INTERNET & WEB PROGRAMMING

By-

Dr. Kailash Aseri
HOD, Department of Computer Science
D.A.V. College, Sri Ganganagar (Raj.)

INTERNET & WEB PROGRAMMING
(4th Semester, Computer Application)

Internet & Web Programming

Duration of Exam: 3 Hours **Maximum Marks:** 150

Internal Exam: 30 Marks **Theory Exam:** 80 Marks **Practical Exam:** 40 Marks

Unit I

Data communication, Transmission Media- Coaxial, UTP, Optical-Fiber, Wireless, Components of Computer Networks, Transmission Mode- Simplex, Half Duplex, Full Duplex, LAN, MAN, WAN, the OSI Model, TCP/IP and others main protocols used on the Web; Types of wireless communication (Mobile, WiFi, WiMAX, Bluetooth, Infrared – concept and definition only). Software Piracy, Firewall, Threats, Hacking and Cracking (basic concepts only for these topics)

Unit II

Evolution of Internet, Introduction to the terms LAN, WAN, MAN, Basic internet terms (Client, Server, MODEM, Web page, Web site, Home page, Browser, URL, ISP, Web server, Download & Upload, Online & Offline etc), Internet applications (Remote login, VoIP, Video Conferencing, Audio-Video streaming, Chatting etc). Identify and solve basic problems related to connecting to networks and the Internet. EMail, Advantages, How it's Works? Anatomy of an e-mail Message, basic of sending and receiving, Email Protocol.

Unit III

Introduction to World Wide Web: History, Working of Web Browsers, Its functions, Search engine category, Concept of Hyper Text Transfer Protocol (HTTP), Web Servers, Internet Explorer, Web publishing Document Interchange Standard, Component of Web Publishing, Site and Domain Name, Overview of Intranet and its applications.

Unit IV

HTML, Designed Tools, HTML Editors, Issue in Web Site Creations and Maintenance, FTP S/W for Upload Website, Elements of HTML & Syntax, Building HTML Documents, Use of Font Size and Attributes, Backgrounds, Formatting tags, Images, Hyperlinks, div tag, List Type and its Tags, Table Layout, , Use of Frames and Forms in Web Pages. Working with Style sheet: Elements and different Type of style sheet; Introduction to Java Script: Identifier & operator, control structure, functions, Predefined functions, numbers & string functions, Array in Java scripts.

Unit V

Basic of Cyber Security and Cyber Crime: Computer Ethics and Application Programs, Cyber Law, Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits.

INDEX

Unit I

I. Data Communication

Data communication refers to the **exchange of digital or analog data between devices** through a transmission medium. It ensures that information is transferred **accurately, efficiently, and securely**.
Data communication simply means sending and receiving information between two or more devices, like computers, phones, or tablets. This information can be in the form of text, images, audio, or video.
Think of it like a conversation between people. Just as we talk and listen to share ideas, devices "talk" to each other by sending data through a path called a transmission medium. This medium can be physical, like cables and wires, or wireless, like Wi-Fi or Bluetooth.
The main goal of data communication is to make sure that the information reaches the right place:

- Accurately (without errors),
- Efficiently (quickly and without wasting resources), and
- Securely (protected from unauthorized access).

For example, when you send a message on your phone, data communication is what allows that message to travel from your device to your friend's device almost instantly.
In short, data communication is what makes modern digital communication possible, connecting devices and helping them share information smoothly.

Characteristics of Effective Data Communication:
1. Delivery (Right Destination)
Data should reach the correct device or person.
For example, if you send a message to your friend, it should go only to them—not to someone else.
2. Accuracy (No Errors)
The data should arrive exactly as it was sent, without any mistakes or changes.
Like sending "Hello" and it should not become "Hillo" or something incorrect.
3. Timeliness (On Time)
Data should be delivered at the right time—not too late.
This is very important for things like video calls or lives streaming, where delays can cause problems.
4. Jitter (Consistent Speed)
Jitter means the variation in the time it takes for data packets to arrive. It should be as low as possible.
If data arrives unevenly (some fast, some slow), it can cause choppy audio or video.
In short: ***Good data communication means the data goes to the right place, stays correct, arrives on time, and flows smoothly without delays or interruptions.***

II. Transmission Media

Transmission media is the **physical or wireless path** through which data travels. Transmission media is simply the **path or way through which data travels** from one device to another. Whenever you send a message, watch a video, or make a call, the information needs a route to move—and that route is called transmission media.
You can think of it like this:
If devices are like people, then transmission media is the **road, air, or bridge** that helps them communicate with each other.
"Transmission media is the **"road" that carries data** between devices—either through **cables (wired)** or **through the air (wireless)**—making communication possible in our daily digital life."

Types of Transmission Media

1. Wired (Guided) Media

- This type uses physical cables to send data.
- Data travels through wires, just like electricity.

Common examples:

- Twisted pair cable (used in internet and telephone lines)
- Coaxial cable (used in TV connections)
- Fiber optic cable (very fast, uses light to send data)

Advantages: Fast, stable, and secure
Disadvantages: Less flexible, needs installation

2. Wireless (Unguided) Media

- This type sends data through the air without using wires.
- Data travels using signals like radio waves.

Common examples:

- Wi-Fi
- Bluetooth
- Mobile networks (4G/5G)

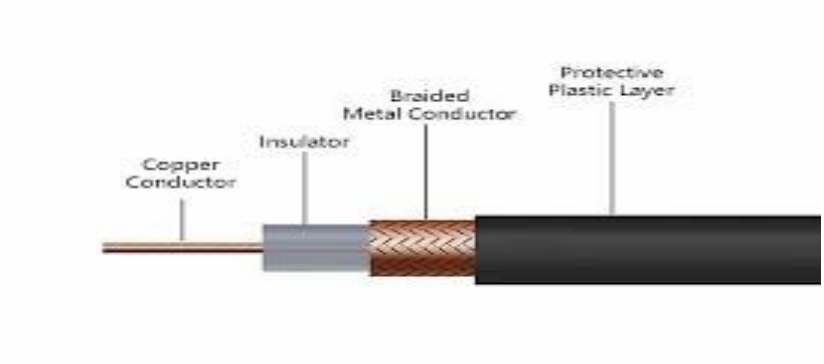
Advantages: Easy to use, no wires, allows movement
Disadvantages: Can be slower or affected by obstacles and interference

Why Transmission Media is Important

- It connects devices like phones, computers, and servers
- It helps data travel quickly and smoothly
- It supports all modern communication like internet browsing, calls, and streaming

1. Coaxial Cable

A coaxial cable is a type of electrical cable used to carry high-frequency signals with minimal interference. It's commonly used in TV connections, internet systems, and radio communications.



Structure of a Coaxial Cable

- It has a unique layered design:
- Inner conductor – Carries the signal (usually copper).
- Dielectric insulator – Keeps the signal insulated.
- Metal shield (braid/foil) – Protects against electromagnetic interference (EMI).
- Outer jacket – Provides physical protection.

How it works

The inner conductor carries the signal, while the outer metallic shield acts as a ground and blocks external interference. This design ensures stable and clear transmission even over long distances.

Common Uses

- Cable TV connections
- Broadband internet (e.g., cable modems)
- CCTV camera systems
- Radio frequency transmission
- Satellite communication

Types of Coaxial Cables

- RG-6 – Most common for TV and internet

- RG-59 – Often used for CCTV
- RG-11 – Used for long-distance, high-quality signals

Advantages

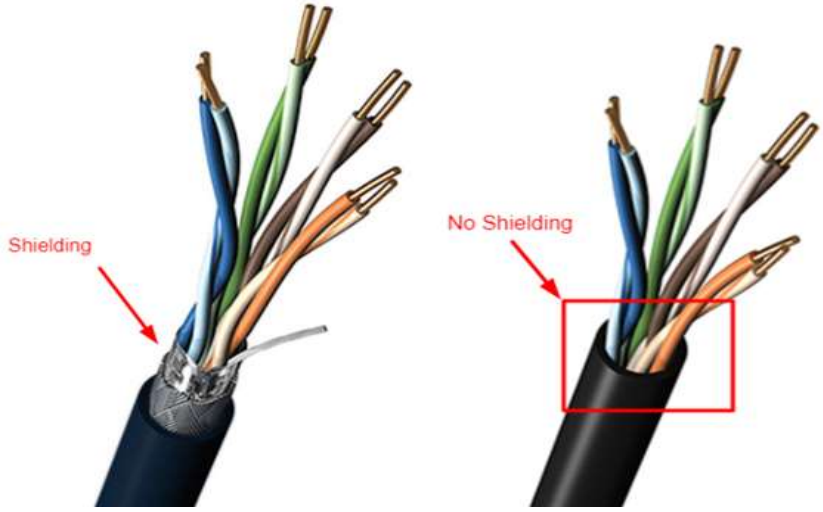
- Good shielding from interference
- Durable and long-lasting
- Supports high-frequency signals

Disadvantages

- Bulkier than newer cables (like fiber optic)
- Limited bandwidth compared to fiber

2. UTP (Unshielded Twisted Pair)

UTP (Unshielded Twisted Pair) is one of the most widely used types of networking cable, especially for Ethernet connections in homes, offices, and data centers.



Structure

A UTP cable contains:

- Pairs of insulated copper wires twisted together
- Typically 4 pairs (8 wires) inside one cable
- No shielding layer (that's why it's called unshielded)
- The twisting helps reduce electromagnetic interference (EMI) and signal crosstalk between wires.

How it works

Each twisted pair carries signals, and the twists cancel out noise from external sources. Even without shielding, this design keeps signal quality stable over typical networking distances.

Common Uses

- LAN (Local Area Network) connections
- Internet/Ethernet cables
- Telephone lines
- Connecting computers, routers, and switches

Categories of UTP Cables

Different categories support different speeds:

- Cat5 – Up to 100 Mbps
- Cat5e – Up to 1 Gbps (most common)
- Cat6 – Up to 10 Gbps (short distances)
- Cat6a / Cat7 – Higher speeds and better performance

Advantages

- Low cost and widely available
- Easy to install and flexible

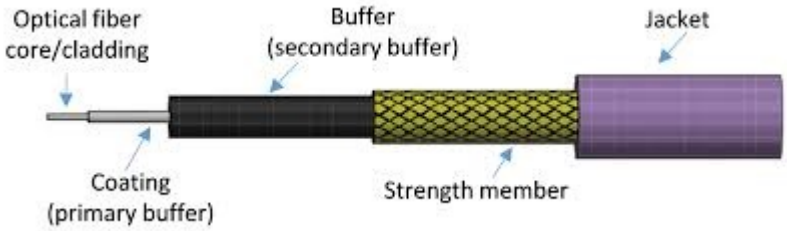
- Lightweight compared to coaxial or fiber

Disadvantages

- More susceptible to interference than shielded cables
- Limited distance (usually up to ~100 meters)
- Lower performance than fiber optics

3. Optical Fiber (Fiber Optic Cable)

Optical fiber is a type of cable that transmits data as light signals instead of electrical signals. It is the fastest and most advanced communication medium used today.



