ DATA DEDUPLICATION :

- Data deduplication emerged as a key technology to dramatically reduce the amount of space and the cost that are associated with storing large amounts of data. Data deduplication is the art of intelligently reducing storage needs in order of magnitude.
- This method is better than common data compression techniques.
- Data deduplication works through the elimination of redundant data so that only one instance of a data set is stored. IBM has the broadest portfolio of data deduplication solutions in the industry, which gives IBM the freedom to solve client issues with the most effective technology.
- Whether it is source or target, inline or post, hardware or software, disk or tape, *IBM has a solution with the technology that best solves the problem:*

  IBM ProtecTIER® Gateway and Appliance

  IBM System Storage N series Deduplication

  IBM Tivoli Storage Manager
- Data deduplication is a technology that reduces the amount of space that is required to store data on disk. It achieves this space reduction by storing a single copy of data that is backed up repetitively.

- Data deduplication products read data while they look for duplicate data. Data deduplication products break up data into elements and create a signature or identifier for each data element.
- Then, they compare the data element signature to identify duplicate data. After they identify duplicate data, they retain one copy of each element. They create pointers for the duplicate items, and discard the duplicate items.
- The effectiveness of data deduplication depends on many variables, including the rate of data change, the number of backups, and the data retention period.
- For example, if you back up the same incompressible data one time a week for six months, you save the first copy and you do not save the next 24. This method provides a 25:1 data deduplication ratio. If you back up an incompressible file on week one, back up the exact same file again on week two, and never back it up again, this method provides a 2:1 data deduplication ratio.
- A more likely scenario is that a portion of your data changes from backup to backup so that your data deduplication ratio changes over time.
- With data deduplication, you can minimize your storage requirements. Data deduplication can provide greater data reduction and storage space savings than other existing technologies.

Figure 6-13 shows the concept of data deduplication.

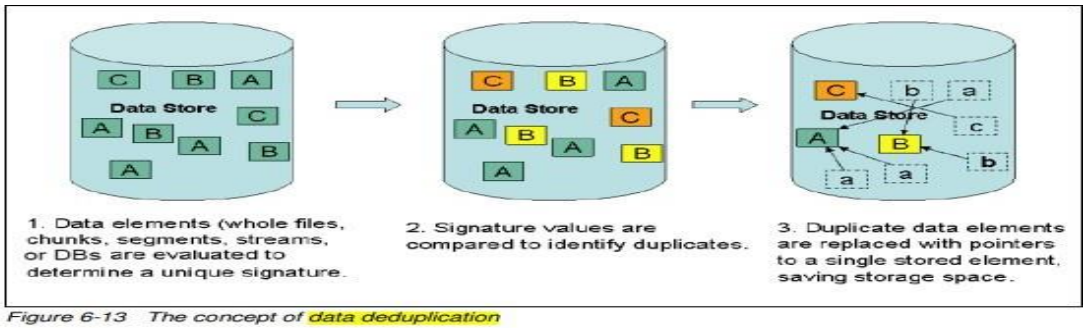


Figure 6-13 The concept of data deduplication

- Data deduplication can reduce your storage requirements but the benefit you derive is determined by your data and your backup policies. Workloads with a high database content have the highest data deduplication ratios.
- However, product functions, such as IBM Tivoli Storage Manager Progressive Incremental or Oracle Recovery Manager (RMAN), can reduce the data deduplication ratio.
- Compressed, encrypted, or otherwise scrambled workloads typically do not benefit from data deduplication.
- Good candidates for data deduplication are text files, log files, uncompressed and non-encrypted database files, email files (PST, DBX, and IBM Domino®), and Snapshots (Filer Snaps, BCVs, and VMware images).

Types of data deduplication and IBM HyperFactor

- Many vendors offer data deduplication products.
- Various methods are available to deduplicate data.
- The following *three methods* are used frequently for data deduplication:
  - ✓ **Hash-based data deduplication** uses a hashing algorithm to identify chunks of data. Secure Hash Algorithm 1 (SHA-1) or Message-Digest Algorithm 5 (MDA-5) is commonly used. The details of each technique are beyond the intended scope of this publication.
  - ✓ **Content-aware data deduplication** methods are aware of the structure of common patterns of data that is used by applications. The content-aware data deduplication method assumes that the best candidate to deduplicate against is an object with the same properties, such as a file name. When a file match is identified, a bit-by-bit comparison is performed to determine whether data changed and the changed data is saved.
  - ✓ **IBM HyperFactor®** is a patented technology that is used in the IBM System Storage ProtecTIER Enterprise Edition and higher software. HyperFactor takes an approach that reduces the phenomenon of missed factoring opportunities, providing a more efficient process. HyperFactor data deduplication uses a 4 GB Memory Resident Index to track similarities for up to 1 petabyte (PB) of physical disk in a single repository.

    HyperFactor technology uses a pattern algorithm that can reduce the amount of space that is required for storage by up to a factor of 25, based on evidence from existing implementations.

Figure 6-14 shows the HyperFactor technology.

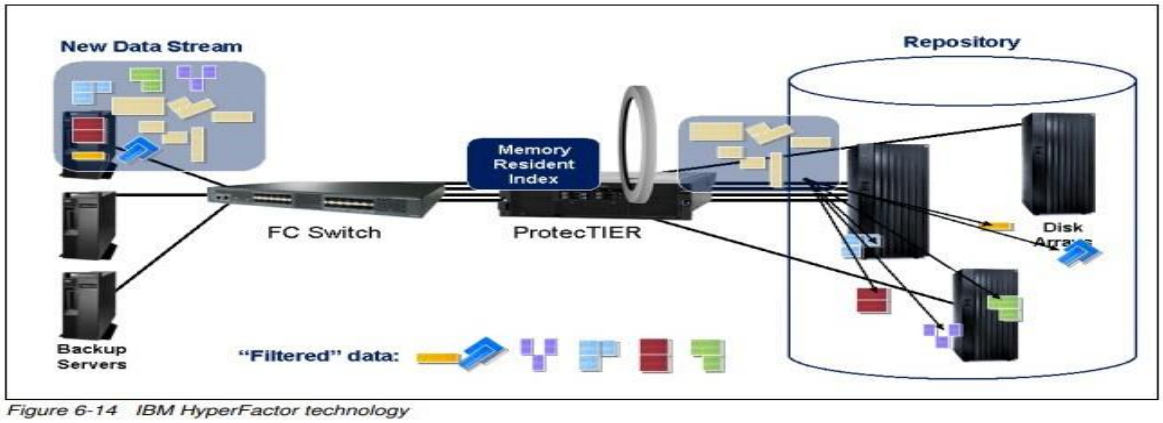


Figure 6-14 IBM HyperFactor technology

Data deduplication processing

- Data deduplication can either occur while the data is backed up to the storage media (real-time or inline) or after the data is written to the storage media (post-processing). Each method contains positive and negative aspects.
- These considerations must be evaluated by the engineer or technical specialist that is responsible for the concrete solution architecture and deployment. IBM decided to use inline data

deduplication processing because it offers larger target storage space without any need of a temporary disk cache pool for post-processed deduplication data.

- Bit comparison techniques, such as the technique that is used by ProtecTIER, were designed to provide 100% data integrity by avoiding the risk of hash collisions.

➔ CLOUD BASED AND MOBILE DEVICE BACKUP

CLOUD BACKUP

- Cloud backup, also known as *online backup* or *remote backup*, is a strategy for sending a Copy of a physical or virtual file or database to a secondary, off-site location for preservation in case of equipment failure, site catastrophe or human malfeasance.
- The backup server and data storage systems are usually hosted by a third-party cloud or SaaS provider that charges the backup customer a recurring fee based on storage space or capacity used, data transmission bandwidth, number of users, number of servers or number of times data is retrieved.
- Implementing cloud data backup can help bolster an organization's data protection, business continuance and regulatory compliance strategies without increasing the workload of IT staff.

➢ There are a variety of approaches to cloud backup, with available services that can easily fit into an organization's existing data protection process. *Varieties of cloud backup include the following:*

Backing up directly to the public cloud.

- One way to store organizational workloads is by duplicating resources in the public cloud. This method entails writing data directly to cloud providers, such as AWS, Google Cloud or Microsoft Azure.
- The organization uses its own backup software to create the data copy to send to the cloud storage service. The cloud storage service then provides the destination and safekeeping for the data, but it doesn't specifically provide a backup application.
- In this scenario, it's important that the backup software is capable of interfacing with the cloud's storage service.
- Additionally, with public cloud options, IT professionals might need to look into supplemental data protection procedures, such as data encryption as well as identity and access management to secure backed up data.

Backing up to a service provider.

- In this scenario, an organization writes data to a cloud service or SaaS provider that offers backup services in a managed data center.
- The backup software that the company uses to send its data to the service might be provided as part of the service, or the service might support specific commercially available backup applications.

Choosing a cloud-to-cloud (C2C) backup.

