UNIT-1 - Network Design Fundamentals

Network Design Methodology, Hierarchical Network Model, Design Objectives, Scalability Concepts, Network Documentation.

Network Design Methodology:

Network Design Methodology is a **structured approach to planning, designing, and implementing computer networks** so they meet business, technical, and performance requirements. Instead of building networks ad hoc, this methodology ensures scalability, reliability, security, and cost-effectiveness.

◆ 1. Requirements Analysis

This is the foundation. You identify:

- Business goals (e.g., growth, services, budget)
- User requirements (number of users, applications)
- Technical needs (bandwidth, security, uptime)
- Constraints (cost, time, existing infrastructure)

◆ 2. Logical Network Design

Focus on *what* the network should do (not physical devices yet):

- Network topology (star, mesh, hybrid)
- IP addressing scheme
- Routing protocols (OSPF, BGP, etc.)
- Network segmentation (VLANs, subnets)
- Security architecture (firewalls, ACLs)

◆ 3. Physical Network Design

Now define *how* to implement the logical design:

- Hardware selection (routers, switches, cables)
- Physical topology (rack layout, cabling paths)
- Data center or site layout
- Redundancy (backup links, failover systems)

◆ 4. Implementation (Deployment)

- Install devices and configure them
- Apply IP addressing and routing
- Set up security policies
- Integrate with existing systems

◆ 5. Testing and Validation

- Connectivity testing (ping, traceroute)
- Performance testing (throughput, latency)
- Security testing (penetration testing)
- Failover testing

◆ 6. Monitoring and Optimization

- Use monitoring tools (SNMP, NetFlow)
- Track performance and usage
- Identify bottlenecks
- Optimize configurations

◆ 7. Documentation

- Network diagrams (logical & physical)
- Device configurations
- IP addressing tables
- mPolicies and procedures

◆ 8. Maintenance and Scaling

- Upgrade hardware/software
- Expand network capacity
- Apply patches and security updates
- Troubleshoot issues

Hierarchical Network Model

The Hierarchical Network Model is a layered approach used in designing computer networks.

It divides the network into different layers, where each layer performs specific functions.

