
BCA
Semester - 5th

Computer Network, Security and Cyber Law

Notes - 1

Contents

Computer Network: Introduction: Definition, its use, goals and structure, network architecture, ISO reference model, Network Model, Connecting Devices, TCP/IP, UDP Network Topology: Topology Design process, connectivity analysis, Delay analysis, Backbone design, Logical Access Design.

Introduction

A computer network is a system in which two or more computers and other devices are connected together to share information, resources, and services.

It allows users to communicate, exchange data, and access shared resources like printers, files, and the internet easily.

Example: When you send an email, browse a website, or share a file over Wi-Fi, you are using a computer network.

Definition

A computer network is defined as:

“A collection of interconnected computers and devices that communicate and share resources (such as data, applications, and hardware) using communication channels.”

In simple words, it means connecting computers together through cables or wireless links to share information.

Uses of Computer Network

Computer networks are used in almost every field. Some important uses are:

Point 1: Resource Sharing – Devices like printers, scanners, and storage can be shared among multiple computers.

Point 2: Data Sharing – Users can share files, documents, images, and videos quickly and easily.

Point 3: Communication – Enables email, chat, video conferencing, and social networking.

Point 4: Remote Access – Users can access data or applications from any location through the internet.

Point 5: Centralized Data Management – Data can be stored and managed on a central server for easy access and security.

Point 6: Entertainment and Media – Streaming music, videos, and online gaming are possible due to networks.

Goals of Computer Network

The main goals of computer networks are to make communication and resource usage efficient, reliable, and cost-effective.

Point 1: Resource Sharing – To allow multiple users to use hardware and software resources.

Point 2: Reliability – To ensure data is transmitted correctly and securely.

Point 3: Scalability – The network can grow easily by adding more devices.

Point 4: Cost Efficiency – Reduces the cost of hardware and data management through sharing.

Point 5: Performance Improvement – Increases speed of data access and processing through distributed computing.

Point 6: Security – Protects data from unauthorized access and cyber threats.

Structure of Computer Network

The structure of a computer network defines how different devices are connected and communicate with each other. It includes:

(a) Network Components:

Nodes: Devices like computers, printers, or routers.

Links: The communication paths (wired cables or wireless signals).

Switches and Routers: Devices that direct data to its destination.

Servers and Clients:
Server: Provides resources or services.
Client: Requests services from the server.

(b) Network Topology:

It represents the physical or logical layout of the network. Common topologies are:

Bus Topology – All devices connected to a single cable.

Star Topology – All devices connected to a central hub.

Ring Topology – Devices connected in a circular path.

Mesh Topology – Every device connected to every other device.

(c) Communication Channels:

Wired – Uses cables like Ethernet, coaxial, or fiber optics.

Wireless – Uses radio waves, Wi-Fi, or Bluetooth.

(d) Network Types:
LAN (Local Area Network) – Within a small area like a building.

MAN (Metropolitan Area Network) – Covers a city.

WAN (Wide Area Network) – Covers large areas like countries or globally (e.g., Internet).

Summary
A computer network connects multiple computers to share resources, data, and communication efficiently. Its main uses include resource sharing, communication, and remote access. The goals are efficiency, reliability, scalability, and security. The structure includes hardware components, topologies, communication channels, and types of networks.

Network Architecture

Definition:
Network architecture is the overall design or structure of a computer network that defines how data is transmitted, how devices are connected, and how communication occurs between them.

In simple words, it is a blueprint that shows how computers and network devices interact and share data.

Main Features of Network Architecture:
Defines Layers: It divides the communication process into layers, where each layer performs a specific function.

Specifies Protocols: It defines rules (protocols) for data communication.

Standardization: Ensures that different devices and systems can communicate easily.

Scalability: Makes it easy to expand the network.

Security and Reliability: Provides secure and error-free data transmission.

Types of Network Architecture:
(a) Peer-to-Peer (P2P) Architecture:
Each computer acts as both client and server.

No central control.

Example: File sharing between two computers via Bluetooth or Wi-Fi.

(b) Client-Server Architecture:
There is a central server that provides resources and services.

Other computers act as clients that request services.

Example: Web servers providing web pages to browsers.

Advantages of Network Architecture:
Better organization and communication between devices.