Structure of Optical Fiber

An optical fiber cable has three main parts:

1. **Core**
   - Thin glass or plastic center where light travels
2. **Cladding**
   - Surrounds the core and reflects light back into it using the principle of Total Internal Reflection
3. **Outer jacket**
   - Protects the fiber from damage

How it works

- Data is converted into light pulses
- These light signals travel through the core
- Due to total internal reflection, the light keeps bouncing inside without escaping
- This allows signals to travel very long distances with minimal loss

Types of Optical Fiber

1. **Single-mode fiber (SMF)**
   - Very thin core
   - Used for long-distance communication (telecom networks)
2. **Multi-mode fiber (MMF)**
   - Thicker core
   - Used for shorter distances (LANs, buildings)

Common Uses

- High-speed internet (fiber broadband)
- Cable TV and telecommunication networks
- Medical instruments (endoscopy)
- Military and aerospace communication

Advantages

- Extremely high speed and bandwidth
- Very low signal loss over long distances
- Immune to electromagnetic interference
- More secure (harder to tap signals)

Disadvantages

- More expensive than copper cables
- Fragile and requires careful handling
- Installation is more complex

4. Wireless Media

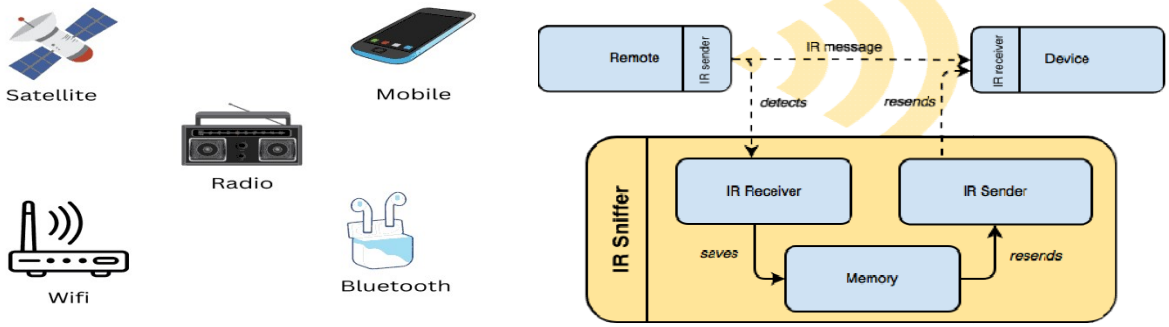
Wireless media refers to communication methods that transmit data without physical cables, using electromagnetic waves through the air or space.

How it works

Data is converted into signals and transmitted using electromagnetic waves such as:

- Radio waves
- Microwaves
- Infrared waves

Devices use transmitters and receivers (like antennas) to send and receive these signals.



Types of Wireless Media

1. Radio Waves
    - Used in radio, TV broadcasting, and Wi-Fi
    - Can travel long distances and pass through walls
2. Microwaves
    - Used in satellite communication and mobile networks
    - Requires line-of-sight (no obstacles in between)
3. Infrared
    - Used in short-range communication (e.g., remote controls)
    - Cannot pass through walls

Common Uses

- Wi-Fi networks
- Mobile phone communication
- Satellite TV and GPS
- Bluetooth devices
- Remote controls

Advantages

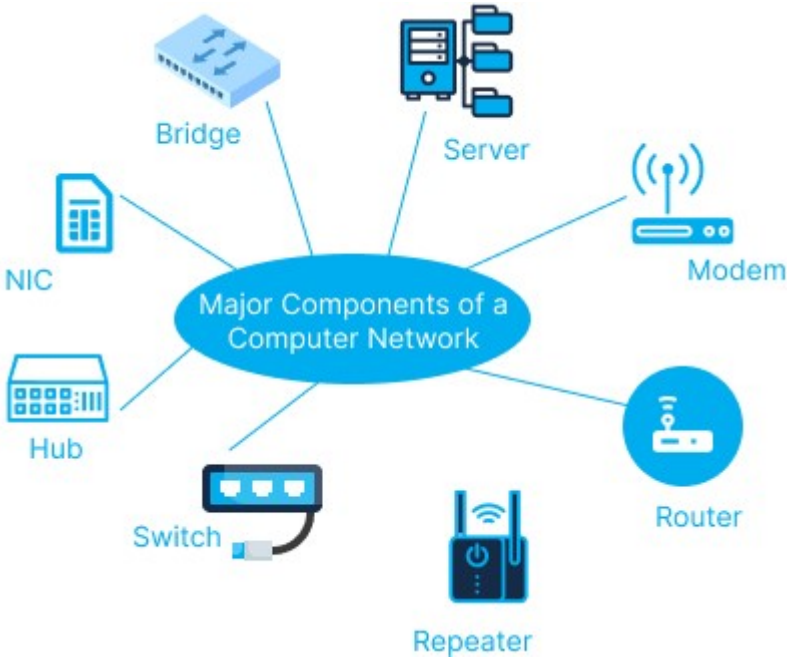
- No cables required (easy installation)
- Mobility and flexibility
- Useful in remote or hard-to-wire areas

Disadvantages

- More interference and signal loss
- Security risks (signals can be intercepted)
- Limited range and speed compared to fiber

III. Components of Computer Networks

A **computer network** is a system in which multiple devices are connected to share data, resources, and services. To make communication possible, a network is made up of several important components. Each component plays a specific role in ensuring smooth and reliable data transfer.



1. Network Devices (Nodes)

A **network node** is any **physical or virtual device** connected to a computer network that is capable of **sending, receiving, processing, or forwarding data**. It acts as a **communication point** within the network and forms the fundamental building block of network architecture.

In a computer network, nodes are interconnected through communication channels such as cables or wireless links. Each node plays a specific role in ensuring that data is transmitted efficiently from one point to another. Without nodes, a network cannot function, as there would be no devices to generate or handle data.

Nodes can be classified into different categories based on their function. **End nodes**, also known as host devices, are responsible for initiating and receiving data. Examples include computers, smartphones, and printers. These devices directly interact with users and are the source or destination of information.

On the other hand, **intermediate nodes** are responsible for controlling and managing the flow of data within the network. Devices such as routers, switches, and gateways fall into this category. They ensure that data packets are directed along the correct path and reach their intended destination.

Each node in a network is identified by a unique address, such as an **IP address** (logical address) or a **MAC address** (physical address). These addresses help in accurately delivering data across the network.

Nodes may also be classified as **active** or **passive**. Active nodes, such as computers and routers, can process and transmit data, whereas passive components like cables and connectors do not perform any data processing and are therefore not considered true nodes.
In modern networks, nodes can also be virtual, such as virtual machines or cloud-based systems, which perform the same functions as physical devices.
In conclusion, network nodes are essential components of a computer network that enable communication, data processing, and resource sharing, making them vital for the operation of any networking system.

Network devices are the physical elements connected in a network. These devices can act as senders, receivers, or both.

- **Computers (Clients):** Used by users to access network resources

- **Servers:** Powerful computers that provide services like file storage, websites, and applications
- **Printers & Other Devices:** Shared resources in the network

These devices are called **nodes** and are essential for communication.

2. Transmission Media

Transmission media refers to the path through which data travels from one device to another.

Types:

- **Wired Media:**
  - Twisted Pair Cable
  - Coaxial Cable
  - Fiber Optic Cable (fastest and most reliable)
- **Wireless Media:**
  - Wi-Fi
  - Bluetooth
  - Satellite communication

The choice of media affects speed, cost, and reliability.

3. Network Interface Card (NIC)

A Network Interface Card (NIC) is a hardware component that enables a computer or other device to connect to a computer network. It acts as an interface between the device and the network, allowing the device to send and receive data.

The NIC is usually installed inside the computer's motherboard or connected externally. It provides a physical connection to the network through cables (wired NIC) or wirelessly (wireless NIC).

Functions of NIC

The Network Interface Card performs several important functions:

Data Transmission and Reception

It converts data from the computer into signals that can be transmitted over the network and vice versa.

Addressing (MAC Address)

Each NIC has a unique MAC (Media Access Control) address, which is used to identify the device on a network.

Data Conversion

Converts digital data into electrical or radio signals and back into digital form.

Network Communication Control

Manages the flow of data between the computer and the network.

Types of NIC

1. Wired NIC

Uses cables (usually Ethernet cables)

Provides stable and high-speed connection

2. Wireless NIC

Uses Wi-Fi technology

Allows connection without physical cables

4. Networking Devices

Networking devices are hardware components used to **connect computers and other devices in a network** and to **facilitate communication and data transfer** between them. These devices ensure that data is transmitted efficiently, securely, and accurately from one device to another. They play a vital role in building and managing both **small networks (LAN)** and **large networks (WAN)** such as the internet.

Types of Networking Devices

1. **Router**

A router is a device that **connects multiple networks** and directs data packets between them using IP addresses. It determines the best path for data transmission and is commonly used to connect a local network to the internet.

2. **Switch**

A switch is used to **connect multiple devices within a local area network (LAN)**. It forwards data only to the intended device using MAC addresses, which improves network efficiency.

3. **Hub**
A hub is a basic networking device that **connects multiple devices** and sends data to all connected devices. It does not filter data, making it less efficient than a switch.

4. **Modem**
A modem (Modulator-Demodulator) is used to **connect a network to the internet**. It converts digital signals into analog signals and vice versa for transmission over communication lines.

5. **Network Interface Card (NIC)**
A NIC is a hardware component that **allows a computer to connect to a network**. It provides a unique MAC address and enables communication between the device and the network.

6. **Access Point (AP)**
An access point provides **wireless connectivity** to devices, allowing them to connect to a wired network using Wi-Fi.

7. **Bridge**
A bridge connects **two similar network segments** and filters traffic to reduce congestion by using MAC addresses.

8. **Repeater**
A repeater is used to **strengthen or regenerate signals** so that they can travel longer distances without losing quality.

9. **Gateway**
A gateway acts as a **protocol converter**, connecting different types of networks and enabling communication between them.

10. **Firewall**
A firewall is a **security device** that monitors and controls incoming and outgoing network traffic, protecting the network from unauthorized access.

5. Protocols

Protocols are a set of rules and standards that govern how data is transmitted, received, and interpreted between devices in a computer network. They ensure that communication between different devices is accurate, reliable, and organized.
Without protocols, devices would not be able to understand each other, even if they are physically connected.

Definition - A protocol is a set of rules that defines how data is communicated between devices in a network.