- These services are among the newest offerings in the cloud backup arena. They specialize in backing up data that already lives in the cloud, either as data created using a SaaS application or as data stored in a cloud backup service.
- As its name suggests, a C2C backup service copies data from one cloud to another cloud. The cloud-to-cloud backup service typically hosts the software that handles this process.

Using online cloud backup systems.

- There are also hardware alternatives that facilitate backing up data to a cloud backup service. These appliances are all-in-one backup machines that include backup software and disk capacity, along with the backup server.
- The appliances are about as close to plug-and-play as backup gets, and most of them also provide a seamless link to one or more cloud backup services or cloud providers.
- The list of vendors that offer backup appliances that include cloud interfaces is long, with Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft and Asigra active in this arena.
- These appliances typically retain the most recent backup locally, in addition to copying it to the cloud backup provider, so any required recoveries can be made from the local backup copy, saving time and transmission costs.

How data is restored

- Cloud backup services are typically built around a client software application that runs on a schedule determined by the purchased level of service and the customer's requirements.
- For example, if the customer has contracted for daily backups, the application collects, compresses, encrypts and transfers data to the cloud service provider's servers every 24 hours. To reduce the amount of bandwidth consumed and the time it takes to transfer files, the service provider might only provide incremental backups after the initial full backup.
- Cloud backup services often include the software and hardware necessary to protect an organization's data, including applications for Microsoft Exchange and SQL Server.
- Whether a customer uses its own backup application or the software the cloud backup service provides, the organization uses that same application to restore backed up data.

Cloud backup vs. cloud storage

- Although they share similarities, cloud backup and cloud storage aren't the same thing.
- Cloud storage is a service model in which data is stored on remote systems. Data in cloud storage is available to users over a network, typically the internet.
  Benefits of cloud storage include global availability, ease of use and off-site security. Potential drawbacks range from performance issues depending on network connection, to loss of complete control over the data, to escalating costs over time.
- Cloud backup is a service that sends an extra copy of an organization's data over a network to an off-site server, the typical user shouldn't need to access that data on a regular basis.

How does Cloud Backup Work?

- Cloud backup copies and stores data from a computer or other computing device to remote servers maintained by a cloud storage provider. For security reasons, the data is encrypted

and delivered via the internet, guaranteeing that only authorized users may access the backup data.

Here's how cloud backup actually works:

Installation

The first step is to install the cloud backup software on the device or devices that will be backed up. Typically, the steps will walk you through the setup process and assist you in configuring backup choices such as which data should be saved and how frequently should backups be performed.

Backup

Once the cloud backup software is installed, it will automatically copy and store your data on the remote servers.

This process is typically performed in the background, so you can continue to use your device while the backup is in progress.

Encryption

Data is encrypted before it is delivered over the internet to guarantee that it is safe from illegal access. The encryption method employs a one-of-a-kind key produced by the cloud backup program, and only the user has access to it.

Storage

After the data has been backed up, it is stored on remote servers operated by the cloud storage provider. The data is kept in a safe, off-site location, which adds an extra degree of security against data loss due to hardware failure, theft, or other sorts of calamities.

Recovery

To restore your data, just log into the cloud backup service and choose the files you want to recover. The data will subsequently, be sent from distant servers to your device. This technique is often quick and simple, and it does not require physical storage media or particular technological knowledge.

MOBILE DEVICE BACKUP

Back up or restore data on your Android device

- You can back up content, data, and settings from your phone to your Google Account. You can restore your backed up information to the original phone or to some other Android phones.
- You can't use back up when you set up a personal device with a work profile or for work only, or when you set up a company-owned device.
- Restoring data varies by phone and Android version. You can't restore a backup from a higher Android version onto a phone running a lower Android version.

Where your phone data is stored

- Backups are uploaded to Google servers and they're encrypted with your Google Account password. For some data, your phone's screen lock PIN, pattern, or password is also used to encrypt your data so it can be backed up safely.

Your backup data (except what you back up to Google Photos) is erased if:

- You don't use your device for 57 days

- You turn off Android backup

Back up content

1. Back up photos and videos.
2. Back up files and folders.

Automatically back up your phone

- To help protect your backed-up data, use a PIN, pattern, or password screen lock, instead of a swipe or Smart Lock.
- You can set up your device to automatically back up your files.

1. Open your device's Settings app.
2. Select **Google** › **Backup**.
   Tip: If this is your first time, turn on **Backup by Google One** and follow the on-screen instructions.
3. Tap **Back up now**.

Your Google One backup can take up to 24 hours. When your data is saved, "On" will be below the data types you selected.

Erase after backing up

- After you back up, you can reset your device by erasing everything on it.

Get your data onto a new phone

- When you add your Google Account to a phone that's been set up, what you'd previously backed up for that Google Account gets put onto the phone.
- To restore a backed-up account to a reset phone, follow the on-screen steps. For more help, get help from your device manufacturer.
- Your photos and videos are already available in Google Photos. But you can restore the rest of the data you backed up while you set up your new phone for the first time or after a factory reset.
- At setup, to restore your data, follow the on-screen steps.The process can take up to 24 hours.

How Backup handles your data

- The data that backup collects is encrypted in transit.
- Backup sends your data to Google's backup servers and helps you transfer data between devices. Backup collects certain information to perform services on your device. Some of this functionality uses Google Play services.
- For example, backup collects:
  Messages, contacts, app settings, and preferences are collected as part of your personal backup.
  Personal identifiers are collected to ensure that your backups are associated with you and your account.
  Crash logs and diagnostics are collected for analytics and troubleshooting purposes.

➔ DATA ARCHIVE :

An electronic data archive is a repository for data that has fewer access requirements.

Types of Archives :

It can be implemented as online, nearline, or offline based on the means of access:

■ **Online archive**: The storage device is directly connected to the host to make the data immediately available. This is best suited for active archives.

■ **Nearline archive**: The storage device is connected to the host and infor- mation is local, but the device must be mounted or loaded to access the information.

■ **Offline archive**: The storage device is not directly connected, mounted, or loaded. Manual intervention is required to provide this service before information can be accessed.

- An archive is often stored on a write once read many (WORM) device, such as a CD-ROM. These devices protect the original file from being overwritten. Some tape devices also provide this functionality by implementing file locking capabilities in the hardware or software.
- Although these devices are inexpensive, they involve operational, management, and maintenance overhead.
- Requirements to retain archives have caused corporate archives to grow at a rate of 50 percent or more per year. At the same time, organizations must reduce costs while maintaining required service-level agreements (SLAs). Therefore, it is essential to find a solution that minimizes the fixed costs of the archive's operations and management.
- Archives implemented using tape devices and optical disks involve many hidden costs.
- The traditional archival process using optical disks and tapes is not optimized to recognize the content, so the same content could be archived several times.
- Additional costs are involved in offsite storage of media and media management. Tapes and optical media are also susceptible to wear and tear. Frequent changes in these device technologies lead to the overhead of converting the media into new formats to enable access and retrieval.
- Government agencies and industry regulators are establishing new laws and regulations to enforce the protection of archives from unauthorized destruction and modification.
- These regulations and standards affect all businesses and have established new requirements for preserving the integrity of information in the archives.
- These requirements have exposed the hidden costs and shortcomings of the traditional tape and optical media archive solutions

➔ REPLICATION :

- Replication is the process of creating an exact copy of data. Creating one or more replicas of the production data is one of the ways to provide Business Continuity (BC).
- *Data replication*, where the same data is stored on multiple storage devices

Benefits of Data Replication

Data replication can be a cost-demanding process/operation in terms of computing power and storage requirements, but it provides an immense set of benefits that overshadow the cost aspect. *Some of the benefits of data replication are as follows:*

- **High Data Availability:** Data replication mechanisms ensures high availability and accessibility of the data by allowing users or applications to access the data from numerous nodes or sites even during an unforeseen failure or technical glitch. It stores data across multiple locations and thus enhances the reliability of systems.
- **Enhanced Data Retrieval:** With data replication in place, users can access data from a diverse set of regions/locations. With data available across different storage locations, data replication reduces latency and allows users to access data from a nearby data replica.
- **Enhanced Server Performance:** Data replication helps reduce the load on the primary server by distributing data across numerous storage regions/locations, thereby boosting the network performance.
- **Fault tolerance & Disaster Recovery:** With the rapid growth in the number of cyberattacks, data breaches, etc., most organizations face the issue of unexpected losses.

Uses of Data Replication

- One common use of data replication is for disaster recovery, to ensure that an accurate backup exists at all times in case of a catastrophe, hardware failure, or a system breach where data is compromised.
- Having a replica can also make data access faster, especially in organizations with a large number of locations.

➔ COMPUTE BASED, STORAGE-BASED, AND NETWORK-BASED REPLICATION :

STORAGE-BASED REPLICATION (REPLICATION STORAGE)

- Replication Storage, also known as storage-based replication, is an approach to replicating data available over a network to numerous distinct storage locations/regions.
- It enhances the availability, accessibility, and retrieval speed of data by allowing users to access data in real-time from various storage locations when unexpected failures occur at the source storage location.