Simplifies troubleshooting and network design.

Helps achieve standard and efficient data exchange.

ISO Reference Model (OSI Model)

Full Form: ISO → International Organization for Standardization

OSI Model → Open Systems Interconnection Model

Definition:
The OSI model is a conceptual framework that defines how data travels from one computer to another in a network using seven layers.

Each layer performs specific functions to complete the communication process.

It was developed by ISO in 1984 to standardize network communication.

The 7 Layers of OSI Model (Bottom to Top):

Layer No.	Layer Name	Function
7	**Application Layer**	Provides user
6	**Presentation Layer**	Translates, encrypts,
5	**Session Layer**	Manages sessions or
4	**Transport Layer**	Ensures reliable
3	**Network Layer**	Handles routing and
2	**Data Link Layer**	Responsible for error
1	**Physical Layer**	Deals with actual

Example (Simple Understanding):
When you send a message online:

Physical layer sends signals →

Data Link ensures no error →

Network finds path →

Transport delivers safely →

Session manages link →

Presentation converts format →

Application shows message on your screen.

Advantages of OSI Model:
Standardization – Common structure for all network types.

Troubleshooting – Easy to identify problems layer by layer.

Flexibility – Each layer can be modified without affecting others.

Interoperability – Allows communication between different systems.

Network Models

A network model defines how data communication is organized, controlled, and managed within a network.

It shows how layers interact and what protocols they use.

There are mainly two network models used in networking:

(a) OSI Model (Open Systems Interconnection)
Developed by ISO (International Organization for Standardization).

Has 7 layers (as explained above).

Theoretical model (used for understanding and teaching).

Purpose: To provide a standard for different systems to communicate easily.

(b) TCP/IP Model (Transmission Control Protocol / Internet Protocol)
Developed by the U.S. Department of Defense (DoD).

Practical model used in real-world Internet communication.

Has 4 layers only.

TCP/IP Layer	Corresponding OSI	Main Functions
Application Layer	Application,	Provides network
Transport Layer	Transport	Responsible for
Internet Layer	Network	Handles addressing
Network Access Layer	Data Link + Physical	Deals with hardware

Comparison: OSI vs TCP/IP

Basis	OSI Model	TCP/IP Model
Layers	7	4
Developed by	ISO	DoD
Use	Theoretical	Practical (used in
Protocols	Generic	Uses TCP, IP, HTTP,
Example	For study purpose	Used in real

Summary

Network Architecture defines the structure and communication method of a network (like Client-Server or P2P).

ISO Reference Model (OSI) provides a 7-layer framework for standardized communication.

Network Models (OSI and TCP/IP) describe how data is transmitted, processed, and received between devices.

Connecting Devices

Definition:
Connecting devices are the hardware components used to connect multiple computers or network segments together to enable data communication.

They act as bridges, filters, or managers for the data traveling through the network.

Types of Connecting Devices:
(a) Network Interface Card (NIC)
It is a hardware component that connects a computer to the network.

Also called LAN card.

Converts data into electrical signals for transmission.

Can be wired (Ethernet) or wireless (Wi-Fi).

Example: Every computer connected to the internet or LAN uses an NIC.

(b) Repeater
Used to extend the range of a network.

It receives weak signals, amplifies them, and then retransmits them.

Works at the Physical Layer (Layer 1) of the OSI model.

Example: Used in long-distance networks to boost signal strength.

(c) Hub
A basic device that connects multiple computers in a network.

When data comes to one port, it sends (broadcasts) it to all other ports.

Works at Physical Layer.

It does not filter data, so it is less secure and slower.

Example: Small office networks or early LAN setups.

(d) Switch
More intelligent than a hub.

Sends data only to the specific device (destination MAC address).

Works at Data Link Layer (Layer 2).

Increases network speed and security.

Example: Used in most modern LAN networks.

(e) Bridge
Connects two similar networks (like two LANs) and filters traffic.

Works at Data Link Layer (Layer 2).

Reduces network congestion.

Example: Connecting two office floors with separate LANs.

(f) Router
Connects different networks (like LAN to WAN or Internet).

Works at Network Layer (Layer 3).

Selects the best path for data packets using IP addresses.

