UNIT 4: Advanced Network Design

Security Design Principles, Multicast Concepts, QoS Design, Cloud & Virtual Networks, Design Case Studies.

Security Design Principles

Security design principles are the foundational guidelines used to build secure computer systems, networks, applications, and cloud environments. These principles help organizations protect information assets from threats such as unauthorized access, data breaches, malware, insider attacks, and service disruptions.

1. Introduction to Security Design Principles

What are Security Design Principles?

Security design principles are a set of best practices and guidelines that ensure a system is designed with security as a core requirement from the beginning of development, rather than adding security later.

Why are they important?

1. Protect sensitive data and resources.
2. Reduce vulnerabilities and attack surfaces.
3. Ensure reliable and continuous system operation.
4. Support compliance with security standards and regulations.
5. Build trust among users and organizations.

2. Objectives of Security Design

The main objectives are based on the CIA Triad:

CIA Triad Diagram



1. Confidentiality

Ensures that information is accessible only to authorized users.

- Encryption
- Access control
- Authentication mechanisms

Example: Encrypting customer passwords in a database.

2. Integrity

Ensures that data remains accurate, consistent, and unmodified.

- Hashing
- Digital signatures
- Checksums

Example: Verifying that a downloaded file has not been tampered with.

3. Availability

Ensures that systems and data are accessible when needed.

- Redundant servers
- Backups
- High Availability (HA)

Example: A website remaining online even if one server fails.

3. Major Security Design Principles

3.1 Principle of Least Privilege

Definition:

Users, applications, and processes should be given only the minimum permissions necessary to perform their tasks.

Explanation

Limiting privileges reduces the risk of accidental or malicious misuse of resources.

Example

A student account can view course materials but cannot modify examination records.

Benefits

- Reduces attack impact.
- Prevents unauthorized actions.
- Improves accountability.

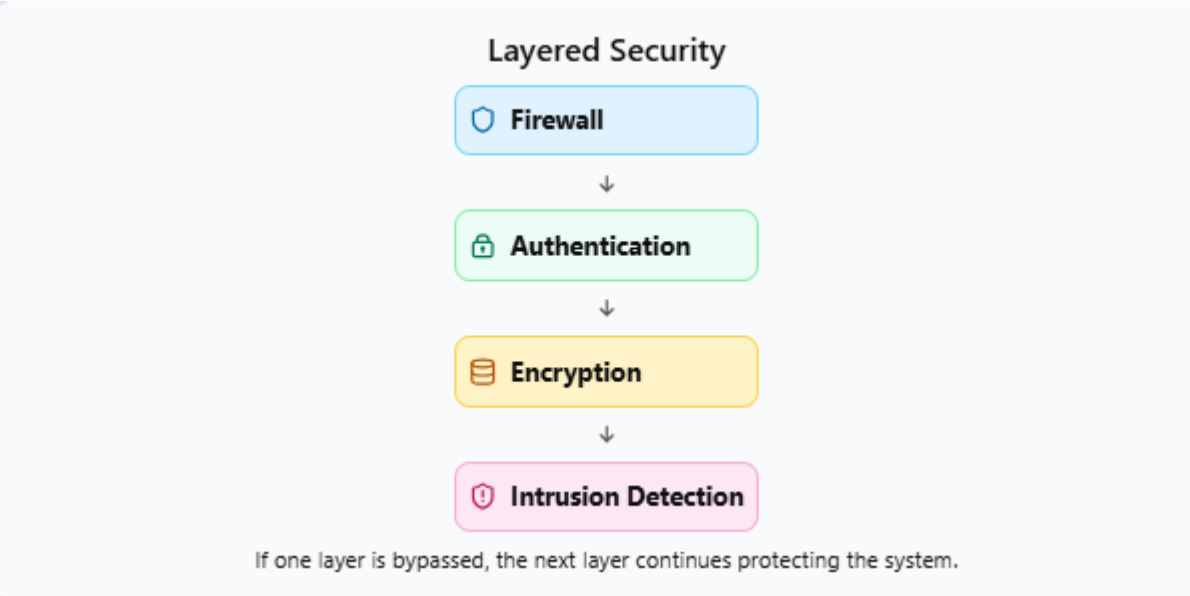
This principle is widely implemented using Role-Based Access Control (RBAC).

3.2 Defense in Depth

Definition:

Security should be implemented in multiple layers so that if one layer fails, others continue to provide protection.