Functions of Protocols

- Protocols perform several important functions:
- Data Formatting
  Defines how data is structured and presented
- Data Transmission
  Determines how data is sent across the network
- Error Detection and Correction
  Ensures data is transmitted without errors
- Flow Control
  Controls the rate of data transmission to avoid congestion
- Addressing
  Ensures data reaches the correct destination

Types of Network Protocols
1. Transmission Control Protocol (TCP)- Provides reliable and connection-oriented communication Ensures data is delivered correctly and in order
2. Internet Protocol (IP)- Responsible for addressing and routing, Assigns IP addresses to devices
3. HyperText Transfer Protocol (HTTP)- Used for transferring web pages on the internet
4. File Transfer Protocol (FTP)-Used to transfer files between computers
5. Simple Mail Transfer Protocol (SMTP)-Used for sending emails
6. Dynamic Host Configuration Protocol (DHCP)-Automatically assigns IP addresses to devices
7. HyperText Transfer Protocol Secure (HTTPS)-Secure version of HTTP using encryption

Characteristics of Protocols
- Standardized rules
- Platform independent
- Enable interoperability between devices
- Ensure secure and efficient communication

Importance of Protocols
- Enable communication between different devices
- Ensure reliable data transfer
- Provide security and error handling
- Standardize networking processes

Short Exam Definition- Protocols are a set of rules and standards that govern communication between devices in a computer network.

6. IP Address
An **IP Address (Internet Protocol Address)** is a **unique numerical identifier** assigned to each device connected to a computer network. It is used to **identify and locate devices** so that data can be sent and received correctly.
Just like a home address helps in delivering mail to the correct location, an IP address ensures that data reaches the correct device in a network.
Definition- An IP address is a unique numerical label assigned to a device in a network to identify it and enable communication using the Internet Protocol.

Types of IP Addresses
1. IPv4 (Internet Protocol Version 4)
- Most commonly used version
- Written in decimal format
- Example: **192.168.1.1**
- Consists of **4 octets (8 bits each)**

2. IPv6 (Internet Protocol Version 6)
- Newer version developed due to shortage of IPv4 addresses
- Written in hexadecimal format
- Example: **2001:0db8:85a3:0000:0000:8a2e:0370:7334**
- Longer and more secure

Classification of IP Addresses
1. Public IP Address
- Used on the internet
- Assigned by Internet Service Provider (ISP)

2. Private IP Address
- Used within local networks (LAN)
- Not accessible directly from the internet

Functions of IP Address

- **Device Identification**
  Uniquely identifies each device on a network
- **Location Addressing**
  Specifies the location of the device in the network
- **Routing**
  Helps routers send data to the correct destination

Structure of IP Address

An IP address consists of two parts:

- **Network Part** → Identifies the network
- **Host Part** → Identifies the specific device

Example

If a device has IP address **192.168.1.5**:

- **192.168.1** → Network portion
- **5** → Host portion

Importance of IP Address

- Essential for communication over networks
- Enables internet access
- Helps in routing and data delivery
- Ensures each device is uniquely identifiable

Short Exam Definition- ***An IP address is a unique numerical identifier assigned to each device on a network to enable communication and data transfer.***

7. Network Topology

Network topology refers to the **physical or logical arrangement of devices (nodes) and connections** in a computer network. It describes how different devices are connected and how data flows between them. Topology plays an important role in determining the **performance, reliability, and scalability** of a network.

Definition-Network topology is the arrangement or layout of nodes and communication links in a computer network.

Types of Network Topology

1. Bus Topology

- All devices are connected to a **single main cable (backbone)**
- Data travels in both directions

Advantages:

- Simple and low cost
- Easy to install

Disadvantages:

- If the main cable fails, entire network stops
- Difficult to troubleshoot

2. Star Topology

- All devices are connected to a **central device** (like a switch or hub)

Advantages:

- Easy to manage and expand
- Failure of one device does not affect others

Disadvantages:

- If central device fails, entire network stops
- Requires more cable

3. Ring Topology

- Devices are connected in a **circular loop**
- Data flows in one direction (or both in some cases)

Advantages:

- Equal access for all devices
- Organized data flow

Disadvantages:

- Failure of one node can affect the whole network
- Difficult to modify

4. Mesh Topology

- Every device is connected to **every other device**

Advantages:

- Highly reliable
- Fault tolerance (failure of one link doesn't affect others)

Disadvantages:

- Expensive
- Complex to install

5. Tree Topology

- Combination of **star and bus topology**
- Devices are arranged in a hierarchical structure

Advantages:

- Scalable
- Easy to manage large networks

Disadvantages:

- Depends on main backbone
- Complex setup

6. Hybrid Topology

- Combination of two or more topologies

Advantages:

- Flexible
- Can be customized

Disadvantages:

- Expensive
- Complex design

Summary Table

Topology	Structure	Key Feature
Bus	Single cable	Simple & low cost
Star	Central device	Easy management
Ring	Circular loop	Equal access
Mesh	Fully connected	High reliability
Tree	Hierarchical	Scalable
Hybrid	Mixed	Flexible

Importance of Network Topology

- Determines **network performance**
- Affects **cost and maintenance**
- Helps in **fault detection**
- Influences **data transmission efficiency**

Short Exam Definition-*Network topology is the physical or logical arrangement of devices and connections in a computer network.*

8. Bandwidth and Data Transmission Rate

Bandwidth refers to the **maximum capacity of a communication channel** to transmit data in a given amount of time. It indicates how much data can flow through a network connection.

It is usually measured in:

- **bits per second (bps)**
- **kilobits per second (Kbps)**
- **megabits per second (Mbps)**
- **gigabits per second (Gbps)**

In simple terms, bandwidth is the **size of the pipe** through which data travels.

Key Points about Bandwidth

- Higher bandwidth = more data can be transmitted
- It does **not guarantee speed**, only capacity
- Affected by network technology and medium (fiber, cable, wireless)

Data Transmission Rate

Data Transmission Rate (or **Data Rate**) refers to the **actual speed at which data is transferred** from one device to another over a network.
It is also measured in **bps, Kbps, Mbps, or Gbps**.
It represents the **actual flow of data**, not the maximum capacity.

Key Points about Data Transmission Rate

- Depends on bandwidth and network conditions
- Affected by:
  - Network congestion
  - Signal strength
  - Hardware performance
- Usually **less than or equal to bandwidth**

Difference Between Bandwidth and Data Transmission Rate

Feature	Bandwidth	Data Transmission Rate
Meaning	Maximum capacity	Actual speed
Nature	Theoretical	Practical
Measurement	bps, Mbps, Gbps	Same units
Dependence	Fixed (based on medium)	Varies with conditions

Example

If a network has:

- **Bandwidth = 100 Mbps**

It means:

- Maximum possible speed = 100 Mbps
- Actual data transmission rate may be:
  - 80 Mbps (due to congestion)
  - 50 Mbps (due to weak signal)

Importance

- Helps in evaluating **network performance**
- Important for **internet speed and quality**
- Determines efficiency of **data communication**

Short Exam Definition-*Bandwidth is the maximum capacity of a network to transmit data, while data transmission rate is the actual speed at which data is transferred.*

9. Network Security Components

Network security components are hardware, software, and policies designed to **protect a computer network from unauthorized access, misuse, and attacks**. They ensure **confidentiality, integrity, and availability** of data and network resources.
Network security is essential for **preventing cyber attacks**, **data breaches**, and **network failures**.

Key Components of Network Security

1. Firewall
- Acts as a **barrier between a trusted network and untrusted networks (like the internet)**
- Monitors and controls incoming and outgoing traffic based on **security rules**
- Can be **hardware-based**, **software-based**, or both
- Examples: Packet filtering firewall, Stateful firewall

2. Antivirus / Anti-malware Software
- Detects, prevents, and removes **malicious software**
- Protects computers and networked devices from viruses, worms, trojans, ransomware, etc.
- Often includes **real-time scanning and automatic updates**

3. Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- **IDS** monitors network traffic to detect suspicious activity
- **IPS** not only detects but also **prevents attacks automatically**
- Helps protect against unauthorized access and cyber threats

4. Virtual Private Network (VPN)
- Provides a **secure and encrypted connection** over the internet
- Ensures privacy and protects sensitive data during transmission
- Commonly used for remote work

5. Access Control Systems
- Determines **who can access what resources** in a network
- Uses methods like:
  - Passwords / PINs
  - Biometric authentication
  - Role-based access control

6. Encryption
- Converts data into a **coded format** to prevent unauthorized access
- Only authorized users with a **decryption key** can read the data
- Examples: SSL/TLS for websites, end-to-end encryption in messaging

7. Security Policies
- Rules and guidelines for **safe network usage**
- Includes:
  - Password policies
  - User privileges
  - Data backup procedures
  - Acceptable use policies

8. Proxy Servers
- Acts as an **intermediary between users and the internet**
- Can filter traffic, hide IP addresses, and improve security

9. Network Segmentation
- Divides a network into **smaller secure sections (subnets)**
- Limits access to sensitive areas
- Reduces impact of attacks

10. Patch Management
- Regular updates to **software and firmware**
- Fixes vulnerabilities and security loopholes

Importance of Network Security Components
- Protects **sensitive data** from theft or alteration
- Ensures **network availability and reliability**

- Prevents unauthorized access and cyber attacks
- Maintains **user trust and compliance with regulations**

Short Exam Definition-*Network security components are hardware, software, and policies that protect a computer network from unauthorized access, attacks, and data breaches.*

10. Network Software

Network software refers to the **programs and applications** that enable devices to **communicate, share resources, and manage a computer network**. It provides the **rules, interfaces, and services** that allow hardware devices to work together efficiently.

Network software is essential for **maintaining connectivity, security, and proper functioning of networks**.

Definition-Network software is a set of programs that control, manage, and facilitate communication between devices in a computer network.

Types of Network Software

1. Network Operating System (NOS)
- Specialized operating system designed to **manage network resources**
- Provides **file sharing, printer access, user authentication, and security**
- Examples: Windows Server, Linux Server (Ubuntu Server, Red Hat), Novell NetWare

2. Communication Software
- Enables **data exchange between devices**
- Manages protocols like TCP/IP, HTTP, FTP, SMTP, etc.
- Ensures proper **data transmission and reception**

3. Network Management Software
- Helps in **monitoring, maintaining, and optimizing** a network
- Features include:
  - Fault detection
  - Performance monitoring
  - Traffic analysis
  - Resource allocation
- Examples: SolarWinds, PRTG Network Monitor

4. Network Security Software
- Protects the network from **unauthorized access and attacks**
- Includes:
  - Firewalls
  - Antivirus / Anti-malware
  - Intrusion Detection / Prevention Systems (IDS/IPS)
  - Encryption software

5. Utility Software
- Provides **additional network services** and tools:
  - Ping and traceroute for testing connections
  - Network analyzers and packet sniffers
  - Bandwidth monitors

6. Collaboration Software
- Allows users to **communicate and work together over a network**
- Examples: Email clients, instant messaging, video conferencing software (Zoom, Microsoft Teams)

Functions of Network Software

1. **Resource Sharing** – Shares files, printers, and other devices across the network
2. **Communication Management** – Ensures reliable and secure data transfer
3. **Network Monitoring** – Tracks performance, usage, and errors
4. **Security Management** – Protects against unauthorized access and malware
5. **Troubleshooting** – Detects and resolves network problems

Short Exam Definition- ***Network software is a collection of programs that enable devices to communicate, share resources, and manage the operations of a computer network.***

IV. Transmission Modes

Transmission modes refer to the **methods by which data is transmitted between two devices in a network**. They define **the direction of data flow** between the sender and receiver.
Transmission modes are essential to **organize communication efficiently** and avoid data collisions or loss.