Example: The device that connects your home Wi-Fi to the Internet.

(g) Gateway
Connects two different types of networks (using different protocols).

Works at multiple layers of the OSI model.

Acts as a translator between systems.

Example: Connecting a company's private network to the public Internet.

Summary of Connecting Devices:

Device	OSI Layer	Function
NIC	Layer 1 & 2	Connects computer
Repeater	Layer 1	Strengthens signals
Hub	Layer 1	Broadcasts data to
Switch	Layer 2	Sends data to
Bridge	Layer 2	Connects similar
Router	Layer 3	Connects different
Gateway	Multiple	Connects networks

TCP/IP (Transmission Control Protocol / Internet Protocol)

Definition:
TCP/IP is a set of communication protocols used to connect computers on the Internet.

It defines how data should be packaged, transmitted, and received across networks.

It is the foundation of the Internet and is used for almost all online communication.

Full Form:
TCP: Transmission Control Protocol
IP: Internet Protocol

Functions:
TCP ensures reliable data transfer between computers.

IP handles addressing and routing of data packets.

Together, they make sure data goes from source → destination correctly.

Layers of TCP/IP Model:

Layer	Functions	Examples
Application Layer	Provides user services	HTTP, FTP, SMTP
Transport Layer	Ensures reliable	TCP, UDP
Internet Layer	Handles addressing	IP, ICMP
Network Access Layer	Manages hardware	Ethernet, Wi-Fi

Working Example:
When you open a website:

Application Layer: Browser sends a request (HTTP).

Transport Layer: TCP ensures data arrives safely.

Internet Layer: IP decides path to reach the website's server.

Network Access Layer: Sends the data physically via network cables or Wi-Fi.

Features of TCP/IP:
Open and standard protocol.

Provides reliable and connection-oriented communication.

Enables interoperability between different systems.

Used globally in Internet communication.

UDP (User Datagram Protocol)

Definition:
UDP is a simple and fast communication protocol used for sending data without checking if it is received correctly.

It is connectionless and does not guarantee delivery, but it is faster than TCP.

Full Form: User Datagram Protocol
Works at: Transport Layer (Layer 4) of the OSI Model.

Characteristics of UDP:
Connectionless: No connection is established before sending data.

Unreliable: Data may get lost or arrive out of order.

Fast Transmission: No error-checking, hence quicker than TCP.

Used for Real-Time Applications: Audio/video streaming, gaming, VoIP, etc.

Comparison: TCP vs UDP

Basis	TCP	UDP
Full Form	Transmission Control	User Datagram
Type	Connection-oriented	Connectionless
Reliability	Reliable (checks	Unreliable (no delivery
Speed	Slower	Faster
Error Checking	Yes	No
Example Uses	Email, Web browsing,	Online gaming, Video

Summary
Connecting Devices help build and connect networks (like switches, routers, bridges, etc.).

TCP/IP is the main communication protocol of the Internet that ensures reliable data transmission.

UDP is a lightweight protocol for fast communication where speed is more important than accuracy.

Network Topology

Definition:
Network topology refers to the arrangement or layout of computers, cables, and other network devices within a computer network.

It shows how devices are physically or logically connected and how data flows between them.

In simple words, topology = structure or map of a network.

Types of Network Topologies (Basic Overview):
Bus Topology – All devices connected to a single communication line.

Star Topology – All devices connected to a central hub or switch.

Ring Topology – Each device connected in a circular path.

Mesh Topology – Every device connected to every other device.

Tree Topology – Combination of star and bus topologies.

Hybrid Topology – Combination of two or more topologies.

Topology Design Process

Definition:
The Topology Design Process is the step-by-step method of planning and creating a network layout that meets performance, cost, and reliability requirements.

It ensures that all devices are properly connected, and the network works efficiently.

Steps in Topology Design Process:

Step 1: Requirement Analysis

Identify the purpose of the network.

Understand user needs, number of computers, data volume, and type of communication (voice, data, video).

Example: A school network needs 50 computers connected to a central server.

Step 2: Selecting Topology Type

Choose the suitable topology (Bus, Star, Ring, Mesh, etc.) based on:

Size of the network

Cost of cables and devices

Performance and reliability needed

Ease of maintenance

Example: Star topology is best for small offices, while Mesh is suitable for high-reliability systems.