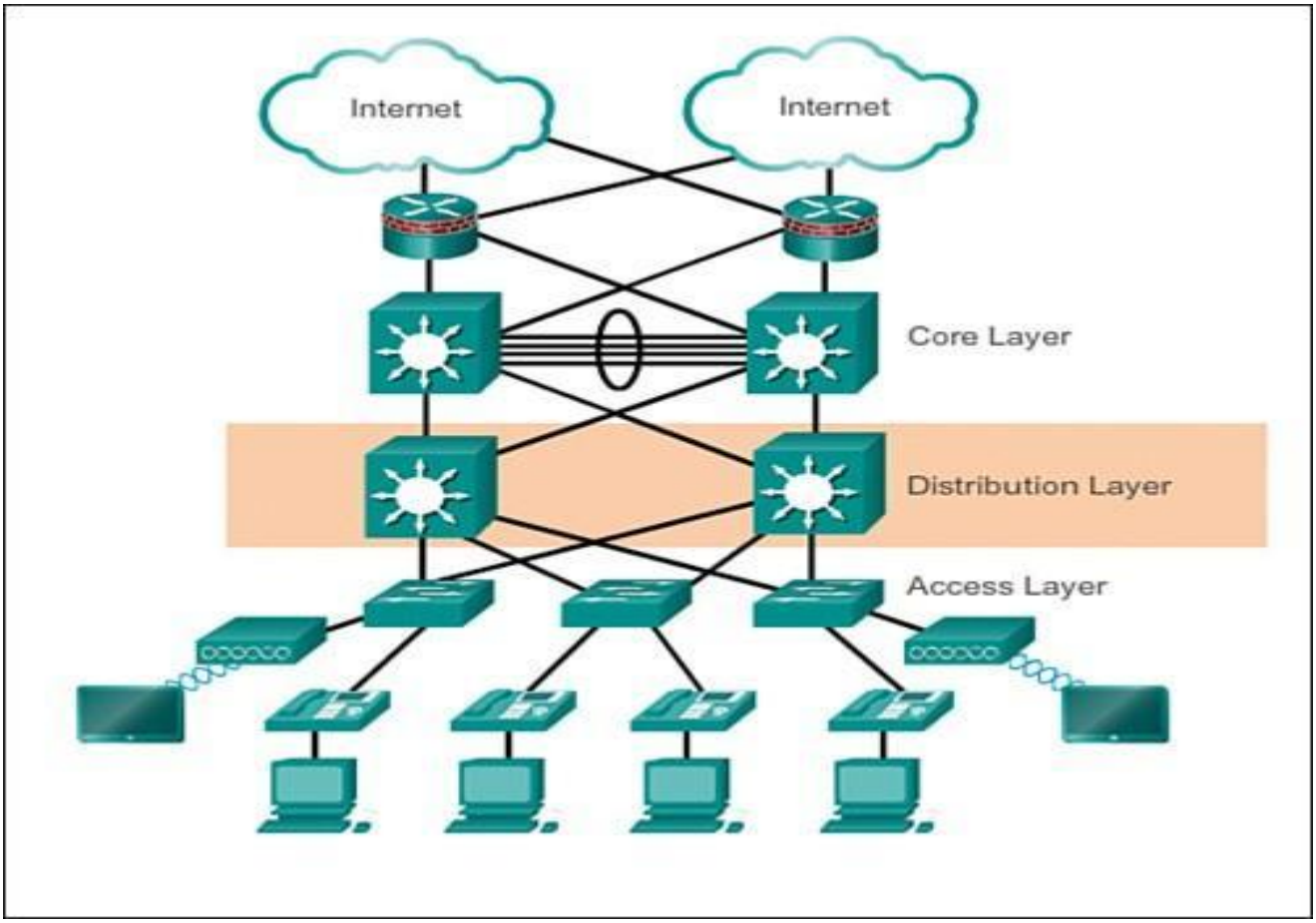
This model helps to:

- Improve network performance
- Simplify management
- Increase scalability
- Enhance security
- Reduce network problems

The most common hierarchical model has three layers:

1. Core Layer
2. Distribution Layer
3. Access Layer

◆ Diagram of Hierarchical Network Model



1. Access Layer

The Access Layer is the lowest layer of the network. It is the layer where end devices connect to the network.

Functions

- Connects PCs, printers, IP phones, and wireless devices
- Provides network access to users
- Controls user access and security
- Supports VLANs and port security

Devices Used

- Access switches
- Wireless access points

Example

In a college:

- Computer lab PCs connect to access switches
- Staff room systems connect through this layer

2. Distribution Layer

- The Distribution Layer acts as the middle layer.
- It connects the access layer to the core layer.

Functions

- Routing between VLANs
- Traffic filtering
- Policy enforcement
- Security implementation
- Load balancing

Devices Used

- Layer 3 switches
- Routers

Example

In an organization:

- Each department network is connected to the distribution switch
- The distribution layer manages communication between departments

3. Core Layer

- The Core Layer is the backbone of the network.

It provides:

- High-speed data transfer
- Reliable communication
- Fast transport between distribution layers

Functions

- High-speed switching
- Fast routing
- Redundancy and fault tolerance
- Devices Used
- High-performance routers
- Core switches

Example

In a university:

- The main data center network acts as the core layer
- It connects all buildings and departments together

Advantages of Hierarchical Network Model

1. Scalability

New devices and departments can be added easily.

2. Easy Management

Each layer has separate responsibilities.

3. Better Performance

Traffic is managed efficiently.

4. Improved Security

Security policies can be applied at distribution layer.

5. Fault Isolation

Problems can be identified quickly.