Definition- Transmission mode is the direction in which data flows between two devices in a communication channel.

Types of Transmission Modes

1. Simplex Mode

- **Data flows in only one direction**
- One device is the **sender**, the other is the **receiver**
- No feedback from receiver to sender

Examples:

- Keyboard → Computer
- Television broadcast

Advantages:

- Simple and inexpensive

Disadvantages:

- No two-way communication

2. Half-Duplex Mode

- **Data flows in both directions, but only one at a time**
- Devices take turns sending and receiving data

Examples:

- Walkie-talkies
- Old Ethernet networks

Advantages:

- Two-way communication possible
- Uses a single channel

Disadvantages:

- Slower than full-duplex due to turn-taking

3. Full-Duplex Mode

- **Data flows in both directions simultaneously**
- Sender and receiver can communicate at the same time

Examples:

- Telephone conversations
- Modern Ethernet networks (Gigabit Ethernet)

Advantages:

- Faster communication
- Efficient use of channel

Disadvantages:

- More expensive hardware required

Summary Table

Mode	Direction of Data	Examples	Advantage	Disadvantage
Simplex	One-way	Keyboard → PC, TV	Simple, cheap	No feedback

Mode	Direction of Data	Examples	Advantage	Disadvantage
Half-Duplex	Two-way (one at a time)	Walkie-talkies	Two-way possible	Slower due to waiting
Full-Duplex	Two-way (simultaneous)	Telephone, Gigabit Ethernet	Fast, efficient	Costly hardware

Importance of Transmission Modes

- Determines **network speed and efficiency**
- Helps in **choosing appropriate communication hardware**
- Reduces **collisions and errors** in data transfer

Short Exam Definition-*Transmission mode is the direction in which data flows between two devices, and can be simplex, half-duplex, or full-duplex.*

Types of Networks

A **network** is a collection of computers, devices, or nodes connected together to **share resources and communicate**. Networks are classified based on **geographical area, ownership, or purpose**.

Definition- A network is a group of two or more connected devices that share resources and information with each other.

Types of Networks Based on Geographical Area

1. LAN (Local Area Network)

- Covers a **small geographical area** such as a home, office, or building
- High data transfer speed and low cost
- Devices are connected using Ethernet cables or Wi-Fi

Examples: Office network, school computer lab

Advantages:

- Fast data transfer
- Easy resource sharing

Disadvantages:

- Limited coverage

2. MAN (Metropolitan Area Network)

- Covers a **city or a large campus**
- Larger than LAN but smaller than WAN
- Connects multiple LANs using high-speed connections

Examples: City-wide Wi-Fi, university networks

Advantages:

- Covers larger areas
- Efficient for cities and large organizations

Disadvantages:

- Expensive to set up

3. WAN (Wide Area Network)

- Covers **large geographical areas**, often a country or continent
- Connects multiple LANs or MANs
- Uses public networks like the internet or leased lines

Examples: Internet, corporate networks spanning multiple countries

Advantages:

- Connects distant locations
- Supports global communication

Disadvantages:

- Expensive and slower than LAN

4. PAN (Personal Area Network)

- Covers **a very small area**, usually around a single person
- Connects personal devices like smartphones, tablets, and laptops
- Uses Bluetooth, USB, or Wi-Fi

Examples: Wireless headphones with a smartphone
Advantages:

- Simple and convenient
- Low cost

Disadvantages:

- Very limited coverage

5. CAN (Campus Area Network)

- Connects **multiple LANs within a campus**
- Medium-sized network for educational institutions or business campuses

Examples: University or corporate campus network
Advantages:

- Efficient for campus communication
- Easy resource sharing

Disadvantages:

- Setup cost can be high

Types of Networks Based on Ownership

- **Private Network** – Owned and managed by an organization
- **Public Network** – Open for public use (e.g., internet)

Types of Networks Based on Communication

- **Wired Network** – Uses cables like Ethernet
- **Wireless Network** – Uses Wi-Fi, Bluetooth, or cellular networks

Summary Table

Type	Coverage	Example	Advantages	Disadvantages
PAN	Few meters	Bluetooth devices	Low cost, convenient	Limited range
LAN	Building / Office	Office network	Fast, easy sharing	Small area
CAN	Campus	University network	Efficient campus comm	Expensive setup
MAN	City	City-wide Wi-Fi	Covers city area	Costly, moderate speed
WAN	Country / Globe	Internet	Global communication	Expensive, slower

Importance of Network Types

- Determines **network design and infrastructure**
- Helps in **resource sharing**
- Supports **communication over different distances**
- Assists in **choosing hardware and software requirements**

Short Exam Definition- ***Types of networks refer to the classification of computer networks based on area, ownership, or communication, including PAN, LAN, CAN, MAN, and WAN.***

V. OSI Model

The **OSI (Open Systems Interconnection) Model** is a **conceptual framework** used to understand and standardize how **data is transmitted and received over a network**. It divides the communication process into **seven distinct layers**, with each layer performing a specific function.
It helps **different devices and protocols communicate** effectively.

Definition- The OSI model is a layered framework that describes how data moves from one device to another across a network, standardizing communication functions into seven layers.

The Seven Layers of OSI Model

Layer Number	Layer Name	Function	Examples
7	**Application Layer**	Interface between the user and network; provides services like email, file transfer, and browsing	HTTP, FTP, SMTP, DNS
6	**Presentation Layer**	Translates data into a readable format, encryption/decryption, compression	JPEG, GIF, SSL/TLS
5	**Session Layer**	Manages sessions or connections between devices; establishes, maintains, and terminates sessions	NetBIOS, RPC
4	**Transport Layer**	Provides reliable or unreliable delivery of data; manages error detection and flow control	TCP, UDP
3	**Network Layer**	Determines logical addressing and routing; handles data packet delivery	IP, ICMP
2	**Data Link Layer**	Ensures error-free transmission over physical medium; manages MAC addresses	Ethernet, Switch, PPP
1	**Physical Layer**	Deals with physical transmission of raw bits over the medium	Cables, Hubs, Repeaters

Key Points About OSI Model

- **Layered Approach**: Each layer performs a **specific function** and interacts only with its adjacent layers
- **Encapsulation**: Data moves down the layers, each adding a **header (and sometimes a trailer)**
- **Decapsulation**: At the receiving end, headers are removed layer by layer
- **Standardization**: Ensures interoperability between different devices and vendors

Importance of OSI Model

1. Provides a **universal standard** for network communication
2. Simplifies **troubleshooting and maintenance**
3. Helps in **protocol development**
4. Separates **hardware and software functions**
5. Supports **interoperability between different networks**

Analogy for Easy Understanding
Think of sending a **letter through post**:

- **Application** → Writing the letter
- **Presentation** → Converting it into proper language or encryption
- **Session** → Scheduling a time to send
- **Transport** → Ensuring the letter is delivered correctly
- **Network** → Choosing the route (postal code)
- **Data Link** → Packaging it in an envelope
- **Physical** → The physical transport via mail van

Short Exam Definition- ***The OSI model is a conceptual framework that divides network communication into seven layers to standardize data transmission and ensure interoperability.***

VI. TCP/IP Model

The **TCP/IP (Transmission Control Protocol / Internet Protocol) Model** is a **practical framework** used for **data communication over the internet and networks**. Unlike the OSI model, TCP/IP is more **implementation-oriented** and widely used in real-world networks.
It defines **how data is packaged, addressed, transmitted, routed, and received** over networks.

Definition-The TCP/IP model is a layered framework that specifies the protocols and standards for communication between devices over a network, especially the internet.

Layers of TCP/IP Model
The TCP/IP model has **four layers**:

Layer	Function	Protocols / Examples
Application Layer	Provides network services to user applications; handles high-level protocols and data formatting	HTTP, HTTPS, FTP, SMTP, DNS
Transport Layer	Ensures reliable or unreliable delivery of data between devices; manages error checking and flow control	TCP (reliable), UDP (unreliable)
Internet Layer	Handles logical addressing, routing, and packet forwarding	IP, ICMP, ARP
Network Access / Link Layer	Manages physical transmission of data over network media; controls hardware addressing	Ethernet, Wi-Fi, Switches, Hubs

Key Points About TCP/IP Model

- Developed for **ARPANET** and now used in the **Internet**
- Combines **OSI layers**:
  - Application = OSI Application + Presentation + Session
  - Network Access = OSI Data Link + Physical
- **Protocol-oriented**, meaning it focuses on actual protocols for communication
- Supports **inter-networking across diverse networks**

Comparison with OSI Model

Feature	OSI Model	TCP/IP Model
Layers	7 layers	4 layers
Approach	Theoretical / Conceptual	Practical / Implementation-oriented
Popularity	Teaching & standardization	Real-world networks & Internet
Layer Combination	Strict separation	Combines some OSI layers
Protocol	Generic / Layer-independent	Protocol-specific

Importance of TCP/IP Model

1. Provides **standard rules for internet communication**
2. Ensures **interoperability between different networks**
3. Supports **routing and addressing of data packets**
4. Enables **reliable and efficient data transfer**
5. Forms the **foundation of the Internet**

Analogy for Easy Understanding
Sending a **package through courier service**:

- **Application Layer** → Writing the letter/package content
- **Transport Layer** → Ensuring it is delivered reliably
- **Internet Layer** → Choosing the address and route
- **Network Access Layer** → Physically sending the package via truck/plane

Short Exam Definition- ***The TCP/IP model is a practical, four-layer framework that defines protocols and standards for data communication over networks, especially the internet.***

VII. Main Protocols Used on the Web

Protocols are **rules and standards** that govern **how data is transmitted, received, and interpreted** over the internet. The web relies on several **key protocols** to ensure smooth communication between devices and servers.

Definition- Web protocols are standardized rules that control how data is exchanged over the World Wide Web (WWW).