- Storage-based data replication makes use of software installed on the storage device to handle the replication.

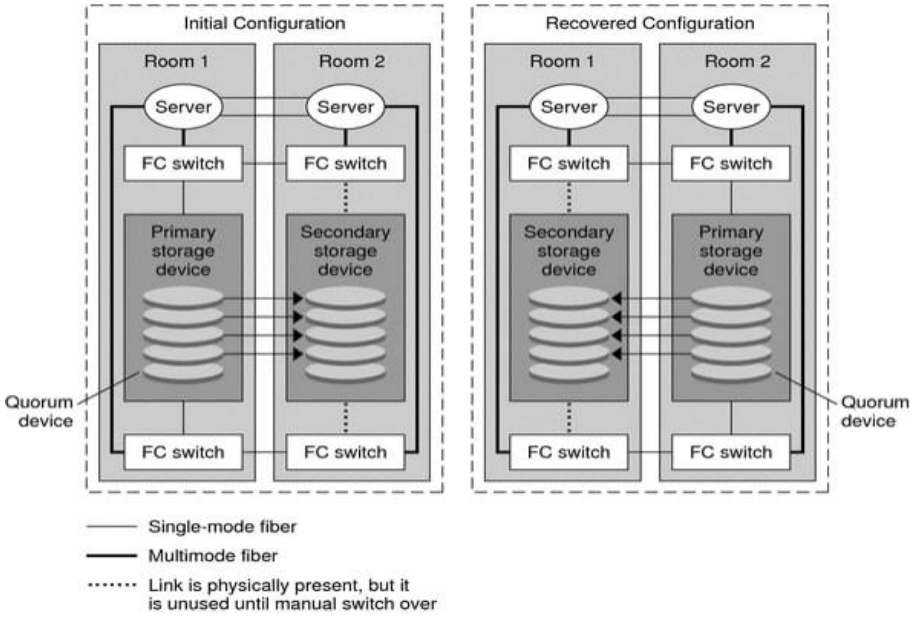


Image Source

- Storage system-based replication supports both local and remote replication.
- In storage system-based local replication, the data replication is carried out within the storage system.
- Local replication enables you to perform recovery operations in the event of data loss and also provides support for backup.
- Whereas in storage system-based remote replication, the replication is carried out between storage systems. In simple words, one of the storage systems is on the source site and the other storage system is on a remote site for data replication.
- Data can be transmitted between the two storage systems over a shared or dedicated network.

Advantages of Storage-Based Replication

- Storage-based replication follows a heterogenous storage mechanism and hence houses support for numerous platforms.
- It operates independently of any server or storage-based device.
- It allows replicating data across multi-vendor products.

Disadvantages of Storage-Based Replication

- Setting up storage-based replication requires you to leverage proprietary hardware and hence, it has a high initial setup, operational, and management cost.
- It requires setting up and implementing a storage area network (SAN).

HOST-BASED DATA REPLICATION (COMPUTE BASED)

- Host-based data replication uses the servers to copy data from one site to another site. Host-based replication software usually includes options like compression, encryption and, throttling, as well as failover.

Advantages of Host-Based Replication

- Flexible: It can leverage existing IP networks
- Can be customized to your business' needs: You can choose what data to replicate
- Can create a schedule for sending data: allows you to throttle bandwidth
- Can use any combination of storage devices on each end

Disdvantages of Host-Based Replication

- Difficult to manage with a large group of servers if there is no centralized management console
- Consumes host resources during replication
- Both storage devices on each end need to be active, which means you will need to purchase dedicated hardware and OS
- Not all applications can support this type of data replication
- Can be affected by viruses or application failure

Use-Cases of Host-Based Replication

- Host-based replication finds application in various scenarios where organizations require flexible and granular control over data replication.
- Some common use cases include:

Application-specific replication: Host-based replication allows organizations to replicate specific applications or databases, ensuring data consistency and availability. For example, a company running a critical database application may utilize host-based replication to replicate the database to a secondary site for disaster recovery purposes.

Virtual machine replication: In virtualized environments, host-based replication is commonly used to replicate virtual machines (VMs) to remote hosts or data centers. This ensures VM availability in case of host failures or enables migration of VMs for load balancing purposes.

File and folder replication: Host-based replication enables the replication of specific files, directories, or folders based on predefined rules or policies. This is useful for organizations that need to replicate specific data sets, such as project files, user home directories, or shared folders, to remote locations for backup or collaboration purposes.

Cross-platform replication: Host-based replication offers the advantage of supporting heterogeneous environments, allowing replication between different operating systems and file systems. This is beneficial for organizations with mixed IT environments that require replication between Windows, Linux, or Unix-based hosts.

Data migration and consolidation: Host-based replication can be used for data migration or consolidation projects. It allows organizations to replicate data from multiple sources to a centralized target host or storage infrastructure. This is useful during system upgrades, data center migrations, or storage platform transitions.

Content distribution and caching: Host-based replication is employed in content delivery networks (CDNs) or caching solutions to distribute content closer to end-users. By replicating content from a central server to edge servers located in different regions, organizations can achieve faster content delivery, reduced latency, and improved user experience.

High availability and disaster recovery: Host-based replication plays a crucial role in providing high availability and disaster recovery solutions. By replicating data and applications to

remote sites or backup locations, organizations can ensure continuous operations and minimize downtime in the event of hardware failures, natural disasters, or other disruptions.

NETWORK-BASED DATA REPLICATION

- Network-based replication is a data replication technique that operates at the network layer. It involves replicating data between source and target systems over a network infrastructure. Unlike array-based or host-based replication, network-based replication is not tightly coupled to storage arrays or hosts but focuses on replicating data at the network level.
- In network-based replication, data is captured and replicated at the application or file system level. It intercepts the input/output (I/O) operations at the network layer, captures the changes made to data, and replicates them to the target system.
- This replication method allows for the replication of specific files, folders, or even individual application transactions.
- Network-based replication can be synchronous or asynchronous.
- In synchronous replication, the data changes are replicated to the target system immediately after they occur on the source system, ensuring a consistent copy of the data at all times.
- This method provides a higher level of data integrity but may introduce some latency due to the delay in acknowledging the write operation until the data is replicated.
- Asynchronous replication, on the other hand, introduces a slight delay between the data changes on the source and their replication to the target system. This delay allows for increased distance between the source and target systems, as well as a higher tolerance for network latency.
- Asynchronous replication is suitable for scenarios where minimal data loss is acceptable, and the focus is on optimizing performance and network utilization.
- Network-based data replication uses a device or appliance that sits on the network in the path of the data to manage replication.
- The data is then copied to a second device. These devices usually have proprietary replication technology but can be used with any host server and storage hardware.

Advantages of network-based data replication:

- Effective in large, heterogeneous storage and server environments
- Supports any host platform and works with any array
- Works separately from the servers and the storage devices
- Allows replication between multi-vendor products

Disadvantages of network-based data replication:

- Higher initial set-up cost because it requires proprietary hardware, as well as ongoing operational and management costs
- Requires implementation of a storage area network (SAN)

Use-Cases of Network-Based Replication

- Network-based replication offers several use cases where application-level consistency, platform independence, and flexibility in data replication are crucial.

- Some common use cases include:

Disaster Recovery: Network-based replication is widely used for disaster recovery purposes. Organizations replicate critical data and applications from their primary data center to a secondary or remote site. In the event of a disaster or site failure, the replicated data can be quickly activated, allowing for business continuity and minimal data loss.

Multi-site Deployments: Organizations with multiple geographically dispersed locations often utilize network-based replication to keep data synchronized across sites. This enables seamless collaboration, data sharing, and consistent access to up-to-date information. It particularly benefits distributed enterprises, branch offices, and global organizations.

Data Migration: When migrating data from one system or infrastructure to another, network-based replication simplifies the process. It allows for the smooth transfer of data, ensuring minimal downtime and disruption. Organizations can replicate data from the source system to the target system, validate its integrity, and seamlessly transition to the new environment.

High Availability and Load Balancing: Network-based replication is employed to achieve high availability and load balancing in environments where continuous data access and minimal downtime are critical. By replicating data across multiple systems, organizations can distribute the workload, handle increased traffic, and maintain service availability even in the event of hardware or system failures.

DevOps and Testing Environments: Network-based replication facilitates the creation of reliable and consistent testing environments. Development and testing teams can replicate production data to their test environments, ensuring realistic testing scenarios without impacting the production environment. This enables thorough testing, debugging, and validation of applications and infrastructure changes.

Data Archiving and Compliance: Network-based replication supports long-term data archiving and compliance requirements. Organizations can replicate data to dedicated archival systems or cloud storage for regulatory compliance, data retention policies, or legal obligations. It ensures data integrity, security, and availability for archival purposes.