Step 3: Network Device Selection

Choose suitable connecting devices like switches, routers, hubs, and gateways.

Select cables (Ethernet, fiber optic, etc.) depending on speed and distance.

Step 4: Network Layout Design
Draw a diagram (logical and physical) showing all connections and devices.

Decide how nodes will communicate and where central devices will be placed.

Plan IP addressing and routing paths.

Step 5: Performance Evaluation
Check network performance, reliability, and fault tolerance.

Use simulation tools or mathematical models to test data flow and delays.

Step 6: Implementation and Testing

Install and configure the network physically.

Test connectivity, data transfer speed, and error handling.

Make necessary adjustments for better performance.

In short:
→ Analyze needs → Choose topology → Select devices → Design layout → Test performance → Implement.

Connectivity Analysis

Definition:
Connectivity analysis means checking whether all nodes (devices) in a network are properly connected and can communicate with each other as per design.

It ensures there is no isolated node or disconnected part in the network.

Purpose:
To ensure every node can reach every other node (directly or indirectly).

To identify weak points or failures that can break communication.

To test network reliability before implementation.

Methods of Connectivity Analysis:
(a) Degree of Connectivity
It shows how well nodes are connected.

Example: In a fully connected (mesh) network, each node is directly connected to all others, giving maximum connectivity.

(b) Graph Representation
The network is represented as a graph, where:
Nodes (vertices) = computers or devices
Edges (links) = communication paths

Connectivity can be tested using graph theory (checking if all nodes are reachable).

(c) Redundancy Check
Ensures alternate paths are available in case of failure.

Example: If one link breaks, data can still travel via another route.

Example:
In a star topology, if the central hub fails, all devices lose connection → low connectivity reliability.

In a mesh topology, even if one link fails, data can still pass through other paths → high connectivity.

Delay Analysis

Definition:
Delay analysis is the process of calculating how much time data takes to travel from one device to another in a network.

It helps to measure network performance and speed.

Types of Delays:
(a) Transmission Delay
Time taken to push all bits of a packet onto the link.

Depends on packet size and data rate.

Formula : Transmission Delay = Packet Size/Bandwidth

Example: 1 MB file over 10 Mbps link = 0.8 seconds.

(b) Propagation Delay
Time taken for data to travel from sender to receiver through the medium.

Depends on distance and signal speed.

Formula : Propagation Delay = Distance/Propagation Speed

Example: Data traveling 2000 km through optical fiber (2×10^8 m/s) → 10 ms delay.

(c) Queuing Delay
Time a packet waits in a queue before being transmitted.

Happens when network traffic is high or router is busy.

(d) Processing Delay
Time taken by routers or switches to process packet headers and make routing decisions.

Total Network Delay:
Total Delay = Transmission + Propagation + Queuing + Processing Delay

Importance of Delay Analysis:
Helps to find bottlenecks in the network.

Ensures real-time applications (video calls, gaming) run smoothly.

Used in network optimization and design decisions.

Summary

Concept	Meaning	Purpose
Network Topology	Arrangement of	Defines structure of
Topology Design	Steps to plan and	For efficient, cost-
Connectivity Analysis	Checks if all nodes are	Ensures reliable
Delay Analysis	Calculates time taken	Measures network

Backbone Design

Definition:
Backbone design refers to the central part of a computer network that connects different LANs, segments, or buildings together.

It acts like the main highway for data, carrying large amounts of information between various parts of the network.

In simple words, the backbone is the core network that joins all sub-networks (LANs, departments, or floors) to make a single big network.

Purpose of Backbone Design:
To provide high-speed data communication between different parts of an organization.

To connect multiple LANs into a larger enterprise network.

To ensure efficient and reliable communication across long distances.

Types of Backbone Networks:

(a) Horizontal Backbone

Connects devices or departments on the same floor or building.

Example: Connecting all computers in one office through a switch.

(b) Vertical Backbone

Connects different floors or buildings together.

Often called “building backbone”.

Example: A fiber cable connecting the 1st floor and 3rd floor LANs.

(c) Collapsed Backbone

Uses a central router or switch as the main point of connection.

All segments are connected through this central device.