Main Protocols

1. HTTP (HyperText Transfer Protocol)

- Used for **transferring web pages** from a server to a browser
- Works on **request-response model**: Browser requests → Server responds
- **Stateless protocol** (doesn't remember previous requests)

Example: Accessing a website like http://example.com

2. HTTPS (HyperText Transfer Protocol Secure)

- Secure version of HTTP using **encryption (SSL/TLS)**
- Protects data during transmission from hackers
- Essential for online banking, shopping, and secure login

Example: https://www.gmail.com

3. FTP (File Transfer Protocol)

- Used to **transfer files** between client and server over the internet
- Requires authentication (username and password)
- Supports uploading and downloading of files

Example: Uploading a website to a hosting server

4. SMTP (Simple Mail Transfer Protocol)

- Used to **send emails** from client to server or between mail servers
- Works with other protocols like POP3 or IMAP for retrieving emails

Example: Sending emails via Gmail or Outlook

5. POP3 (Post Office Protocol version 3)

- Used to **retrieve emails from a mail server**
- Downloads emails to the client and usually deletes them from the server

6. IMAP (Internet Message Access Protocol)

- Retrieves emails while **keeping them on the server**
- Allows access from **multiple devices**

7. DNS (Domain Name System)

- Converts **human-readable domain names** into IP addresses
- Makes browsing easier without remembering numeric IP addresses

Example: www.google.com → 142.250.190.78

8. Telnet / SSH (Secure Shell)

- Telnet allows **remote access** to servers (not secure)
- SSH is the **secure version** used for encrypted remote login

Importance of Web Protocols

- Ensure **data is transmitted correctly and efficiently**
- Provide **security and privacy**
- Enable **email, browsing, and file transfer**
- Standardize communication across different devices and servers

Short Exam Definition- ***Main protocols used on the web are standardized rules like HTTP, HTTPS, FTP, SMTP, POP3, IMAP, and DNS that control data transfer, security, and communication over the internet.***

VIII. Types of Wireless Communication

Wireless communication is the transfer of data between devices **without physical cables**, using **radio waves, infrared, microwaves, or other electromagnetic signals**. It allows mobility, convenience, and connectivity over various distances.

Definition- Wireless communication is the transfer of information between devices using electromagnetic waves instead of physical cables.

Types of Wireless Communication

1. Infrared Communication

- Uses **infrared light waves** for short-range communication
- Works **line-of-sight** and usually in **small areas**

Examples:

- TV remote controls
- IrDA ports in older devices

Advantages:

- Simple and inexpensive
- Secure (limited range)

Disadvantages:

- Short range
- Cannot penetrate walls

2. Radio Frequency (RF) Communication

- Uses **radio waves** for medium to long-range communication
- Most common wireless technology

Examples:

- Wi-Fi (Wireless LAN)
- Bluetooth
- Radio broadcasting

Advantages:

- Longer range than infrared
- Can penetrate obstacles

Disadvantages:

- Interference possible
- Security risks if unencrypted

3. Microwave Communication

- Uses **high-frequency microwave signals** for long-distance communication
- Often used for **point-to-point communication**

Examples:

- Satellite communication
- Long-distance telephone networks

Advantages:

- High bandwidth
- Suitable for long-distance transmission

Disadvantages:

- Requires line-of-sight
- Expensive infrastructure

4. Satellite Communication

- Involves **transmitting signals to satellites** and back to Earth
- Supports **global communication**

Examples:

- GPS
- Satellite TV
- Satellite internet

Advantages:

- Covers large areas
- Enables global connectivity

Disadvantages:

- Expensive
- Signal delay (latency)

5. Bluetooth

- Short-range communication (typically **10 meters**)
- Used for connecting personal devices wirelessly

Examples:

- Wireless headphones
- Smartwatches
- File transfer between phones

Advantages:

- Low power consumption
- Easy pairing

Disadvantages:

- Limited range
- Slower compared to Wi-Fi

6. Wi-Fi (Wireless Fidelity)

- Provides **high-speed wireless internet** over a local area
- Uses radio waves, usually in **2.4 GHz or 5 GHz bands**

Examples:

- Home Wi-Fi networks
- Public hotspots

Advantages:

- High speed
- Supports multiple devices

Disadvantages:

- Limited range
- Can be insecure without proper encryption

7. Cellular Communication

- Uses **cell towers** to provide wireless mobile connectivity
- Covers local, regional, or national areas

Examples:
- 4G LTE, 5G networks
- Mobile phone calls and internet

Advantages:
- Wide coverage
- Supports mobility

Disadvantages:
- Expensive infrastructure
- Signal may drop in remote areas

Summary Table

Type	Medium	Range	Examples	Advantages	Disadvantages
Infrared	Light waves	Short	TV remotes	Simple, secure	Line-of-sight, short range
Radio Frequency	Radio waves	Medium	Wi-Fi, Bluetooth	Penetrates walls	Interference possible
Microwave	Microwave signals	Long	Satellite links	High bandwidth	Line-of-sight, costly
Satellite	Electromagnetic waves via satellite	Global	GPS, Satellite TV	Global coverage	Expensive, latency
Bluetooth	Radio waves	Short	Headphones, watches	Low power	Limited range
Wi-Fi	Radio waves	Local	Home internet	High speed	Limited range
Cellular	Radio waves	Local to national	Mobile phones	Wide coverage	Expensive, signal drops

Importance of Wireless Communication
- Enables **mobility and flexibility**
- Reduces **dependence on cables**
- Supports **global and remote communication**
- Facilitates **IoT, smartphones, and smart devices**

Short Exam Definition- ***Wireless communication is the transfer of data between devices using electromagnetic waves instead of physical cables, including technologies like Wi-Fi, Bluetooth, satellite, and cellular networks.***

IX. Software Piracy

Software piracy is the **unauthorized copying, distribution, or use of software** without the permission of the copyright owner. It is an **illegal activity** that violates intellectual property laws.
Software piracy can affect **software developers, businesses, and users**, causing financial loss and security risks.

Definition- Software piracy is the illegal use, duplication, or distribution of copyrighted software without authorization from the owner.

Types of Software Piracy
1. Counterfeiting
- Making **unauthorized copies** of software and **selling them as originals**
- Often comes in **fake packaging**

Example: Selling copied versions of Microsoft Office or Adobe Photoshop

2. End-User Piracy
- Using a **legally purchased software on more devices than allowed**
- Violates the **license agreement**

Example: Installing a single-user license on multiple computers

3. Online Piracy / Internet Piracy
- Downloading or distributing software illegally over the **internet**
- Common for **games, operating systems, and applications**

Example: Downloading paid software from torrent websites

4. Softlifting
- Copying software from a **licensed CD or DVD** and using it without paying for extra licenses

Example: Installing one purchased software on multiple computers in an office

5. Hard Disk Loading
- Pre-installing unauthorized software on **newly sold computers**
- Users pay only for hardware, not software

6. Client-Server Overuse
- Using software on a **network server** in excess of the purchased licenses

Effects of Software Piracy
- **Financial Loss:** Companies lose revenue from software sales
- **Legal Consequences:** Users can face **fines and imprisonment**
- **Security Risks:** Pirated software often contains **viruses, malware, or spyware**
- **Reduced Innovation:** Developers lose incentive to create new software

Legal Protection Against Software Piracy
- **Copyright laws** protect software as intellectual property
- **Licensing agreements** specify how software can be used
- Organizations like **BSA (Business Software Alliance)** work against piracy

Short Exam Definition- ***Software piracy is the illegal copying, use, or distribution of software without permission, violating copyright laws and licensing agreements.***

X. Firewall

A **firewall** is a **network security device or software** that **monitors, filters, and controls incoming and outgoing network traffic** based on predefined security rules. It acts as a **barrier between a trusted internal network and untrusted external networks**, such as the Internet.
Firewalls are essential for **protecting networks from unauthorized access, cyber attacks, and data theft**.

Definition- A firewall is a security system that controls and monitors network traffic between trusted and untrusted networks according to defined security rules.

Functions of a Firewall
1. **Packet Filtering** – Examines data packets and allows or blocks them based on **IP addresses, protocols, or ports**.
2. **Proxy Service** – Acts as an **intermediary between internal and external networks**, hiding internal IP addresses.
3. **Stateful Inspection** – Monitors the **state of active connections** and determines whether packets are safe.

4. **Network Address Translation (NAT)** – Hides internal network addresses from the external network.
5. **Logging and Alerts** – Records suspicious activities and **alerts network administrators**.

Types of Firewalls

1. Hardware Firewall

- A **physical device** installed between a network and the Internet
- Often used in offices and large organizations

Advantages:

- High speed
- Protects entire network

Disadvantages:

- Expensive
- Requires setup and maintenance

2. Software Firewall

- Installed on **individual computers**
- Controls traffic for that device

Advantages:

- Easy to install
- Customizable per device

Disadvantages:

- Uses system resources
- Less protection for entire network

3. Packet Filtering Firewall

- Filters packets based on **IP addresses, port numbers, and protocols**
- Simple but cannot detect advanced attacks

4. Stateful Inspection Firewall

- Monitors **active connections** and allows only valid packets
- More secure than simple packet filtering

5. Proxy Firewall

- Acts as an **intermediary** between user and external network
- Can cache content and block malicious sites

Importance of Firewalls

- **Prevents unauthorized access** to the network
- **Blocks malware and cyber attacks**
- **Monitors and logs network traffic**
- Helps enforce **security policies**
- Protects sensitive **data and resources**

Short Exam Definition- ***A firewall is a network security system that monitors, filters, and controls network traffic to protect internal networks from unauthorized access and attacks.***

XI. Network Threats

Network threats are any **potential dangers that can compromise the security, integrity, or availability of a network**. They can result in **data loss, unauthorized access, or disruption of services**. Understanding threats is crucial for designing **effective network security**.

Definition- Network threats are potential risks or attacks that can harm computer networks, data, or connected devices.

Types of Network Threats

1. Malware (Malicious Software)

- Software designed to **damage, disrupt, or gain unauthorized access** to a system
- Types include:
  - **Virus** – Attaches to files and spreads
  - **Worm** – Self-replicates over networks
  - **Trojan Horse** – Disguised as legitimate software
  - **Ransomware** – Encrypts data and demands payment

Example: WannaCry ransomware attack

2. Phishing

- Fraudulent attempts to **obtain sensitive information** (passwords, credit card numbers)
- Often done via **emails, messages, or fake websites**

Example: Fake bank emails requesting login credentials

3. Denial of Service (DoS) / Distributed DoS (DDoS)

- **Overloads a network or server** with traffic, making it unavailable
- DDoS involves **multiple systems attacking simultaneously**

Example: Mirai Botnet attack on websites

4. Man-in-the-Middle (MITM) Attack

- Attacker **intercepts communication** between two parties
- Can **steal or alter data**

Example: Eavesdropping on public Wi-Fi

5. Unauthorized Access

- Gaining access to a network or device **without permission**
- Often exploits weak passwords or security flaws

Example: Hacking into a company network

6. Sniffing

- Capturing network traffic to **steal sensitive information**
- Usually done using **packet sniffers**

7. SQL Injection / Website Attacks

- Exploiting **vulnerabilities in web applications** to access database information
- Can lead to **data theft or modification**

8. Social Engineering

- Manipulating people into **revealing confidential information**
- Techniques include impersonation, pretexting, and baiting

9. Insider Threats

- Threats originating from **employees or trusted personnel**
- Can be intentional or accidental

Example: Employee leaking confidential data

Importance of Understanding Threats

- Helps in **designing security measures**
- Prevents **financial and data loss**

- Ensures **confidentiality, integrity, and availability (CIA triad)**
- Supports **compliance with legal and regulatory standards**

Short Exam Definition- ***Network threats are potential dangers, such as malware, phishing, or unauthorized access, that can compromise the security, integrity, or availability of a network.***

XII. Hacking and Cracking

Hacking and **Cracking** are terms used in cybersecurity to describe **unauthorized actions on computer systems**, but they differ in intent and methods. Understanding the difference is crucial for **network security awareness**.