Layered Security Diagram



Explanation

No single security mechanism is sufficient. Multiple independent controls provide stronger protection.

Examples

1. Firewall filters incoming traffic.
2. Antivirus detects malware.
3. Multi-factor authentication verifies users.
4. Encryption protects stored data.

Benefits

- Improves resilience against attacks.
- Reduces single points of failure.
- Provides comprehensive protection.

3.3 Fail-Safe Defaults

Definition:

Access should be denied by default unless explicitly permitted.

Explanation

A secure system starts with no permissions and grants access only when authorized.

Example

A newly created user account has no access rights until an administrator assigns them.

Benefits

- Prevents accidental exposure of resources.
- Reduces unauthorized access.
- Enforces strict access control.

3.4 Economy of Mechanism (Simplicity)

Definition:

Security mechanisms should be simple, small, and easy to understand.

Explanation

Complex systems are harder to test, maintain, and secure. Simplicity reduces the chance of security flaws.

Example

A simple password policy is easier to enforce than a highly complicated authentication process.

Benefits

- Fewer vulnerabilities.
- Easier maintenance and auditing.
- Improved reliability.

3.5 Complete Mediation

Definition:

Every access request to a resource must be checked for authorization.

Explanation

The system should not assume that a user who was previously authenticated is always authorized for future requests.

Example

Each time a user accesses a confidential file, the system verifies their permissions.

Benefits

- Prevents unauthorized access.
- Ensures consistent enforcement of security policies.
- Improves accountability.

3.6 Open Design

Definition:

Security should not depend on secrecy of the system design or implementation.

Explanation

A system should remain secure even if its design is publicly known. Only secret keys or credentials should remain confidential.

Example

The AES encryption algorithm is publicly available, but data remains secure because the encryption key is secret.

Benefits

- Allows public review and testing.
- Builds trust in security mechanisms.
- Encourages strong cryptographic practices.

3.7 Separation of Privilege

Definition:

Access to critical operations should require multiple conditions or approvals.

Explanation

No single user or process should have complete control over sensitive operations.

Example

A financial transaction above a certain amount requires approval from two managers.

Benefits

- Reduces insider threats.
- Prevents abuse of power.
- Improves accountability and oversight.

3.8 Least Common Mechanism

Definition:

Minimize the sharing of resources among users and processes.

Explanation

Shared resources can become channels for information leakage or attacks.

Example

Different departments use separate file servers and user accounts.

Benefits

- Limits information leakage.
- Reduces attack surfaces.
- Improves isolation between users.

3.9 Psychological Acceptability

Definition:

Security mechanisms should be easy for users to understand and use.

Explanation

If security controls are too complicated, users may avoid or bypass them.

Example

A simple and user-friendly multi-factor authentication app encourages users to adopt it.

Benefits

- Improves user compliance.
- Reduces human errors.
- Enhances overall security effectiveness.

3.10 Accountability and Auditing

Definition:

All significant system activities should be recorded and monitored.

Explanation

Audit logs help detect suspicious activities, investigate incidents, and ensure compliance.

Example

Recording login attempts, file access, and administrative actions in system logs.

Benefits

- Detects security incidents early.
- Supports forensic investigations.
- Ensures compliance with regulations.

4. Security Design Process

A professional security design typically follows these steps:

1. Requirement Analysis
2. Risk Assessment
3. Security Architecture Design
4. Implementation
5. Testing and Validation
6. Monitoring and Maintenance

5. Real-World Applications

Banking Systems

- Multi-factor authentication.
- Encryption of transactions.
- Separation of duties for approvals.
- Continuous monitoring and auditing.

Cloud Computing

- Identity and Access Management (IAM).
- Network segmentation.
- Redundant infrastructure for availability.
- Encryption of data at rest and in transit.

Healthcare Systems

- Least privilege for medical staff.
- Audit logs for patient record access.
- High availability for critical medical applications.

Multicast Concepts

Introduction

Multicasting is a communication method in computer networks where a sender transmits data to a **group of interested receivers** simultaneously. Instead of sending separate copies to each receiver (unicast) or sending to all devices (broadcast), multicast sends data only to members of a multicast group.

Types of Data Transmission

1. Unicast

- One sender → One receiver.

- Example: Accessing a website.

Sender ----> Receiver

2. Broadcast

- One sender → All devices in the network.
- Example: ARP requests.