◆ **Disadvantages**

1. High Initial Cost

Requires multiple networking devices.

2. Complex Design

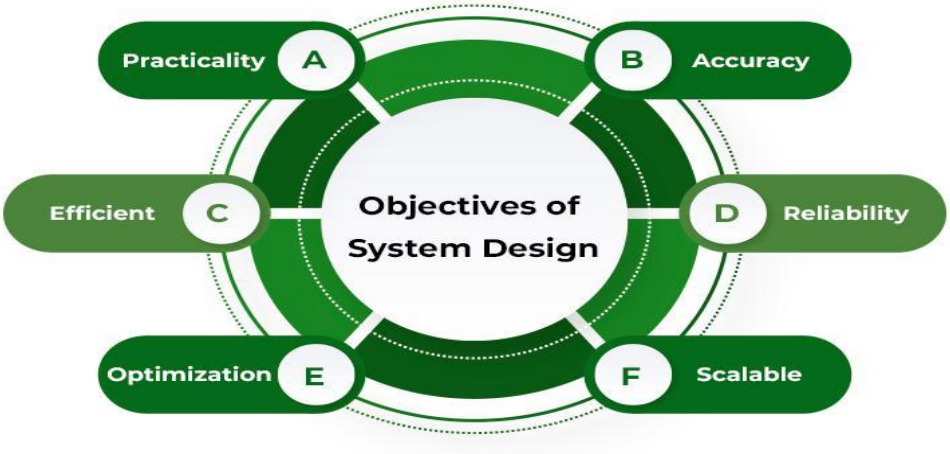
Needs proper planning and configuration.

3. Dependency on Core Layer

Failure in core layer may affect entire network.

Design Objectives in Network Design

Design Objectives are the **goals and requirements** that guide the planning and implementation of a computer network.
These objectives ensure that the network operates efficiently, securely, and reliably according to organizational needs.



1. Scalability

Scalability means the network should support future growth without major redesign.

Features

- Easy addition of new users and devices
- Expansion of departments and branches
- Supports increasing traffic

Example

A college network designed for 500 users should later support 2000 users without replacing the entire infrastructure.

2. Reliability

Reliability means the network should work continuously with minimum downtime.

Features

- Backup links
- Redundant devices
- Fault tolerance

Example

If one network link fails, another link automatically carries the traffic.

3. Performance

Performance refers to the speed and efficiency of the network.

Features

- Low latency
- High bandwidth
- Fast data transfer
- Efficient traffic management

Example

Video conferencing and online classes should run smoothly without delay.

4. Security

Security protects the network from unauthorized access and cyber threats.

Features

- Firewalls
- Encryption
- Authentication
- Access control lists (ACLs)

Example

Only authorized staff can access the server room network.

5. Availability

Availability means the network should be accessible whenever users need it.

Features

- 24/7 connectivity
- Backup power systems
- High uptime

Example

Banking networks must remain available all the time for transactions.

6. Manageability

Manageability means the network should be easy to monitor and maintain.

Features

- Centralized management
- Monitoring tools
- Easy troubleshooting

Example

Administrators can monitor all switches and routers from one system.

7. Flexibility

Flexibility means the network can adapt to new technologies and requirements.

Features

- Supports upgrades
- Easy integration of new devices
- Compatible with different technologies

Example

Adding wireless networking to an existing wired network.

8. Cost Efficiency

The network should provide maximum performance within the available budget.