Definitions

Hacking- Hacking is the act of exploring, testing, or gaining unauthorized access to computer systems or networks, sometimes with ethical intent.

- Hackers may **identify vulnerabilities** to improve security (**Ethical Hackers / White Hat**)
- Or exploit systems for personal gain (**Black Hat Hackers**)

Cracking- Cracking is the act of breaking software or security measures to bypass protections, usually for illegal purposes.

- Focuses on **removing restrictions, bypassing licensing, or exploiting systems**
- Always illegal and malicious

Types of Hackers

Type	Intent	Description
White Hat	Ethical	Tests systems to **find and fix vulnerabilities**
Black Hat	Malicious	Breaks into systems to **steal, damage, or exploit data**
Grey Hat	Both	Exploits vulnerabilities without permission but **doesn't always have malicious intent**
Script Kiddie	Malicious	Uses pre-made tools to hack without deep knowledge

Types of Cracking

1. **Software Cracking**
   - Removes copy protection or licensing restrictions
   - Example: Using pirated versions of software
2. **Password Cracking**
   - Gaining unauthorized access by **guessing or decrypting passwords**
   - Tools: Brute-force attacks, dictionary attacks
3. **Network Cracking**
   - Breaking into **secured networks**
   - Example: Hacking Wi-Fi passwords

Differences Between Hacking and Cracking

Feature	Hacking	Cracking
Intent	Can be ethical or malicious	Always illegal/malicious
Purpose	Testing, learning, improving security	Bypass security, steal data, or pirate software
Examples	Ethical penetration testing	Software piracy, password theft
Legality	Can be legal (ethical hacking)	Illegal
Focus	Understanding systems and vulnerabilities	Exploiting or breaking protections

Importance of Understanding Hacking and Cracking

- Helps in **strengthening network and system security**
- Raises awareness of **ethical vs. illegal practices**
- Guides **implementation of preventive measures**
- Reduces risk of **cybercrime and data breaches**

Short Exam Definitions

- **Hacking:** Unauthorized access to systems or networks, can be ethical or malicious.
- **Cracking:** Illegal breaking of software or security measures to bypass protections or steal data.

Unit II

2.1 Evolution of Internet

The evolution of the internet is one of the most significant technological developments in modern history. It began in the late 1960s with **ARPANET**, a project developed by the United States Department of Defense to enable communication between computers on different networks. This early system introduced the concept of packet switching, which allowed data to be broken into smaller pieces and transmitted efficiently.

In the 1970s and 1980s, the development of **TCP/IP protocols** provided a standard way for computers to communicate, leading to the creation of a true global network. By 1983, ARPANET had adopted TCP/IP, marking the beginning of the modern internet. During this period, the network was mainly used by researchers, scientists, and academic institutions.

The 1990s marked a turning point with the invention of the **World Wide Web** by Tim Berners-Lee. His introduction of HTML, HTTP, and web browsers made the internet accessible to the general public. As a result, websites began to grow rapidly, transforming the internet into a user-friendly platform for information sharing.

In the 2000s, the internet became commercialized, with the rise of companies like Google and Amazon. Faster broadband connections replaced dial-up services, enabling smoother browsing and the growth of e-commerce. In the following decade, smartphones and social media platforms revolutionized internet usage, making it more interactive and accessible anytime, anywhere.

Today, the internet continues to evolve with advancements in artificial intelligence, 5G technology, and the Internet of Things. It has become an essential part of daily life, shaping communication, education, business, and entertainment. Overall, the internet's journey from a simple research network to a global digital ecosystem highlights its transformative impact on society.

2.2 Introduction to the terms LAN, WAN, MAN

A computer network is a system that connects multiple devices to share data and resources. Based on geographical coverage, networks are commonly classified into **LAN (Local Area Network)**, **MAN (Metropolitan Area Network)**, and **WAN (Wide Area Network)**.

A **LAN (Local Area Network)** covers a small geographical area such as a home, school, or office. It is usually owned and managed by a single organization. LANs provide high-speed connectivity and are commonly used for sharing files, printers, and internet access within a limited space.

A **MAN (Metropolitan Area Network)** is larger than a LAN and spans across a city or town. It connects multiple LANs within a metropolitan area. MANs are often operated by government bodies or large organizations and are used to provide services like cable television networks and city-wide internet connectivity.

A **WAN (Wide Area Network)** covers a very large geographical area, such as a country or even the entire world. It connects multiple LANs and MANs together. The best example of a WAN is the Internet, which enables communication and information sharing across the globe.

In summary, LAN, MAN, and WAN differ mainly in their size, coverage, and ownership, but all play a vital role in modern communication systems.

2.3 Basic internet terms (Client, Server, MODEM, Web page, Web site, Home page, Browser, URL, ISP, Web server, Download & Upload, Online & Offline etc)

1) **Client**
   A client is a device or software (like your computer or phone) that requests services or information from another computer called a server.
2) **Server**
   A server is a powerful computer that provides data, services, or resources to clients over a network.
3) **Modem (MOdulator-DEModulator)**
   A modem is a device that connects your computer to the internet by converting digital signals into analog signals and vice versa.
4) **Web Page**
   A web page is a single document on the internet, usually written in HTML, that can display text, images, and videos.
5) **Website**
   A website is a collection of related web pages grouped under a single domain name.
6) **Home Page**
   The home page is the main or first page of a website that opens when you visit it.

7) **Browser**
   A browser is software used to access and view websites, such as Google Chrome, Mozilla Firefox, or Microsoft Edge.
8) **URL (Uniform Resource Locator)**
   A URL is the address of a webpage on the internet (for example: https://www.example.com).
9) **ISP (Internet Service Provider)**
   An ISP is a company that provides internet access to users, such as Airtel or Jio.
10) **Web Server**
   A web server is a system that stores website data and delivers web pages to users when requested.
11) **Download**
   Downloading means receiving data or files from the internet to your device (e.g., saving a file).
12) **Upload**
   Uploading means sending data or files from your device to the internet (e.g., posting a photo).
13) **Online**
   Being online means your device is connected to the internet.
14) **Offline**
   Being offline means your device is not connected to the internet.

2.4 Internet applications (Remote login, VoIP, Video Conferencing, Audio-Video streaming, Chatting etc).

Internet Applications

Internet applications are services that allow users to communicate, share information, and perform tasks online.

Remote Login

Remote login allows a user to access and control a computer from a different location using the internet.
Example: Using SSH to manage a server from home.

VoIP (Voice over Internet Protocol)

VoIP enables voice communication over the internet instead of traditional telephone lines.
Examples include apps like Skype and WhatsApp.

Video Conferencing

This allows people in different locations to have face-to-face meetings using video and audio in real time.
Examples: Zoom and Google Meet.

Audio-Video Streaming

Streaming allows users to watch videos or listen to music online without downloading files.
Examples: YouTube and Spotify.

Chatting (Instant Messaging)

Chatting enables real-time text communication between users over the internet.
Examples: Facebook Messenger and Telegram.

2.5 Identify and solve basic problems related to connecting to networks and the Internet.

Common Problems & Solutions

1. No Internet Connection

Possible causes:

- Loose cables or Wi-Fi turned off
- Router/modem not working

Solutions:

- Check cables and power supply
- Turn Wi-Fi on
- Restart your router and modem
- Reconnect to the network

2. Weak or Slow Internet

Possible causes:

- Weak Wi-Fi signal
- Too many users on the network
- Network congestion

Solutions:

- Move closer to the router

- Reduce the number of connected devices
- Restart router
- Upgrade your internet plan if needed

3. Unable to Connect to Wi-Fi

Possible causes:

- Wrong password
- Network not in range
- Device issue

Solutions:

- Re-enter correct password
- Forget and reconnect to the network
- Restart your device
- Check if Wi-Fi is enabled

4. Limited or No Network Access

Possible causes:

- IP address conflict
- Router configuration issue

Solutions:

- Restart device and router
- Run network troubleshooter (on Windows)
- Set IP settings to automatic (DHCP)

5. Web Pages Not Loading

Possible causes:

- DNS issue
- Browser problem
- Server down

Solutions:

- Refresh the page
- Try another browser like Google Chrome or Mozilla Firefox
- Clear browser cache
- Check internet connection

6. No Signal from Modem/Router

Possible causes:

- ISP issue
- Faulty modem

Solutions:

- Check modem lights
- Restart modem
- Contact your ISP such as Airtel or Jio

Basic Troubleshooting Steps

1. Restart your device
2. Restart router/modem
3. Check cables and Wi-Fi
4. Reconnect to network
5. Test with another device
6. Contact ISP if problem continues

2.6 E-Mail

E-Mail (Electronic Mail) is a method of exchanging digital messages over the Internet. It is one of the earliest and most widely used internet applications, enabling fast, reliable, and cost-effective communication across the world. E-mail allows users to send text messages as well as multimedia files such as images, documents, and videos.

Components of an E-Mail

An e-mail message consists of several important parts:

- **To:** The e-mail address of the recipient
- **From:** The sender's e-mail address
- **Subject:** A short description of the message content
- **Body:** The main message written by the sender
- **CC (Carbon Copy):** Sends a copy to additional recipients
- **BCC (Blind Carbon Copy):** Sends copies without revealing other recipients
- **Attachments:** Files (documents, images, etc.) sent along with the email

Working of E-Mail

The process of sending and receiving e-mail involves different protocols and servers:

1. The sender composes an e-mail using a mail service such as Gmail or Microsoft Outlook.
2. The message is sent to a **mail server** using **SMTP (Simple Mail Transfer Protocol)**.
3. The mail server forwards the message to the recipient's mail server.
4. The recipient retrieves the message using **POP3 (Post Office Protocol)** or **IMAP (Internet Message Access Protocol)**.

This entire process happens within seconds, making communication very fast.

Types of E-Mail Services

- **Web-based E-Mail:** Accessed through browsers (e.g., Gmail, Yahoo Mail)
- **Client-based E-Mail:** Requires software installation (e.g., Microsoft Outlook)

Advantages of E-Mail

- Very fast communication
- Low cost or free
- Can send messages worldwide instantly
- Supports file attachments
- Easy to store, organize, and search messages
- Can send a message to multiple recipients at once

Disadvantages of E-Mail

- Requires internet connection
- Risk of spam or junk mails
- Security threats like phishing and malware
- Messages may be ignored or overlooked

2.6.1Advantages

Advantages of E-Mail

- Very fast communication
- Low cost or free
- Can send messages worldwide instantly
- Supports file attachments
- Easy to store, organize, and search messages
- Can send a message to multiple recipients at once

2.6.2 How it's Works?

The process of sending and receiving e-mail involves different protocols and servers:

1. The sender composes an e-mail using a mail service such as Gmail or Microsoft Outlook.
2. The message is sent to a **mail server** using **SMTP (Simple Mail Transfer Protocol)**.
3. The mail server forwards the message to the recipient's mail server.
4. The recipient retrieves the message using **POP3 (Post Office Protocol)** or **IMAP (Internet Message Access Protocol)**.