Cloud Data Replication: With the growing adoption of cloud services, network-based replication plays a crucial role in replicating data from on-premises environments to cloud-based infrastructure. Organizations can replicate data to the cloud for backup, disaster recovery, or as part of hybrid cloud strategies. It enables seamless data movement between on-premises and cloud environments.

➔ DATA MIGRATION

- In general, data migration means moving digital information.
- Transferring that information to a different location, file format, environment, storage system, database, datacenter, or application all fit within the definition of data migration.
- Data migration is the process of selecting, preparing, extracting, and transforming data and permanently transferring it from one computer storage system to another.
- Data migration is a common IT activity. However, data assets may exist in many different states and locations, which makes some migration projects more complex and technically challenging than others.

- Examples of data assets include:
  - ✓ Unorganized assortments of files stored across many different devices.
  - ✓ Applications, operating systems, and environments.
  - ✓ Relational databases like SQL Server, MySQL, PostgreSQL, and MariaDB.
  - ✓ Unstructured databases such as MongoDB, Azure Cosmos DB, DocumentDB, Cassandra, Couchbase, HBase, Redis, and Neo4j.
  - ✓ Data lakes, data blobs, and entire datacenters.

- Data migration projects require planning, implementation, and validation to ensure their success.

Importance of Data migration

- Data migration ensures that data is successfully and securely transferred to another application, storage system or cloud.
- Although moving data from one platform to another can be risky and costly, it also provides an organization with numerous benefits.
- For example, in addition to upgrading applications and services, organizations can boost their productivity and reduce storage costs.

Types of data migrations and their challenges

Data migration is typically performed using one of the following methods:

- **Storage migration** transfers data from one storage device to another. This involves moving blocks of storage and files from storage systems, whether they're on disk, tape or in the cloud. During migration is also an optimal time for organizations to perform data validation and reduction by identifying obsolete or corrupt data.
- **Database migrat**ion moves database files to a new device. This is done when an organization changes database vendors, upgrades the database software or moves a database to the cloud. Databases must be backed up before migrating.
- **Application migration** moves an application or program from one environment to another. Application migration typically occurs when an organization switches to another vendor, application or platform. This process is complex because applications interact with other applications, and each one has its own data model. Successful application migration may require using middleware products to bridge technology gaps.
- **Cloud migration** moves data or applications from an on-premises location to the cloud or from one cloud service to another. Cloud migration is a common form of data migration. Cloud environments provide on-demand flexibility and scalability and reduce the capital expenditure (Capex) for on-premises infrastructures. Public cloud providers offer a variety of services for storage, database and application migrations.
- **Business process migration** moves business applications -- including customer, product and operational data -- and processes to a new environment.

During data migrations, teams must pay careful attention to the following challenges:

- **Source data.** Not preparing the source data being moved might lead to data duplicates, gaps or errors when it's brought into the new system or application.

- **Wrong data formats.** Data must be opened in a format that works with the system. Files might not have access controls on a new system if they aren't properly formatted before migration.
- **Mapping data.** When stored in a new database, data should be mapped in a sensible way to minimize confusion.
- **Sustainable governance**. Having a data governance plan in place can help organizations track and report on data quality, which helps them understand the integrity of their data.
- **Security**. Maintaining who can access, edit or remove data is a must for security.

Data migration strategies

Although implementation differs by migration type, there are still **two main strategies** organizations use: ***big bang* and *trickle* migrations.**

- **Big bang migrations** transfer all associated data within a set time window. The advantages of creating a migration strategy around this method include lower cost, a quicker move and less complexity. The downside, however, is that big bang migrations require the system to be offline for the entire migration. There's also a risk of losing data if it isn't properly backed up to another location ahead of time.
- **Trickle migrations** complete a data migration within phases. During the migration, both old and new systems run at the same time, so there's no downtime, which means there's less risk of losing data. However, trickle migrations are more complicated and need more planning and time to implement properly.

How to create a data migration plan

- A data migration project can be challenging because administrators must maintain data integrity and time the project so there's minimal effect on the business and they can keep an eye on costs.
- Having a data migration plan helps to ensure there's minimal disruption and downtime to business processes.
- Factors to consider during a data migration project include how long the migration will take, the amount of downtime required, and the risk to the business due to technical compatibility issues, data corruption or application performance.

Phases of Data Migration

Discovery. This should include considerations such as data sources, destinations, security, cost and which migration strategy to use.

Resource assessment. Identify who will be taking part in the migration.

Data inspection. Examine the data being migrated for data quality, anomalies or duplications. Data should also be backed up.

Design. Data is organized and mapped out for where it's being moved to.

Software tools. Any software that will help in the transition is purchased or created.

Migration. The migration process is initiated.

Cleanup. Old or legacy systems are shut down and decommissioned.

Examples of data migration tools

- Microsoft SQL, AWS Data Migration Service, Varonis DatAdvantage and Varonis Data Transport Engine.

There are ***three broad categories*** of data movers: host-based, array-based and network appliances.

Host-based software is best for application-specific migrations, such as platform upgrades, database replication and file copying.

Array-based-based software is primarily used to migrate data between similar systems.

Network appliances migrate volumes, files or blocks of data depending on their configuration.

Data migration vs. data integration vs. data conversion

- ✓ Data migration is the process of transferring data between data storage systems or formats,
- ✓ Data integration is the process of combining data from multiple source systems -- creating a unified set of data for operational and analytical uses. The primary goal of data integration is to produce consolidated data sets that are clean and consistent. Integration is a core element of the data management process.
- ✓ Data conversion is the process of changing data from one format to another. If a legacy system and a new system have identical fields, an organization could just do a data migration; however, the data from the legacy system is generally different and needs to be modified before migrating. Data conversion is often a step in the data migration process.

➔ DISASTER RECOVERY AS A SERVICE (DRAAS)

- Disaster recovery as a service(DRaaS) is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third party cloud computing environment and provide all the DR orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster.
- The as-a-service model means that the organization itself doesn't have to own all the resources or handle all the management for disaster recovery, instead relying on the service provider.
- Disaster recovery planning is critical to business continuity.
- Many disasters that have the potential to wreak havoc on an IT organization have become more frequent in recent years:
  - Natural disasters such as hurricanes, floods, wildfires and earthquakes
  - Equipment failures and power outages
  - Cyberattacks

Using DRaaS to prepare for a disaster

- True DRaaS mirrors a complete infrastructure in fail-safe mode on virtual servers, including compute, storage and networking functions.
- An organization can continue to run applications—it just runs them from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers. This means recovery time after a disaster can be much faster, or even instantaneous.
- Once the physical servers are recovered or replaced, the processing and data is migrated back onto them. Customers may experience higher latency when their applications are

running from the cloud instead of from an on-site server, but the total business cost of downtime can be very high, so it's imperative that the business can get back up and running.

How does disaster recovery as a service work?

- DRaaS works by replicating and hosting servers in a third-party vendor's facilities versus in the physical location of the organization that owns the workload. The disaster recovery plan is executed on the third-party vendor's facilities in the event of a disaster that shuts down a customer's site.
- Organizations may purchase DRaaS plans through a traditional subscription model or a pay-per-use model that allows them to pay only when disaster strikes.
- As-a-service solutions vary in scope and cost—organizations should evaluate potential DRaaS providers according to their own unique needs and budget.

DRaaS can save organizations money by eliminating the need for provisioning and maintaining an organization's own off-site disaster recovery environment. However, organizations should evaluate and understand service level agreements.

For instance, what happens to recovery times if both the provider and customer are affected by the same natural disaster, such as a large hurricane or earthquake. Different DRaaS providers have different policies on prioritizing which customers get help first in a large regional disaster or allowing customers to perform their own disaster recovery testing.

Advantages of Disaster recovery as a service

- Many businesses with lean IT teams simply can't afford to take the time needed to research, implement and fully test disaster recovery plans. DRaaS takes the burden of planning for a disaster off of the organization and puts it into the hands of experts in disaster recovery.
- It can also be much more affordable than hosting your own disaster recovery infrastructure in a remote location with an IT staff standing by if disaster strikes.
- If a disaster doesn't happen, that expensive second infrastructure and staff never get used. Many DRaaS providers charge you only if you need their services.
- For many organizations, DRaaS is a helpful solution to a nagging problem.

Is disaster recovery as a service right for you?

- Organizations may choose to hand over all or part of their disaster recovery planning to a DRaaS provider.
- There are many different disaster recovery as a service providers to choose from, with **three mainmodels:**

  Managed DRaaS: In a managed DRaaS model, a third party takes over all responsibility for disaster recovery. Choosing this option requires an organization to stay in close contact with their DRaaS provider to ensure that it stays up to date on all infrastructure, application and services changes. If you lack the expertise or time to manage your own disaster recovery, this may be the best option for you.