Features

- Efficient resource usage
- Low maintenance cost
- Energy-efficient devices

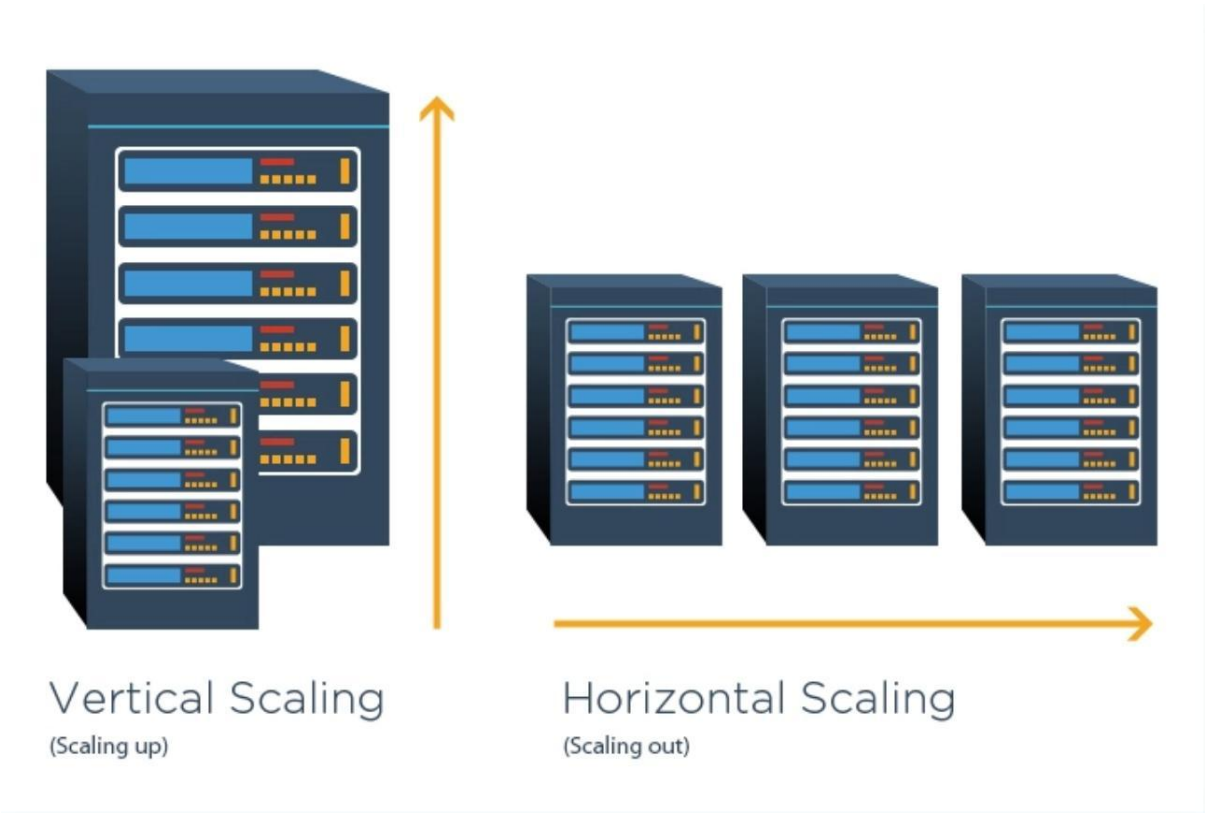
Example

Using VLANs instead of purchasing separate switches for each department.

Scalability Concepts in Computer Networks

Scalability is the ability of a network to **grow and handle increasing users, devices, applications, and traffic** without reducing performance or requiring complete redesign.

A scalable network can expand smoothly as organizational requirements increase.



◆ **Definition**

Scalability refers to:

"The capability of a network system to support future growth efficiently."

This growth may include:

- More users
- More devices
- More branches
- Increased bandwidth
- New services and applications

◆ Importance of Scalability

Scalability is important because organizations continuously grow.

Without scalability:

- Network congestion increases
- Performance decreases
- Maintenance becomes difficult
- Costs become higher

◈ Types of Scalability

1. Vertical Scalability (Scale-Up)

Vertical scalability means increasing the capacity of existing devices.

Methods

- Upgrading CPU
- Increasing RAM
- Adding storage
- Using higher-capacity switches or routers

Example

Replacing a 24-port switch with a 48-port switch.