This entire process happens within seconds, making communication very fast.

2.6.3 Anatomy of an e-mail Message

An **e-mail message** is made up of different parts that help in sending, receiving, and understanding the message clearly over the Internet.

Main Parts of an E-Mail

1. Header Section

The header contains basic information about the message:

- **From:** Sender's e-mail address
- **To:** Recipient's e-mail address
- **CC (Carbon Copy):** Additional recipients who receive a copy
- **BCC (Blind Carbon Copy):** Hidden recipients
- **Date:** Date and time when the e-mail was sent
- **Subject:** Short summary of the message

2. Body

- The **body** is the main content of the e-mail.
- It contains the message written by the sender.
- It can be plain text or formatted (fonts, colors, links, etc.).

3. Attachments

- Files sent along with the e-mail (documents, images, videos, etc.).
- Example: PDF, Word file, photos.

4. Signature

- A block of text automatically added at the end of the e-mail.
- Usually includes sender's name, contact details, and designation.

5. Additional Fields (Optional)

- **Reply-To:** Specifies a different reply address
- **Forward:** Sends received message to another person
- **Spam/Junk Indicator:** Marks unwanted emails

Example (Simple Structure)

From: abc@gmail.com
To: xyz@gmail.com
Subject: Meeting Reminder

Dear Sir,
This is a reminder for tomorrow's meeting.

Regards,
ABC

[Attachment: Meeting.pdf]

2.6.4 Basic of sending and receiving

E-mail is a simple and fast way to communicate over the Internet. Understanding how to **send and receive e-mails** is an essential digital skill.

Sending an E-Mail

To send an e-mail, follow these basic steps:

1. Open an e-mail service such as Gmail or Microsoft Outlook.
2. Click on **Compose** or **New Mail**.
3. Enter the recipient's e-mail address in the **To** field.
4. Add a **Subject** to describe the message.
5. Type your message in the **Body** section.
6. Attach files if needed using the **Attachment** option.
7. Click the **Send** button.

Once sent, the message is delivered through mail servers using protocols like SMTP.

Receiving an E-Mail

To receive an e-mail:

1. Log in to your e-mail account.
2. Open your **Inbox**.
3. New messages will appear in the inbox list.
4. Click on any message to read it.
5. You can **Reply**, **Reply All**, or **Forward** the message.

E-mails are received using protocols like POP3 or IMAP.

Simple Process Flow

- Sender writes and sends the message
- Mail server processes and transfers it
- Receiver's server stores it
- Receiver opens and reads it

2.6.5 Email Protocol

E-mail protocols are a set of rules that control how e-mail messages are sent, received, and stored over the Internet. These protocols ensure smooth communication between different mail servers and e-mail applications.

Main E-mail Protocols

1. SMTP (Simple Mail Transfer Protocol)

- Used for **sending e-mails** from the sender to the mail server and between servers.
- Works like a "postman" that delivers outgoing mail.
- Used when you click the **Send** button in services like Gmail or Microsoft Outlook.

2. POP3 (Post Office Protocol version 3)

- Used for **receiving e-mails** from the mail server to the user's device.
- Downloads e-mails and usually deletes them from the server.
- Allows offline reading of messages.

3. IMAP (Internet Message Access Protocol)

- Also used for **receiving e-mails**, but more advanced than POP3.
- Keeps e-mails stored on the server.
- Allows users to access the same mailbox from multiple devices (mobile, laptop, etc.).

Working Summary

- **SMTP → Sends e-mail**
- **POP3 → Downloads e-mail (offline access)**
- **IMAP → Syncs e-mail across devices (online access)**

Unit III

3.1 Introduction to World Wide Web: History, Working of Web Browsers, Its functions,

The **World Wide Web (WWW)** is a system of interlinked documents and resources (web pages) that are accessed through the Internet using a web browser. It allows users to view text, images, videos, and other multimedia content on websites.

The Web was invented in 1989 by **Tim Berners-Lee**, and it became publicly available in the early 1990s. Since then, it has grown into one of the most important communication and information-sharing systems in the world.

History of the World Wide Web

- **1989:** Tim Berners-Lee proposed the idea of the Web at CERN.
- **1990:** First web browser and web server were developed.
- **1991:** The first website went live.
- **1993:** Web became publicly accessible and started growing rapidly.
- **Today:** The Web is used globally for education, communication, business, and entertainment.

Working of Web Browsers

A **web browser** is a software application used to access and view websites on the Internet.

How it works:

1. User enters a **URL (Uniform Resource Locator)** in the browser.
2. The browser sends a request to a **web server**.
3. The server processes the request and sends back the web page data.
4. The browser interprets the data (HTML, CSS, JavaScript).
5. The web page is displayed on the screen.

Examples of browsers include Google Chrome, Mozilla Firefox, and Microsoft Edge.

Functions of Web Browsers

Web browsers perform several important functions:

1. Access Web Pages

- Open and display websites using URLs.

2. Interpret Web Content

- Read and display HTML, CSS, and JavaScript.

3. Navigation

- Move between pages using links, back, and forward buttons.

4. Search Function

- Allow users to search information using search engines.

5. Download and Upload

- Download files from websites and upload data where needed.

6. Security

- Protect users from unsafe websites and phishing attacks.

3.2 Search engine category

Search engines are tools that help users find information on the Internet by searching web pages, images, videos, and other content. They can be classified into different categories based on how they collect and present information.

1. Crawler-Based Search Engines

- These search engines use **software programs called crawlers or spiders** to automatically scan and index web pages.
- They continuously update their database by visiting websites.

Examples:

- Google Search
- Bing

Features:

- Fast and large database
- Automatically updated
- Most widely used type

2. Directory-Based Search Engines

- These are **human-powered search engines** where websites are manually submitted and categorized.
- Websites are organized into topics and subtopics.

Examples:

- Early Yahoo Directory (historical example)

Features:

- Classified information
- High quality listings
- Slower updates compared to crawler-based systems

3. Meta Search Engines

- These engines **do not have their own database**.
- They collect results from multiple search engines and combine them.

Examples:

- Dogpile (meta search engine)

Features:

- Aggregates results from different sources
- Wider range of results
- No independent indexing

4. Specialized Search Engines

- Designed to search **specific types of content or topics**.
- Focused on a particular field or service.

Examples:

- YouTube Search (videos)
- Google Scholar (research papers)

Features:

- Topic-specific results
- More accurate for specialized searches

3.3 Concept of Hyper Text Transfer Protocol (HTTP)

HTTP (Hyper Text Transfer Protocol) is the foundation protocol used for communication between a web browser and a web server on the Internet. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to different commands.

What is HTTP?

- HTTP is a **request–response protocol**.
- It is used to transfer **web pages (HTML documents)** and other web content.
- It works on a **client–server model**, where:
    - The **client** is the web browser
    - The **server** stores and sends web pages

How HTTP Works

1. A user enters a URL in a browser (e.g., a website address).
2. The browser sends an **HTTP request** to the web server.
3. The server processes the request and finds the required web page.
4. The server sends back an **HTTP response** containing the webpage.
5. The browser displays the content to the user.

Example

- When you open Google Chrome and visit a website:
    - Chrome sends an HTTP request
    - The web server sends the page back
    - You see the website on your screen

HTTP vs HTTPS

- **HTTP:** Standard, not encrypted (less secure)
- **HTTPS:** Secure version of HTTP with encryption (used for safe browsing)

Importance of HTTP

- Enables communication between browsers and servers

- Allows access to websites and online services
- Forms the basis of the World Wide Web

3.4 Web Servers

A **web server** is a computer system (or software) that stores, processes, and delivers web pages to users over the Internet. It responds to requests made by web browsers and provides the required website content.

What is a Web Server?

- A web server hosts **websites and web applications**.
- It delivers web pages using protocols like **HTTP (Hyper Text Transfer Protocol)**.
- It works on a **client–server model**, where the browser is the client and the web server provides data.

Working of a Web Server

1. A user enters a website address in a browser (e.g., URL).
2. The browser sends an **HTTP request** to the web server.
3. The web server processes the request and searches for the required file.
4. It sends back an **HTTP response** containing the web page.
5. The browser displays the page to the user.

Example browsers include Google Chrome and Mozilla Firefox.

Types of Web Servers

- **Static Web Server:** Delivers fixed content (HTML pages, images).
- **Dynamic Web Server:** Generates content dynamically using applications and databases.

Examples of Web Servers

- Apache HTTP Server
- Microsoft IIS (Internet Information Services)
- Nginx

Functions of a Web Server

- Stores website files (HTML, CSS, images, etc.)
- Processes browser requests
- Sends web pages to users
- Handles multiple users at the same time
- Provides security and access control

3.5 Internet Explorer

Internet Explorer (IE) is a **web browser** developed by Microsoft. It was used to access and view websites on the Internet.

History

- Released in **1995** by Microsoft.
- Became one of the most widely used browsers in the early 2000s.
- Later replaced by modern browsers like Microsoft Edge.
- Officially **retired in 2022**.

Features of Internet Explorer

- Allowed users to browse websites using URLs
- Supported basic web technologies like HTML and CSS
- Included tools like favorites (bookmarks) and history
- Provided security features like pop-up blockers (later versions)
- Supported file downloads and online forms

Working

- User enters a website address (URL).
- Internet Explorer sends a request to the web server.
- The server sends back the web page.
- The browser displays the content on the screen.

Limitations

- Slower compared to modern browsers
- Limited support for new web technologies
- Security issues in older versions

- Gradually replaced by better browsers

Replacement

Internet Explorer was replaced by Microsoft Edge, which is faster, more secure, and supports modern web standards.

3.6 Web publishing Document Interchange Standard

The **Web Publishing Document Interchange Standard** refers to the set of **rules and formats used to create, publish, store, and exchange documents on the Internet**, especially for the World Wide Web.
It ensures that web documents can be properly shared and displayed across different systems, browsers, and platforms.

Purpose

- To standardize how documents are created and shared on the web
- To ensure compatibility between different devices and browsers
- To make web content easy to access, read, and exchange globally

Key Elements Used in Web Document Interchange

1. HTML (HyperText Markup Language)

- Standard language for creating web pages
- Defines structure like headings, paragraphs, images, and links

2. XML (eXtensible Markup Language)

- Used to store and transfer data in a structured format
- Helps in exchanging information between systems

3. HTTP (HyperText Transfer Protocol)

- Transfers documents between web browsers and servers

4. URL (Uniform Resource Locator)

- Provides the address of web documents

How Document Interchange Works

1. A document is created using standard formats (like HTML/XML).
2. It is stored on a **web server**.
3. A user requests it using a web browser like Google Chrome.
4. The server sends the document using HTTP.
5. The browser displays the document correctly on the screen.