Easy to manage and secure.

(d) Distributed Backbone

Uses multiple routers or switches connected in hierarchy.

Offers high performance and redundancy (backup paths).

Suitable for large organizations.

Backbone Design Considerations:
When designing a network backbone, the following points are considered:

Speed and Bandwidth:
Backbone must support high-speed data transfer (e.g., 1 Gbps or more).

Reliability:
It should have backup links to avoid total failure.

Scalability:
Easy to expand by adding more LANs or devices.

Cost Efficiency:
Choose between fiber optic or Ethernet depending on budget and need.

Security:
Protect backbone traffic using firewalls and VLANs.

Topology:
Common backbone topologies: Bus, Ring, Star, Mesh, and Hybrid.

Example:
In a university campus:

Each department has its own LAN.

The backbone connects all department LANs to the main server room using fiber optic cables.

This setup allows students and staff to access data or internet from any department.

Advantages of a Good Backbone Design:
High-speed data transfer between networks.

Efficient and reliable communication.

Supports a large number of users.

Easier management and maintenance.

Reduces network congestion (traffic jams).

Logical Access Design

Definition:
Logical access design defines how users, computers, and devices logically (not physically) connect and communicate within a network.

It focuses on data flow, addressing, and permissions rather than physical cables.

In simple words, it's the "software view" of how the network operates — how data moves, who can access what, and how communication is controlled.

Purpose of Logical Access Design:
To organize data communication and access control.

To decide who can access which network resources (like files, printers, databases).

To define logical paths for data transmission.

Key Components of Logical Access Design:

(a) Logical Topology

Describes the path of data flow between devices.
It may differ from physical topology.
Example: In a physically star network, data may flow logically like a ring.

(b) Addressing Scheme

Assigns IP addresses and subnets to all devices.
Ensures unique identification for communication.
Example: IP address 192.168.1.10 identifies a specific computer.

(c) Access Control

Determines who can access what data or service.
Uses permissions, passwords, and authentication systems.
Example: Only the admin can access the server files.

(d) Routing and Switching

Defines how data packets travel through the network.
Routing → choosing best path between networks (Routers).
Switching → transferring data inside the same network (Switches).

(e) VLAN (Virtual LAN) Design

Divides one physical network into multiple logical segments for security and performance.
Example: One VLAN for students and another VLAN for teachers.

(f) Security Policies

Implements firewalls, encryption, and monitoring systems.
Prevents unauthorized access and data theft.

Steps in Logical Access Design Process:
Identify Users and Resources – Who will use the network and what devices are involved.

Define Data Flow – How data will travel between users, servers, and internet.

Plan IP Addressing – Assign subnets and IP ranges.

Define Access Levels – Set permissions for users or groups.

Design VLANs and Routing – For performance and security.

Implement Security Rules – Firewalls, passwords, encryption, etc.

Example (Simple Understanding):
In a company:

HR department can access employee data.

Accounts team can access financial files.

Both are connected to the same physical network, but logically separated using VLANs and access rules.

That’s logical access design — controlling who can communicate or access what.

Advantages of Logical Access Design:
Enhances data security and privacy.

Improves network performance by controlling traffic.

Allows better management of user access.

Provides flexibility — easy to modify access without rewiring.

Simplifies troubleshooting using logical mapping.

Summary

Concept	Meaning	Purpose
Backbone Design	Central structure that connects all LANs or	Provides high-speed, reliable
Logical Access Design	Defines logical communication data	Controls how users and devices

Practice Questions

1. What is a Computer Network? Explain its definition, uses, goals, and structure.
2. Explain Network Architecture and its types.
3. What is the ISO-OSI Reference Model? Describe its seven layers in detail.
4. What are Network Models? Compare the OSI Model and TCP/IP Model.
5. What are Connecting Devices in a computer network? Explain different connecting devices with their functions.
6. What is TCP/IP? Explain its layers and functions.
7. What is UDP? Differentiate between TCP and UDP.
8. What is Network Topology? Explain the topology design process, connectivity analysis, and delay analysis.
9. What is Backbone Design? Explain its types and importance.
10. What is Logical Access Design? Describe its components and advantages.

Check the answer in the Practice Questions section on our website.

Visit Website