  Assisted DRaaS: If you prefer to maintain responsibility for some aspects of your disaster recovery plan, or if you have unique or customized applications that might be challenging for a third party to take over, assisted DRaaS might be a better option. In this model, the service provider offers its expertise for optimizing disaster recovery procedures, but the customer is responsible for implementing some or all of the disaster recovery plan.

Self-service DRaaS: The least expensive option is self-service DRaaS, where the customer is responsible for the planning, testing and management of disaster recovery, and the customer hosts its own infrastructure backup on virtual machines in a remote location. Careful planning and testing are required to make sure that processing can fail over to the virtual servers instantly in the event of a disaster. This option is best for those who have experienced disaster recovery experts on staff.

- ✓ Whichever of these models suits you, VMware has a solution.
- ✓ If you would drive your own DRaaS solution to your own target DR site, you can consider solutions like Site Recovery Manager and VMware vSphere Replication.
- ✓ If you would like a service provider to assist you with DR, whether fully managed or self service, consider VMware Cloud Director Availability from one of our DRaaS Validate partners

DRaaS vs. BaaS :

- With **disaster recovery as a service**, the service provider moves an organization's computer processing to its cloud infrastructure in the event of a disaster. This way, the business can continue to operate, even if the original IT infrastructure is totally destroyed or held hostage.
- This differs from **backup as a service**, where only the data, but not the ability to process the data, is duplicated by a third-party provider.
- Because BaaS is only protecting the data, and not the infrastructure, it is typically less expensive than DRaaS. BaaS can be a good solution for companies that need to archive data or records for legal reasons, but most organizations who use BaaS will want to combine it with another disaster recovery tool to ensure business continuity.
- Planning for disaster and getting the help you need is something every business needs to consider. Whatever option you choose, a disaster recovery plan is essential for business continuity, and organizations are increasingly turning to DRaaS.

UNIT V
SECURING STORAGE INFRASTRUCTURE

Information security goals, Storage security domains, Threats to a storage infrastructure, Security controls to protect a storage infrastructure, Governance, risk, and compliance, Storage infrastructure management functions, Storage infrastructure management processes.

➔ INFORMATION SECURITY GOALS

- In Information security, it is a collection of practices intended to convey personal information secure from unapproved access and modification throughout of storing or broadcasting from one place to another place.
- Information security is designed and required to secure the print, digital, and some personal, sensitive, and private information from unapproved persons. It very well may be utilized to get information from being misused, affirmation, destruction, modification, and interruption.

- There are the major goals of information security which are as follows −

Confidentiality − The goals of confidentiality is that only the sender and the predetermined recipient should be adequate to approach the element of a message. Confidentiality have negotiate if an unauthorized person is capable to create the message.

For example, it can be a confidential email message sent by user A to user B, which is penetrated by user C without the authorization or knowledge of A and B. This kind of attack is known as interception.

Integrity − When the element of a message are transformed after the sender sends it, but since it reaches the intended recipient, and it can said that the principle of the message is lost.

For example, consider that user A sends message to user B and User C alter with a message basically sent by user A, which is absolutely intended for user B.
User C somehow handles to access it, modify its elements and send the changed message to user B. User B has no method of understanding that the element of the message changed after user A had sent it. User A also does not understand about this change. This kind of attack is known as modification.

Availability − The main goals of information security is availability. It is that resources must be available to authorized parties at all times.

For instance, because of the intentional actions of an unauthorized user C, an authorized user A cannot allow contact a server B. This can overthrow the principle of availability. Such an attack is known as interruption.

➔ STORAGE SECURITY DOMAINS

- Storage devices that are not connected to a storage network are less vulnerable because they are not exposed to security threats via networks. However, with increasing use of networking in storage environments, storage devices are becoming highly exposed to security threats from a variety of sources.
- If each component within the storage network is considered a potential access point, one must analyze the attack surface that each of these access points provides and identify the associated vulnerability.
- In order to identify the threats that apply to a storage network, *access paths to data storage can be categorized into three security domains: application access, management access, and BURA (backup, recovery, and archive).*
- Figure 15-1 depicts the three security domains of a storage system environment.

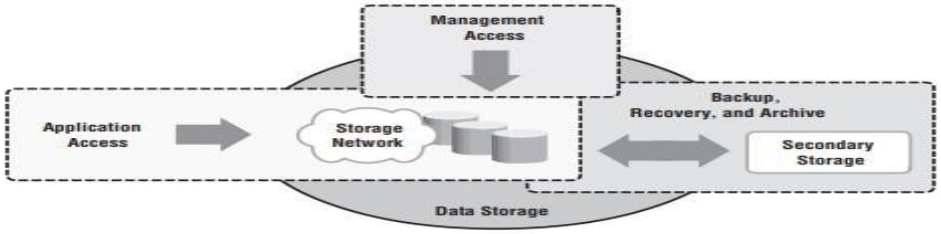


Figure 15-1: Three security domains of data storage

SECURING THE APPLICATION ACCESS DOMAIN

- The application access domain may include only those applications that access the data through the file system or a database interface.
- Figure 15-2 shows application access in a storage networking environment. Host A can access all V1 volumes; host B can access all V2 volumes.
- These volumes are classified according to access level, such as confidential, restricted, and public. Some of the possible threat in this scenario could be host A spoofing the identity or elevating the privileges of host B to gain access to host B's resources.
- Another threat could be an unauthorized host gain access to the network; the attacker on this host may try to spoof the identity of another host and tamper with data, snoop the network, or execute a DoS attack.
- Also any form of media theft could also compromise security.

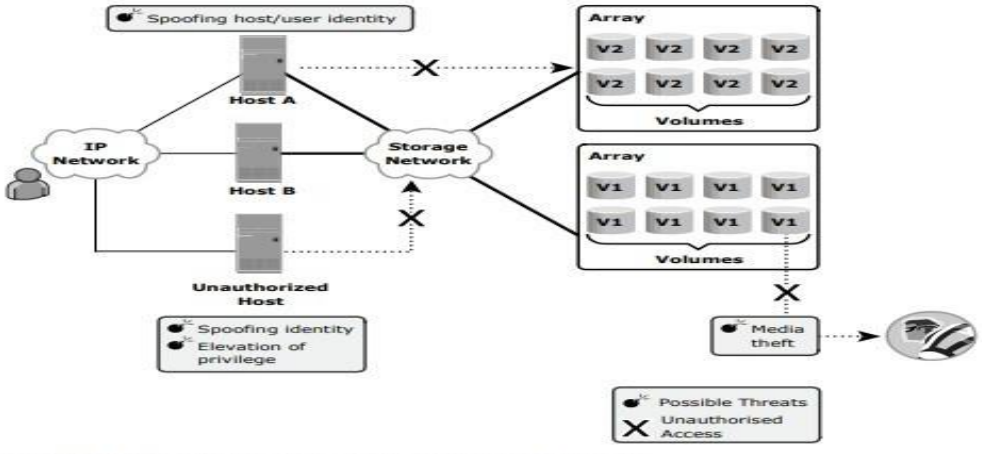


Figure 15-2: Security threats in application access domain

Controlling User Access to Data

- Access control services regulate user access to data. These services mitigate the threats of spoofing host identity and elevating host privileges. Both of these threats affect data integrity and confidentiality.
- Technical control in the form of user authentication and administrative control in the form of user authorization are the two access control mechanisms used in application access control

Protecting the Storage Infrastructure

- Securing the storage infrastructure from unauthorized access involves protecting all the elements of the infrastructure.
- Security controls for protecting the storage infrastructure address the threats of unauthorized tampering of data in transit that leads to a loss of data integrity, denial of service that compromises availability, and network snooping that may result in a loss of confidentiality.
- The security controls for protecting the network fall into two general categories: connectivity infrastructure integrity and storage network encryption

Data Encryption

- The most important aspect of securing data is protecting data held inside the storage arrays. Threats at this level include tampering with data, which violates data integrity, and media theft, which compromises data availability and confidentiality.
- To protect against these threats, encrypt the data held on the storage media or encrypt the data prior to being transferred to the disk.

SECURING THE MANAGEMENT ACCESS DOMAIN

- Management access, whether monitoring, provisioning, or managing storage resources, is associated with every device within the storage network. Most management software supports some form of CLI, system management console, or a web-based interface.
- Figure 15-3 depicts a storage networking environment in which production hosts are connected to a SAN fabric and are accessing storage Array A, which is connected to storage Array B for replication purposes.
- Further, this configuration has a storage management platform on Host B and a monitoring console on Host A.