--> Device 1
Sender --> Device 2
--> Device 3
--> Device 4

3. Multicast

- One sender → Selected group of receivers.
- Example: Live video streaming.

--> Receiver 1
Sender ----> Receiver 2
--> Receiver 3

Multicast Group

A **multicast group** is a collection of devices interested in receiving the same data stream.

Features

- Devices can join or leave at any time.
- Each group is identified by a multicast IP address.
- Reduces network bandwidth usage.

Multicast IP Addressing

IPv4 Multicast Address Range

- **224.0.0.0 to 239.255.255.255**
- Class D IP addresses

Examples:

- 224.0.0.1 → All hosts
- 224.0.0.2 → All routers

Multicast Components

1. Sender (Source)

- Generates and sends multicast traffic.

2. Receiver

- Joins a multicast group to receive data.

3. Multicast Router

- Forwards multicast packets only to networks with interested receivers.

Internet Group Management Protocol (IGMP)

IGMP is used by hosts and routers to manage multicast group membership.

Functions

- Join multicast groups
- Leave multicast groups
- Report membership status

Versions

- IGMPv1
- IGMPv2
- IGMPv3

Multicast Routing Protocols

These protocols help routers forward multicast traffic efficiently.

1. PIM (Protocol Independent Multicast)

- Most commonly used multicast routing protocol.

2. DVMRP

- Distance Vector Multicast Routing Protocol.

3. MOSPF

- Multicast Open Shortest Path First.

Advantages of Multicast

1. Efficient bandwidth utilization.

2. Reduces network congestion.
3. Scalable for large groups.
4. Ideal for real-time applications.
5. Lowers server workload.

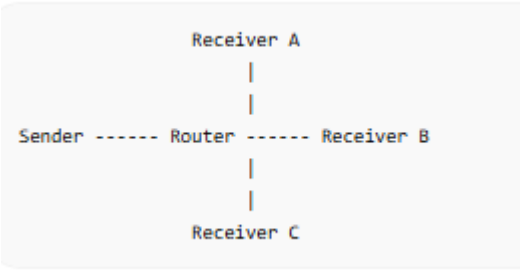
Disadvantages of Multicast

1. Complex network configuration.
2. Requires multicast-enabled routers.
3. Security management is difficult.
4. Not supported by all networks.

Applications of Multicast

- Video conferencing
- Live video streaming
- Online learning platforms
- IPTV services
- Stock market updates
- Multiplayer gaming
- Software distribution

Diagram



QoS (Quality of Service) Design

Definition

Quality of Service (QoS) is a network design technique used to manage and prioritize network traffic so that important applications receive the required bandwidth, low delay, low jitter, and minimal packet loss.

QoS ensures that critical services such as voice calls, video conferencing, and real-time applications perform efficiently even during network congestion.

Objectives of QoS Design

1. Prioritize important traffic.
2. Reduce network congestion.
3. Minimize packet loss.
4. Control delay (latency).
5. Reduce jitter (variation in packet arrival times).
6. Improve overall network performance.

Need for QoS

Without QoS:

- All packets are treated equally.
- Voice and video traffic may suffer delays.
- Network congestion can affect critical applications.

With QoS:

- Important traffic receives higher priority.
- Better user experience.
- Efficient utilization of bandwidth.

QoS Parameters

1. Bandwidth

- Amount of data transmitted per second.
- Measured in bps, Kbps, Mbps, or Gbps.

Example:
A video conferencing application may require 5 Mbps bandwidth.

2. Delay (Latency)

- Time taken for a packet to travel from source to destination.
- Measured in milliseconds (ms).

Formula:

Delay=Processing+Queuing+Transmission+Propagation

3. Jitter

- Variation in packet arrival times.
- High jitter affects voice and video quality.

Example:

- Packet 1 arrives in 10 ms.
- Packet 2 arrives in 30 ms.
- Packet 3 arrives in 15 ms.

This variation is called jitter.

4. Packet Loss

- Occurs when packets are dropped due to congestion or errors.

Effects:

- Poor audio quality.
- Video interruptions.
- Data retransmissions.

QoS Architecture



QoS Design Components

1. Traffic Classification

- Identifies different types of traffic.
- Packets are grouped into classes.

Examples:

- Voice
- Video
- Email
- Web traffic

2. Traffic Marking

- Marks packets according to priority.