Advantages

- Simple implementation
- Less configuration changes

Disadvantages

- Hardware upgrade cost is high
- Limited expansion capability

2. Horizontal Scalability (Scale-Out)

Horizontal scalability means adding more devices to the network.

Methods

- Adding switches
- Adding routers
- Adding servers
- Expanding network segments

Example

Adding another switch to support a new computer lab.

Advantages

- Easy expansion
- Better fault tolerance
- Supports large networks

Disadvantages

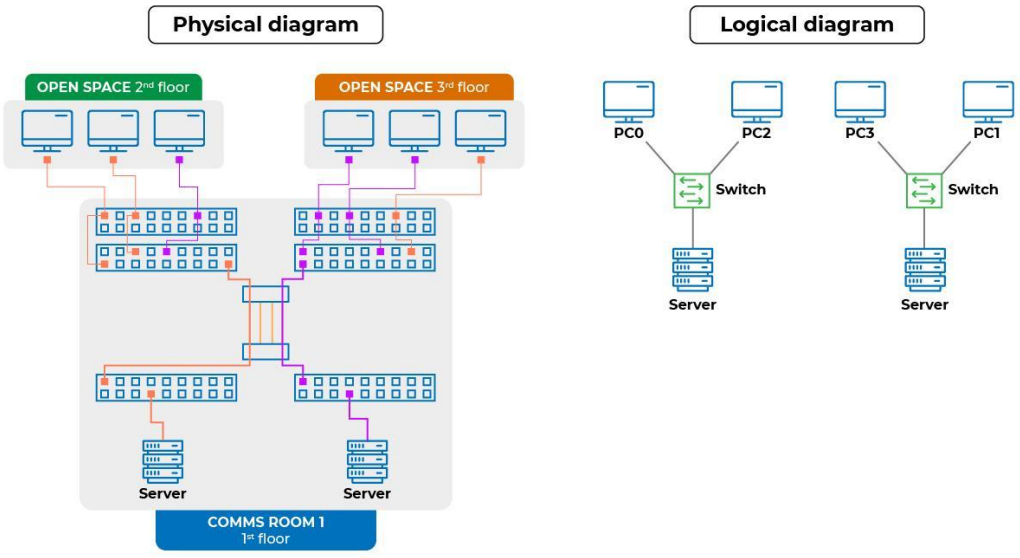
- More complex management
- Requires proper planning

Network Documentation

Network Documentation is the process of recording all important information about a computer network.
It includes details about:

- Network devices
- IP addresses
- Configurations
- Topology diagrams
- Security settings
- Maintenance procedures

Proper documentation helps administrators understand, manage, troubleshoot, and expand the network efficiently.



🔷 Definition

Network Documentation is a collection of records, diagrams, configurations, and technical details related to a network infrastructure.

◆ Importance of Network Documentation

Network documentation is very important because it:

- Simplifies troubleshooting
- Helps in network maintenance
- Supports future expansion
- Reduces downtime
- Improves security management
- Assists new administrators

◆ Types of Network Documentation

1. Physical Network Documentation

Shows the physical arrangement of devices and cables.

Includes

- Device locations
- Cable connections
- Rack layouts
- Patch panels

Example

Switches placed in server racks and cable paths between rooms.

2. Logical Network Documentation

Shows how data flows through the network.

Includes

- IP addressing
- VLAN structure
- Routing information
- Network topology

Example

Communication between departments using VLANs.

3. Configuration Documentation

Contains device configuration details.

Includes

- Router configuration
- Switch settings
- Firewall rules

- Wireless settings

Example

Cisco router configuration commands.

4. Security Documentation

Contains security-related information.

Includes

- Firewall policies
- Access control lists (ACLs)
- User permissions
- VPN settings

Example

Rules allowing only authorized users to access servers.

5. Operational Documentation

Used for daily network operations.

Includes

- Backup procedures
- Troubleshooting guides
- Maintenance schedules
- Monitoring reports