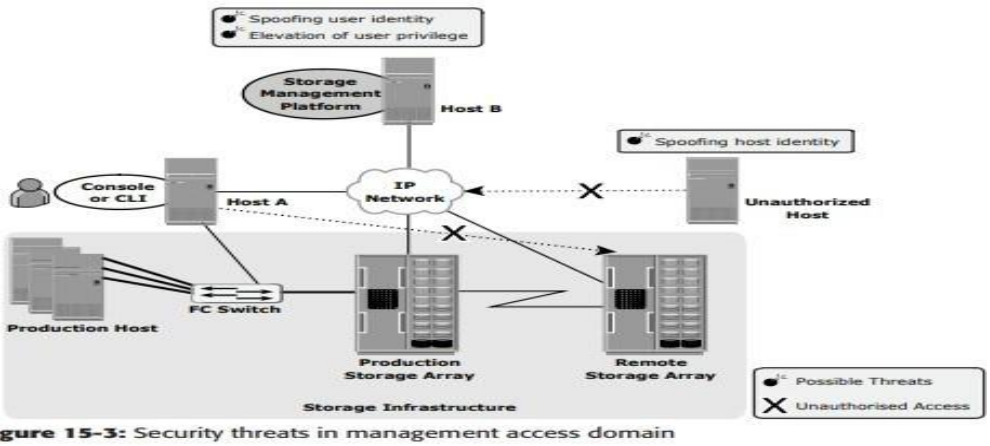


Figure 15-3: Security threats in management access domain

Controlling Administrative Access

- Controlling administrative access to storage aims to safeguard against the threats of an attacker spoofing an administrator's identity or elevating another user's identity and privileges to gain administrative access.
- Both of these threats affect the integrity of data and devices.
- To protect against these threats, administrative access regulation and various auditing techniques are used to enforce accountability.

Protecting the Management Infrastructure

- Protecting the management network infrastructure is also necessary. Controls to protect the management network infrastructure include encrypting management traffic, enforcing management access controls, and applying IP network security best practices.

SECURING BACKUP, RECOVERY, AND ARCHIVE (BURA)

- BURA is the third domain that needs to be secured against attack. A backup involves copying the data from a storage array to backup media, such as tapes or disks. Securing BURA is complex and is based on the BURA software accessing the storage arrays.
- It also depends on the configuration of the storage environments at the primary and secondary sites, especially with remote backup solutions performed directly on a remote tape device or using array-based remote replication.
- Protecting the BURA infrastructure requires addressing several threats, including spoofing the legitimate identity of a DR site, tampering with data, network snooping, DoS attacks, and media theft. Such threats represent potential violations of integrity, confidentiality, and availability.
- Figure 15-4 illustrates a generic remote backup design whereby data on a storage array is replicated over a disaster recovery (DR) network to a secondary storage at the DR site.

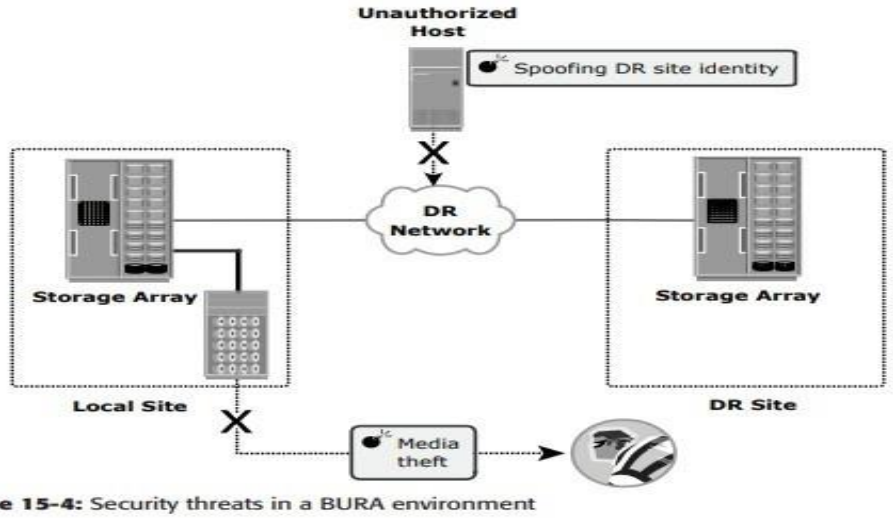


Figure 15-4: Security threats in a BURA environment

➔ THREATS TO A STORAGE INFRASTRUCTURE

Risk Triad

- Risk triad defines the risk in terms of threats, assets, and vulnerabilities. Risk arises when a threat agent (an attacker) seeks to access assets by exploiting an existing vulnerability.
- To manage risks, organizations primarily focus on vulnerabilities because they cannot eliminate threat agents that may appear in various forms and sources to its assets. Organizations can install countermeasures to reduce the impact of an attack by a threat agent, thereby reducing vulnerability.
- Risk assessment is the first step in determining the extent of potential threats and risks in an IT infrastructure. To determine the probability of an adverse event occurring, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the existing security controls.
- The severity of an adverse event is estimated by the impact that it may have on critical business activities. Based on this analysis, a relative value of criticality and sensitivity can be assigned to IT assets and resources.

- ***Assets, threats, and vulnerability*** are considered from the perspective of risk identification and control analysis.

Assets

- Information is one of the most important assets for any organization. Other assets include hardware, software, and the network infrastructure required to access this information.
- To protect these assets, organizations must develop a set of parameters to ensure the availability of the resources to authorized users and trusted networks. These parameters apply to storage resources, the network infrastructure, and organizational policies.
- Several factors need to be considered when planning for asset security. Security methods have two objectives.
- *First objective is to ensure that the network is easily accessible to authorized users. It should also be reliable and stable under disparate environmental conditions and volumes of usage.*
- *Second objective is to make it very difficult for potential attackers to access and compromise the system. These methods should provide adequate protection against unauthorized access to resources, viruses, worms, Trojans and other malicious software programs.*

Threats

- 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. They pose threats to data integrity and availability. In a modification attack, the unauthorized user attempts to modify information for malicious purposes.

- A modification attack can target data at rest or data in transit. These attacks pose a threat to data integrity. Denial of Service (DoS) attacks denies the use of resources to legitimate users.
- These attacks generally do not involve access to or modification of information on the computer system. Instead, they pose a threat to data availability.
- The intentional flooding of a network or website to prevent legitimate access to authorized users is one example of a DoS attack. Repudiation is an attack against the accountability of the information.
- It attempts to provide false information by either impersonating someone or denying that an event or a transaction has taken place.
- Table 15-1 describes different forms of attacks and the security services used to manage them.

Table 15-1: Security Services for Various Types of Attacks

ATTACK	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	ACCOUNTABILITY
Access	X			X
Modification	X	X		X
Denial of Service			X	
Repudiation		X		X

Vulnerability

- The paths that provide access to information are the most vulnerable to potential attacks. Each of these paths may contain various access points, each of which provides different levels of access to the storage resources.
- It is very important to implement adequate security controls at all the access points on an access path. Implementing security controls at each access point of every access path is termed as defense in depth.
- 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. Each component of a storage network is a source of potential vulnerability
- An attack vector is a step or a series of steps necessary to complete an attack. For example, an attacker might exploit a bug in the management interface to execute a snoop attack whereby the attacker can modify the configuration of the storage device to allow the traffic to be accessed from one more host.
- Work factor refers to the amount of time and effort required to exploit an attack vector.
- For example, if attackers attempt to retrieve sensitive information, they consider the time and effort that would be required for executing an attack on a database.
- The preventive control attempts to prevent an attack; the detective control detects whether an attack is in progress; and after an attack is discovered, the corrective controls are implemented.

- *Preventive controls avert the vulnerabilities from being exploited and prevent an attack or reduce its impact. Corrective controls reduce the effect of an attack, while detective controls discover attacks and trigger preventive or corrective controls.*

➔ SECURITY CONTROLS TO PROTECT A STORAGE INFRASTRUCTURE

- Security controls for protecting the storage infrastructure address the threats of unauthorized tampering of data in transit that leads to a loss of data integrity, denial of service that compromises availability, and network snooping that may result in a loss of confidentiality.
- There are several types of security controls that can be implemented to protect hardware, software, networks, and data from actions and events that could cause loss or damage.
- For example:

Physical security controls include such things as data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.

Digital security controls include such things as usernames and passwords, two-factor authentication, antivirus software, and firewalls.

Cybersecurity controls include anything specifically designed to prevent attacks on data, including DDoS mitigation, and intrusion prevention systems.

Cloud security controls include measures you take in cooperation with a cloud services provider to ensure the necessary protection for data and workloads. If your organization runs workloads on the cloud, you must meet their corporate or business policy security requirements *and* industry regulations.

➔ GOVERNANCE, RISK, AND COMPLIANCE

- Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations.
- It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption.

Governance

Governance is the set of policies, rules, or frameworks that a company uses to achieve its business goals.

It defines the responsibilities of key stakeholders, such as the board of directors and senior management.

For example, good corporate governance supports your team in including the company's social responsibility policy in their plans.

Good governance includes the following:

- ✓ Ethics and accountability
- ✓ Transparent information sharing
- ✓ Conflict resolution policies
- ✓ Resource management

Risk management

Businesses face different types of risks, including financial, legal, strategic, and security risks. Proper risk management helps businesses identify these risks and find ways to remediate any that are found.