Common Marking Methods:

- DSCP (Differentiated Services Code Point)
- IP Precedence

Example:

- Voice traffic → High priority
- Email traffic → Low priority

3. Traffic Policing

- Controls the traffic rate.
- Drops packets that exceed the configured limit.

Advantages

- Prevents bandwidth abuse.
- Maintains network stability.

4. Traffic Shaping

- Delays excess packets instead of dropping them.
- Smooths traffic flow.

Example

Incoming Traffic
|
v
Traffic Shaper
|
v
Smooth Output Traffic

5. Queuing

- Stores packets before transmission.

Types of Queuing

a) FIFO (First In First Out)

- Packets are transmitted in arrival order.

Packet1 -> Packet2 -> Packet3

b) Priority Queuing (PQ)

- High-priority traffic transmitted first.

High Priority Queue
|
Medium Priority Queue
|
Low Priority Queue

c) Weighted Fair Queuing (WFQ)

- Allocates bandwidth fairly among applications.

QoS Design Process

Step 1: Identify Applications

Examples:

- VoIP
- Video conferencing
- Web services

Step 2: Analyze Traffic

Determine:

- Bandwidth requirements
- Delay sensitivity
- Packet loss tolerance

Step 3: Classify Traffic

Create traffic categories.

Step 4: Apply QoS Policies

Assign priorities and bandwidth limits.

Step 5: Monitor Performance

Continuously evaluate network behaviour.

Advantages of QoS Design

1. Improved application performance.
2. Better voice and video quality.
3. Reduced packet loss.
4. Efficient bandwidth utilization.
5. Higher user satisfaction.
6. Better network reliability.

Disadvantages of QoS Design

1. Increased configuration complexity.
2. Higher implementation cost.
3. Requires continuous monitoring.
4. Misconfiguration can degrade performance.

Cloud & Virtual Networks

Introduction

Cloud Networking refers to the use of network resources and services hosted in a cloud environment. It enables users to access applications, storage, and computing resources over the Internet.

Virtual Networking is the creation of software-based networks that operate independently of the underlying physical network infrastructure. It allows devices, servers, and applications to communicate as if they were connected on the same physical network.

Cloud Computing Overview

Cloud computing provides on-demand access to computing resources such as:

- Servers
- Storage
- Databases
- Networking
- Software applications

Characteristics of Cloud Computing

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

Cloud Service Models

1. Infrastructure as a Service (IaaS)

Provides virtualized computing resources over the Internet.

Examples

- Amazon Web Services EC2
- Microsoft Virtual Machines

Benefits

- Flexible
- Scalable
- Cost-effective

2. Platform as a Service (PaaS)

Provides a platform for developing and deploying applications.

Examples

- Google App Engine
- Microsoft App Service

Benefits

- Faster development

- Reduced management effort

3. Software as a Service (SaaS)

Provides software applications through the Internet.

Examples

- Google Workspace
- Microsoft 365

Benefits

- No installation required
- Accessible anywhere

Cloud Deployment Models

1. Public Cloud

- Services available to the general public.
- Managed by cloud providers.

Examples:

- Amazon Web Services
- Microsoft Azure

Advantages

- Low cost
- Easy scalability

2. Private Cloud

- Dedicated to a single organization.
- Greater security and control.

Advantages

- Better privacy
- Customization

3. Hybrid Cloud

Combines public and private clouds.

Advantages

- Flexibility
- Cost optimization

Virtual Networks

A **Virtual Network (VNet)** is a logically isolated network created within a cloud environment.

It allows:

- Virtual machines to communicate.
- Secure connection between resources.
- Network segmentation.

Components of Virtual Networks

1. Virtual Machines (VMs)

Software-based computers running on physical servers.

Features

- Independent operating systems
- Easy deployment
- Resource sharing

2. Virtual Switch (vSwitch)

A software-based switch that connects virtual devices.

Functions

- Packet forwarding
- Traffic management
- Network isolation

Diagram

```
 VM1 ----|
         |
 VM2 ----|---- Virtual Switch ---- Physical Network
```

```
        |
VM3 ----|
```

3. Virtual Router

Routes packets between virtual networks.

Functions

- Traffic routing
- Security policy enforcement

4. Virtual Firewall

Protects virtual resources from unauthorized access.

Functions

- Packet filtering
- Access control
- Threat prevention

Network Virtualization

Network virtualization separates network services from physical hardware.

Benefits

1. Simplified management
2. Improved flexibility
3. Faster deployment
4. Better resource utilization
5. Reduced operational costs

Software Defined Networking (SDN)

SDN is a networking approach where the control plane is separated from the data plane.

Components

1. Application Layer

Contains network applications.

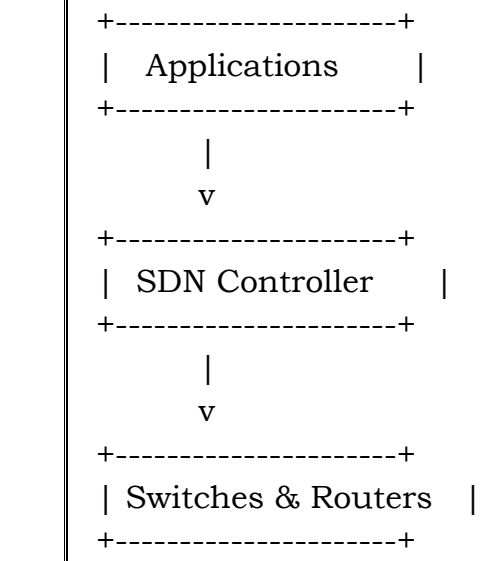
2. Control Layer

Makes routing decisions.

3. Infrastructure Layer

Contains physical and virtual devices.

SDN Architecture



Advantages

- Centralized control
- Easy configuration
- Better scalability

Virtual Private Cloud (VPC)

A **Virtual Private Cloud (VPC)** is a private network inside a public cloud.

Features

- Logical isolation
- Private IP addressing
- Security groups
- Route tables

Advantages

- Enhanced security
- Flexible networking
- Easy scalability

Benefits of Cloud & Virtual Networks

1. Reduced hardware costs
2. Improved scalability
3. Faster deployment

4. Better disaster recovery
5. High availability
6. Centralized management
7. Efficient resource utilization

Design Case Studies

Introduction

A **Design Case Study** is a detailed analysis of how a network is planned, designed, implemented, and managed to meet the requirements of an organization. It helps understand real-world applications of network design principles such as scalability, security, reliability, performance, and cost-effectiveness.

Objectives of Network Design Case Studies

1. Understand business requirements.
2. Design efficient network architectures.
3. Improve security and reliability.
4. Ensure scalability for future growth.
5. Optimize network performance.
6. Reduce operational costs.

Case Study 1: Campus Network Design

Scenario

A university campus consists of:

- Administration Block
- Library
- Computer Labs
- Hostels
- Wi-Fi Zones

The network should support:

- 5000+ users
- Internet access
- Online learning
- VoIP communication

Network Design

Core Layer

- High-speed backbone network.
- Connects all buildings.

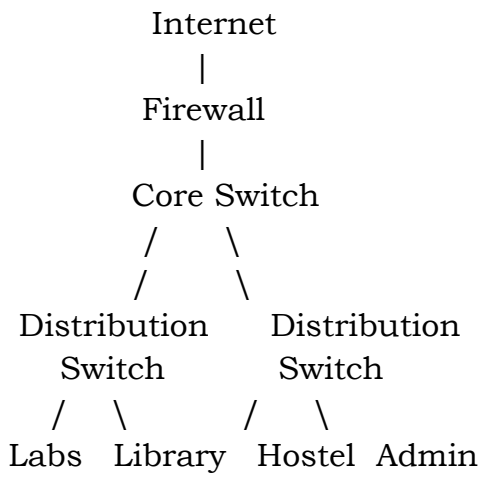
Distribution Layer

- Connects departments and buildings.
- Implements routing and policies.

Access Layer

- Connects end-user devices.

Diagram



Advantages

- Easy management.
- High-speed communication.
- Scalable architecture.
- Enhanced security.

Case Study 2: Enterprise Network Design

Scenario

A company has:

- Headquarters

- Branch Offices
- Remote Employees

Requirements:

- Secure communication
- Video conferencing
- Cloud services
- High availability

Network Design Components

WAN Connectivity

- Connects branches using leased lines or VPN.

Firewall

- Protects corporate resources.