Companies use an enterprise risk management program to predict potential problems and minimize losses.

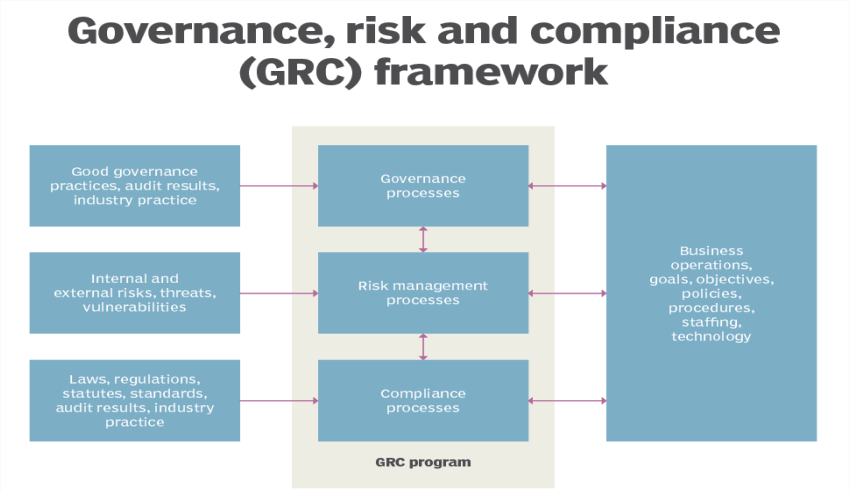
For example, you can use risk assessment to find security loopholes in your computer system and apply a fix.

Compliance

Compliance is the act of following rules, laws, and regulations. It applies to legal and regulatory requirements set by industrial bodies and also for internal corporate policies.

In GRC, compliance involves implementing procedures to ensure that business activities comply with the respective regulations.

For example, healthcare organizations must comply with laws like HIPAA that protect patients' privacy.



BENEFITS OF GRC :

- By implementing GRC programs, businesses can make better decisions in a risk-aware environment.
- An effective GRC program helps key stakeholders set policies from a shared perspective and comply with regulatory requirements.
- With GRC, the entire company comes together in its policies, decisions, and actions.

The following are some benefits of implementing a GRC strategy at your organization.

Data-driven decision-making

You can make data-driven decisions within a shorter time frame by monitoring your resources, setting up rules or frameworks, and using GRC software and tools.

Responsible operations

GRC streamlines operations around a common culture that promotes ethical values and creates a healthy environment for growth. It guides strong organizational culture development and ethical decision-making in the organization.

Improved cybersecurity

With an integrated GRC approach, businesses can employ data security measures to protect customer data and private information. Implementing a GRC strategy is essential for your organization due to increasing cyber risk that threatens users' data and privacy. It helps organizations comply with data privacy regulations like the General Data Protection Regulation (GDPR). With a GRC IT strategy, you build customer trust and protect your business from penalties.

IMPLEMENTATION OF GRC:

Companies of all sizes face challenges that can endanger revenue, reputation, and customer and stakeholder interest.

Some of these challenges include the following:

- ✓ Internet connectivity introducing cyber risks that might compromise data storage security
- ✓ Businesses needing to comply with new or updated regulatory requirements
- ✓ Companies needing data privacy and protection
- ✓ Companies facing more uncertainties in the modern business landscape
- ✓ Risk management costs increasing at an unprecedented rate
- ✓ Complex third-party business relationships increasing risk

WORKING OF GRC :

GRC in any organization works on the following principles:

Key stakeholders

GRC requires cross-functional collaboration across different departments that practices governance, risk management, and regulatory compliance.

Some examples include the following:

- ✓ Senior executives who assess risks when making strategic decisions
- ✓ Legal teams who help businesses mitigate legal exposures
- ✓ Finance managers who support compliance with regulatory requirements
- ✓ HR executives who deal with confidential recruitment information
- ✓ IT departments that protect data from cyber threats

GRC framework

A GRC framework is a model for managing governance and compliance risk in a company.

It involves identifying the key policies that can drive the company toward its goals. By adopting a GRC framework, you can take a proactive approach to mitigating risks, making well-informed decisions, and ensuring business continuity.

Companies implement GRC by adopting GRC frameworks that contain key policies that align with the organization's strategic objectives.

Key stakeholders base their work on a shared understanding from the GRC framework as they devise policies, structure workflows, and govern the company.

Companies might use software and tools to coordinate and monitor the success of the GRC framework.

GRC maturity

GRC maturity is the level of integration of governance, risk assessment, and compliance within an organization.

You achieve a high level of GRC maturity when a well-planned GRC strategy results in cost efficiency, productivity, and effectiveness in risk mitigation.

Meanwhile, a low level of GRC maturity is unproductive and keeps business units working in silos.

GRC CAPABILITY MODEL:

- The GRC Capability Model contains guidelines that help companies implement GRC and achieve principled performance.
- It ensures a common understanding of communication, policies, and training.
- You can take a cohesive and structured approach to incorporate GRC operations across your organization.

Learn

You learn about the context, values, and culture of your company so you can define strategies and actions that reliably achieve objectives.

Align

Ensure that your strategy, actions, and objectives are in alignment. You do so by considering opportunities, threats, values, and requirements when making decisions.

Perform

GRC encourages you to take actions that bring results, avoid those that hinder goals, and monitor your operations to detect sudden changes.

Review

You revisit your strategy and actions to ensure they align with the business goals. For example, regulatory changes could require a change of approach.

GRC TOOLS:

GRC tools are software applications that businesses can use to manage policies, assess risk, control user access, and streamline compliance.

There are some of the following GRC tools to integrate business processes, reduce costs, and improve efficiency.

GRC software

GRC software helps automate GRC frameworks by using computer systems. Businesses use GRC software to perform these tasks:

- ✓ Oversee policies, manage risk, and ensure compliance
- ✓ Stay updated about various regulatory changes that affect the business
- ✓ Empower multiple business units to work together on a single platform
- ✓ Simplify and increase the accuracy of internal auditing

User management

You can give various stakeholders the right to access company resources with user management software.

This software supports granular authorization, so you can precisely control who has access to what information.

User management ensures that everyone can securely access the resources they need to get their work done.

Security information and event management

You can use security information and event management (SIEM) software to detect potential cybersecurity threats. IT teams use SIEM software like AWS CloudTrail to close security gaps and comply with privacy regulations.

Auditing

You can use auditing tools like AWS Audit Manager to evaluate the results of integrated GRC activities in your company.

By running internal audits, you can compare actual performance with GRC goals. You can then decide if the GRC framework is effective and make necessary improvements.

CHALLENGES OF GRC IMPLEMENTATION

Businesses might face challenges when they integrate GRC components into organizational activities.

Change management

GRC reports provide insights that guide businesses to make accurate decisions, which helps in a fast-changing business environment. However, companies need to invest in a change management program to act quickly based on GRC insights.

Data management

Companies have long been operating by keeping departmental functions separated. Each department generates and stores its own data. GRC works by combining all the data within an organization. This results in duplicate data and introduces challenges in managing information.

Lack of a total GRC framework

A complete GRC framework integrates business activities with GRC components. It serves the changing business environment, particularly when you are dealing with new regulations. Without a seamless integration, your GRC implementation is likely to be fragmented and ineffective.

Ethical culture development

It takes great effort to get every employee to share an ethically compliant culture. Senior executives must set the tone of transformation and ensure that information is passed through all layers of the organization.

Clarity in communication

The success of GRC implementation depends on seamless communication. Information sharing must be transparent between GRC compliance teams, stakeholders, and employees. This makes activities like creating policies, planning, and decision-making easier.

How do organizations implement an effective GRC strategy?

You must bring different parts of your business into a unified framework to implement GRC.

Building an effective GRC requires continuous evaluation and improvement.

The following tips make GRC implementation easier.

Define clear goals

Start by determining what goals you want to accomplish with the GRC model. For example, you might want to address the risk of noncompliance to data privacy laws.

Assess existing procedures

Evaluate current processes and technologies in your company that you use to handle governance, risk, and compliance. You can then plan and choose the right GRC frameworks and tools.

Start from the top

Senior executives play a leading role in the GRC program. They must understand the benefits of implementing GRC for policies and how it helps them make decisions and build a risk-aware culture.

Use GRC solutions

You can use GRC solutions to manage and monitor an enterprise GRC program. These GRC solutions give you a holistic view of the underlying processes, resources, and records. Use the tools to monitor and meet regulatory compliance requirements.

For example, Netflix uses AWS Config to make sure its AWS resources meet security requirements. Symetra uses AWS Control Tower to quickly provision new accounts that fully adhere to their corporate policy.

Test the GRC framework

Test the GRC framework on one business unit or process, and then evaluate whether the chosen framework aligns with your goals. By conducting small-scale testing, you can make helpful changes to the GRC system before you implement it in the entire organization.

Set clear roles and responsibilities

GRC is a collective team effort. Although senior executives are responsible for setting key policies, legal, finance, and IT personnel are equally accountable for GRC success. Defining the roles and responsibilities of each employee promotes accountability. It allows employees to report and address GRC issues promptly.

Some examples of GRC products are the following:

- ✓ Diligent HighBond.
- ✓ IBM OpenPages.

- ✓ LogicManager.
- ✓ LogicGate Risk Cloud.
- ✓ MetricStream Enterprise GRC.
- ✓ Navex Global Lockpath.
- ✓ ServiceNow Governance, Risk, and Compliance.

➔ STORAGE INFRASTRUCTURE MANAGEMENT FUNCTIONS :

Storage Management Activities

- All the management tasks in a storage infrastructure can be broadly categorized into availability management, capacity management, performance management, security management, and reporting.

Availability management

- The critical task in availability management is establishing a proper guideline for all configurations to ensure availability based on service levels.
- For example, when a server is deployed to support a critical business function, the highest availability standard is usually required.
- This is generally accomplished by deploying two or more HBAs, multipathing software with path failover capability, and server clustering. The server must be connected to the storage array using at least two independent fabrics and switches that have built-in redundancy. Storage devices with RAID protection are made available to the server using at least two front-end ports. In addition, these storage arrays should have built-in redundancy for various components, support backup, and local and remote replication. Virtualization technologies have significantly improved the availability management task. With virtualization in place resources can be dynamically added or removed to maintain the availability.

Capacity management

- The goal of capacity management is to ensure adequate availability of resources for all services based on their service level requirements.
- Capacity management provides capacity analysis, comparing allocated storage to forecasted storage on a regular basis.
- It also provides trend analysis of actual utilization of allocated storage and rate of consumption, which must be rationalized against storage acquisition and deployment timetables.
- Storage provisioning is an example of capacity management.
- It involves activities such as device configuration and LUN masking on the storage array and zoning configuration on the SAN and HBA components. Capacity management also takes into account the future needs of resources, and setting up monitors and analytics to gather such information.

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 the information — whether a component is meeting expected performance levels. Several performance management activities are initiated for the deployment of an application or server in the existing storage infrastructure.
- Every component must be validated for adequate performance capabilities as defined by the service levels. For example, to optimize expected performance levels, activities on the server such as the volume configuration, designing the database, application layout configuration of multiple HBAs, and intelligent multipathing software must be fine-tuned. The performance management tasks on a SAN include designing sufficient ISLs in a multi-switch fabric with adequate bandwidth to support the required performance levels. The storage array configuration tasks include selecting the appropriate RAID type and LUN layout, front-end and back-end ports, and LUN accessibility (LUN masking) while considering the end-to-end performance.

Security Management

- Security management prevents unauthorized access and configuration of storage infrastructure components.
- For example, while deploying an application or a server, the security management tasks include managing user accounts and access policies, that authorizes users to perform role-based activities.
- The security management tasks in the SAN environment include configuration of zoning to restrict an HBA's unauthorized access to the specific storage array ports. LUN masking prevents data corruption on the storage array by restricting host access to a defined set of logical devices.

Reporting

- It is difficult for businesses to keep track of the resources they have in their data centers, for example, the number of storage arrays, the array vendors, how the storage arrays are being used, and by which applications.
- Reporting on a storage infrastructure involves keeping track and gathering information from various components/processes.
- This information is compiled to generate reports for trend analysis, capacity planning, chargeback, performance, and to illustrate the basic configuration of storage infrastructure components.
- Capacity planning reports also contain current and historic information about utilization of storage, file system, database tablespace, and ports.
- Configuration or asset management reports include details about device allocation, local or remote replicas, and fabric configuration; and list all equipment, with details such as their value, purchase date, lease status, and maintenance records.
- Chargeback reports contain information about the allocation or utilization of storage infrastructure components by various departments or user groups. Performance reports provide details about the performance of various storage infrastructure components.

➔ STORAGE INFRASTRUCTURE MANAGEMENT PROCESSES :

- **Storage Management** is defined as it refers to the management of the data storage equipment's that are used to store the user/computer generated data.
- Hence it is a tool or set of processes used by an administrator to keep your data and storage equipment's safe.
- Storage management is a process for users to optimize the use of storage devices and to protect the integrity of data for any media on which it resides and the category of storage management generally contain the different type of subcategories covering aspects such as security, virtualization and more, as well as different types of provisioning or automation, which is generally made up the entire storage management software market.

Storage management key attributes: Storage management has some key attribute which is generally used to manage the storage capacity of the system. These are given below:

1. Performance
2. Reliability
3. Recoverability
4. Capacity

Feature of Storage management: There is some feature of storage management which is provided for storage capacity. These are given below:

- ✓ Storage management is a process that is used to optimize the use of storage devices.
- ✓ Storage management must be allocated and managed as a resource in order to truly benefit a corporation.
- ✓ Storage management is generally a basic system component of information systems.
- ✓ It is used to improve the performance of their data storage resources.

Advantage of storage management: There are some advantage of storage management which are given below:

- ✓ It becomes very simple to manage a storage capacity.
- ✓ It generally reduces the time consumption.
- ✓ It improves the performance of system.
- ✓ In virtualization and automation technologies, it can help an organization improve its agility.

Limitations of storage management:

- ✓ Limited physical storage capacity: Operating systems can only manage the physical storage space that is available, and as such, there is a limit to how much data can be stored.
- ✓ Performance degradation with increased storage utilization: As more data is stored, the system's performance can decrease due to increased disk access time, fragmentation, and other factors.
- ✓ Complexity of storage management: Storage management can be complex, especially as the size of the storage environment grows.
- ✓ Cost: Storing large amounts of data can be expensive, and the cost of additional storage capacity can add up quickly.

- ✓ Security issues: Storing sensitive data can also present security risks, and the operating system must have robust security features in place to prevent unauthorized access to this data.
- ✓ Backup and Recovery: Backup and recovery of data can also be challenging, especially if the data is stored on multiple systems or devices.

- ***Storage management consists of several different processes. Some storage management plans only use a few processes, while others might use them all. Below are the most common processes found in storage management:***

PROVISIONING

- This method entails assigning storage capacity by analyzing current capabilities, such as storage on physical drives or the cloud, and deciding the proper information to store in each location.
- It's important to consider factors such as ease of access and security when determining where to store your data.
- Planning where to store data allows organizations to discover whether they have ample storage space available or whether they should reconfigure their system for better efficiency.

DATA COMPRESSION

- This is the act of reducing the size of data sets without compromising them. Compressing data allows users to save storage space, improve file transfer speeds and decrease the amount of money they spend on storage hardware and network bandwidth.
- Data compression works by either removing unnecessary bits of information or redundancies within data.
- For example, to compress an audio file, a data compression tool may remove parts of the file that contain no audible noise.
- This would reduce the size of the file while still preserving essential parts of the data.

DATA MIGRATION

- This method entails moving data from one location to another. This can include the physical location, such as from one hard drive to another, or the application that uses the data.
- Data migration is often necessary when introducing new hardware or software components into an organization.
- For example, if a business purchases new computers for its office, it's important to transfer all data from the old systems to the new ones.
- Important factors to consider while implementing data migration include ensuring network bandwidth, effective transfer speeds, data integrity and ample storage space for the new location throughout the transfer.

DATA REPLICATION

- This process includes making one or more copies of a particular data set, as there are several reasons why a company may want to replicate its data.
- For example, you may wish to create a backup if there's a problem with an original data set. You may also want to replicate data so you can store it across different locations, improving the overall accessibility across your network.
- There are two types of data replication***: synchronous and asynchronous***. **Synchronous data** replication is when companies copy any changes to an original data set in the replicated data set. This type of replication ensures updated information but may also use require more resources than asynchronous replication.

  Asynchronous replication only occurs when a professional enters a command into the database, so it's not an automatic process. With this type, your company has more control over the resources used to replicate data but may not possess real-time data backups.

AUTOMATION

- Automation is the process of having tools automatically manage your data. Rather than updating your data manually, you can use software tools to accomplish this task for you.
- For example, you could use a tool to automatically update a shared database whenever you make a change on your local computer, rather than requiring manual updates. This would ensure that the database contains updated information for all users and prevents users from viewing outdated information if a user forgets to submit changes.

DISASTER RECOVERY

- Disaster recovery is a plan companies create for potential scenarios regarding data issues.
- For example, if the hard drive that stores your data breaks, it's important to have an effective plan that allows your business to return to normal operations. This plan might include switching to a backup hard drive, making a new copy of that backup and purchasing a new primary hard drive.
- Important elements in a disaster recovery plan include speed, data integrity and costs. Effective organizations often have plans that decrease technological downtime as much as possible.
- In addition, it's important to prevent loss of essential data.
- Finally, organizations typically aim to reduce costs wherever possible, such as compressing data to save money on storage requirements.