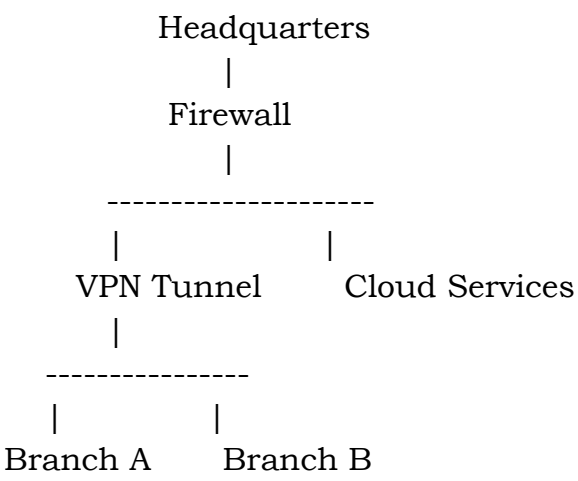
VPN

- Enables secure remote access.

Cloud Integration

- Supports SaaS and business applications.

Diagram



Benefits

- Secure communication.
- Centralized management.

- Business continuity.
- Efficient resource sharing.

Case Study 3: Data Center Network Design

Scenario

A data center hosts:

- Web servers
- Database servers
- Storage systems
- Backup infrastructure

Requirements:

- High availability
- Load balancing
- Redundancy
- Fault tolerance

Design Architecture

Core Switches

- Provide high-speed connectivity.

Load Balancers

- Distribute incoming traffic.

Firewalls

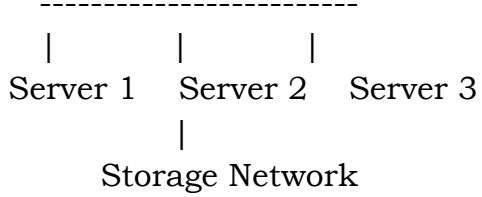
- Secure the data center.

Storage Network

- Supports centralized storage.

Diagram

Internet
|
Firewall
|
Load Balancer
|



Advantages

- Improved performance.
- High availability.
- Better fault tolerance.
- Scalability.

Case Study 4: Cloud-Based Network Design

Scenario

A startup moves its applications to the cloud.

Requirements:

- Cost-effective infrastructure
- Scalability
- Remote access
- Data security

Cloud Network Components

Virtual Private Cloud (VPC)

- Isolated network environment.

Virtual Machines

- Host applications.

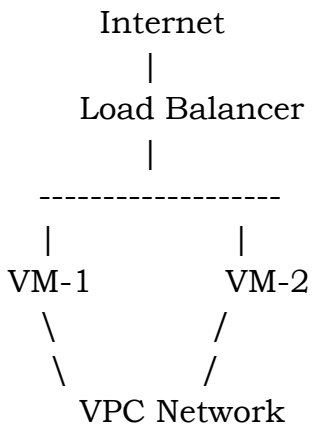
Security Groups

- Control access.

Load Balancer

- Distributes traffic.

Diagram



Benefits

- Reduced infrastructure cost.
- Rapid deployment.
- High scalability.
- Easy maintenance.

Case Study 5: Hospital Network Design

Scenario

A hospital requires:

- Electronic Health Records (EHR)
- Medical imaging systems
- Internet access
- Secure patient data

Network Design

Segmentation

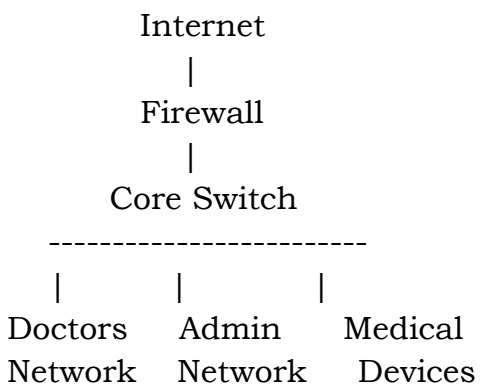
Separate networks for:

- Doctors
- Administration
- Patients
- Medical Devices

Security

- Firewalls
- Access Control Lists (ACLs)
- Encryption

Diagram



Benefits

- Patient data security.
- Reliable healthcare services.
- Network isolation.
- Regulatory compliance.

Design Methodology

Step 1: Requirement Analysis

- Identify business needs.
- Determine user requirements.

Step 2: Logical Design

- Create network topology.
- Define IP addressing scheme.

Step 3: Physical Design

- Select devices and technologies.

Step 4: Implementation

- Deploy the network.

Step 5: Testing and Optimization

- Verify performance and security.