Importance

- Ensures **uniform display** of web pages worldwide
- Makes data exchange between systems easier
- Supports **cross-platform compatibility**
- Forms the foundation of web publishing systems

3.7 Component of Web Publishing

Web publishing is the process of creating and making web content available on the Internet. It involves designing, developing, uploading, and maintaining web pages so that users can access them through a browser.

Main Components of Web Publishing

1. Content Creation

- This is the process of preparing information for the website.
- Includes text, images, videos, audio, and documents.
- Content must be clear, useful, and well-organized.

2. Web Page Design

- Designing the layout and appearance of web pages.
- Uses technologies like HTML, CSS, and JavaScript.
- Ensures the website is user-friendly and attractive.

3. Web Hosting

- A service that stores website files on a **web server**.
- Makes the website accessible to users online.
- Provided by hosting companies.

4. Domain Name

- The unique address of a website (e.g., www.example.com).
- Helps users easily access websites without remembering IP addresses.
- Registered through domain providers.

5. Web Server

- Stores website files and delivers them to users.
- Works with protocols like HTTP to respond to browser requests.

6. Web Browser

- Software used to access and view websites.
- Examples include Google Chrome, Mozilla Firefox, and Microsoft Edge.

7. Uploading and Maintenance

- Uploading means transferring website files to a server.
- Maintenance includes updating content, fixing errors, and improving performance.

3.8 Site and Domain Name

A **website (site)** and a **domain name** are two important concepts used to access information on the Internet. They are closely related but serve different purposes.

Website (Site)

A **website** is a collection of related web pages that are stored on a web server and accessed through a browser.

Key Points:

- Contains multiple web pages (home page, about page, contact page, etc.)
- Includes text, images, videos, and other multimedia
- Accessed using a web browser like Google Chrome
- Hosted on a web server

Example:

A news website, educational website, or shopping website.

Domain Name

A **domain name** is the unique address of a website used to identify and access it on the internet.

Key Points:

- It is the **human-readable address** of a website
- It replaces complex IP addresses
- It is used in URLs (Uniform Resource Locators)
- Registered through domain registration services

Example:

- www.google.com
- www.wikipedia.org

Difference Between Site and Domain Name

Website (Site)	Domain Name
Collection of web pages	Address of a website
Contains actual content	Used to locate the website
Stored on a web server	Registered name system
Example: Google search page, Wikipedia pages	Example: google.com, wikipedia.org

3.9 Overview of Intranet and its applications.

An **Intranet** is a private network used within an organization to share information, resources, and services securely using the Internet technologies. It works like the internet but is restricted only to authorized users within a company, school, or institution.

What is Intranet?

- An intranet is a **private internal network**
- It uses internet technologies (like web browsers and protocols such as HTTP)

- Access is limited to employees or members of the organization
- It is secured using passwords, firewalls, and authentication systems

Example: A company's internal website used only by employees.

Features of Intranet

- Private and secure network
- Fast internal communication
- Easy sharing of files and information
- Controlled access for users
- Cost-effective communication system

Applications of Intranet

1. Communication

- Used for sending internal messages, notices, and emails within an organization
- Helps in quick communication between departments

2. File Sharing

- Employees can share documents, reports, and data securely
- Central storage of important files

3. Employee Information System

- Stores employee records, attendance, and payroll details
- Easy access for HR departments

4. Collaboration

- Supports teamwork through shared platforms and tools
- Used for project management and discussions

5. Training and Learning

- Provides online training materials and e-learning resources
- Helps employees improve skills

6. Company Announcements

- Used to publish notices, policies, and updates
- Ensures all employees receive the same information

Intranet vs Internet (Brief Difference)

Intranet	Internet
Private network	Public global network
Restricted access	Open to everyone
Used within organizations	Used worldwide
More secure	Less restricted

Unit IV

4.1 HTML, Designed Tools, HTML Editors

1. HTML (HyperText Markup Language)

HTML is the basic language used to create and structure web pages on the Internet. It tells the browser how content should be displayed.

Structure of HTML

An HTML document has a basic structure:

```
<html>
 <head>
  <title>My Web Page</title>
 </head>
 <body>
  <h1>Welcome</h1>
  <p>This is a paragraph.</p>
 </body>
</html>
```

Important HTML Tags:

- <html> → Root of the page
- <head> → Contains page information
- <title> → Title of the webpage
- <body> → Main visible content
- <h1> to <h6> → Headings
- <p> → Paragraph
- <a> → Links
- <img> → Images

Features of HTML:

- Easy to learn and use
- Works with all web browsers
- Used to create static web pages
- Forms the base of all websites

2. Web Design Tools

Web design tools are software applications used to create attractive and user-friendly website layouts without manually writing all code.

Types of Design Tools:

1. Graphic Design Tools

Used to design images, logos, and UI elements:

- Adobe Photoshop
- Canva
- Figma

2. Website Builders

Used to create complete websites easily:

- WordPress
- Wix
- Squarespace

Features of Design Tools:

- Drag-and-drop interface
- Pre-made templates
- Color and font customization
- Responsive design (mobile-friendly)
- Easy editing without coding knowledge

Uses:

- Designing website layout
- Creating banners and icons
- Improving visual appearance of websites

3. HTML Editors

An **HTML editor** is software used to write, edit, and manage HTML code for creating web pages.

Types of HTML Editors:

1. Text-Based Editors

These editors are simple and used for writing raw code.

Examples:

- Notepad (Windows)
- Notepad++
- Sublime Text

Features:

- Manual coding required
- Lightweight and fast
- Good for learning HTML

2. WYSIWYG Editors

(WYSIWYG = *What You See Is What You Get*)

These editors show a live preview of the web page while designing.

Examples:

- Adobe Dreamweaver
- Microsoft Visual Studio Code (with extensions)
- BlueGriffon

Features:

- No need to write full code manually
- Live preview of design
- Beginner-friendly
- Supports drag-and-drop editing

Common Features of HTML Editors:

- Syntax highlighting (colors for code)
- Auto-completion of tags
- Error detection
- Live preview option
- Code formatting tools

Relationship Between HTML, Design Tools, and Editors

- **HTML** → Creates the structure of a webpage
- **HTML Editors** → Help write and manage HTML code
- **Design Tools** → Improve visual appearance and layout

4.2 Issue in Web Site Creations and Maintenance

Creating and maintaining a website on the Internet involves several challenges. These issues can affect performance, security, design, and user experience of a website.

1. Technical Issues

- Errors in coding (HTML, CSS, JavaScript)
- Browser compatibility problems (website may not work the same in all browsers like Google Chrome or others)
- Server downtime or slow response from web servers
- Broken links and missing pages

2. Security Issues

- Hacking and unauthorized access
- Data theft or leakage
- Malware or virus attacks
- Phishing websites copying real sites

3. Performance Issues

- Slow loading speed due to large images or poor coding

- High traffic causing server overload
- Poor optimization of website resources

4. Design and Usability Issues

- Poor layout or confusing navigation
- Not mobile-friendly (lack of responsive design)
- Unattractive interface affecting user experience
- Difficult-to-read content

5. Maintenance Issues

- Regular updates required for content and software
- Fixing bugs and errors continuously
- Updating security patches
- Managing backups and data recovery

6. Hosting and Domain Issues

- Expired domain name registration
- Unreliable hosting services
- Limited storage or bandwidth
- Server configuration problems

7. Content Management Issues

- Outdated information on the website
- Inconsistent content updates
- Difficulty in managing large amounts of data

4.3 FTP S/W for Upload Website

FTP (File Transfer Protocol) software is used to transfer website files from a local computer to a web server on the Internet. It is an essential tool for web developers to publish and maintain websites online.

What is FTP?

- FTP stands for **File Transfer Protocol**
- It is a standard method used to **upload and download files** between a computer and a server
- It works on a **client–server model**

What is FTP Software?

FTP software (also called an FTP client) is a program that helps users:

- Upload website files to a web server
- Download files from a server
- Manage website directories and folders remotely

Popular FTP Software Tools

- FileZilla
- WinSCP
- Cyberduck
- CuteFTP

How FTP Works for Website Uploading

1. User creates a website on a local computer
2. FTP software is opened and login details are entered (host, username, password)
3. Connection is made with the web server
4. Website files are selected and uploaded
5. Files are stored on the server and the website becomes live

Common Uses of FTP in Web Development

- Uploading HTML, CSS, and JavaScript files
- Updating website content
- Managing images and media files
- Organizing folders on the server
- Backing up website data

Advantages of FTP Software

- Fast file transfer
- Easy website management

- Supports large file uploads
- Remote access to server files

Limitations

- Requires internet connection
- Needs correct login credentials
- Basic FTP is not always secure (SFTP is safer)

4.4 Elements of HTML & Syntax

HTML (HyperText Markup Language) is used to create and structure web pages on the Internet. It is made up of **elements and tags** that tell the browser how content should be displayed.

1. HTML Elements

An **HTML element** is the basic building block of a web page. It usually consists of:

Structure of an HTML Element:

<tagname> Content goes here </tagname>

Example:

This is a paragraph.

Parts of an Element:

- **Opening tag** →
- **Content** → Text or media inside the tag
- **Closing tag** →

Types of HTML Elements

1. Container Elements

- Have both opening and closing tags
- Contain content inside them

Examples:

- <html>...</html>
- <body>...</body>
- ...

2. Empty (Void) Elements

- Do not have closing tags
- Stand alone

Examples:

-
 → line break
- <img> → image
- <hr> → horizontal line

2. HTML Syntax

HTML syntax refers to the rules used to write HTML code correctly.

Basic Syntax Rules:

1. Tags must be in angle brackets

Paragraph

2. Tags must be properly closed

<h1>Heading</h1>

3. HTML documents have a structure

```
<html>
 <head>
  <title>Page Title</title>
 </head>
 <body>
  Content here
 </body>
</html>
```

4. Tags are usually nested

This is bold text.

5. Attributes provide extra information

Click Here

- href is an attribute
- It gives the link address

Example of Full HTML Structure

```
<html>
 <head>
  <title>My Website</title>
 </head>
 <body>
  <h1>Welcome</h1>
  <p>This is my first webpage.</p>
 </body>
</html>
```

4.5 Building HTML Documents

Building an **HTML document** means creating a structured web page using **HTML (HyperText Markup Language)**, which is displayed on the Internet through a web browser.

Basic Structure of an HTML Document

Every HTML document follows a standard structure:

```
<!DOCTYPE html>
<html>
 <head>
  <title>My First Web Page</title>
 </head>

 <body>
  <h1>Welcome</h1>
  <p>This is a simple HTML document.</p>
 </body>
</html>
```

Parts of an HTML Document

1. <!DOCTYPE html>

- Declares the document type
- Tells the browser it is an HTML5 document

2. <html> Tag

- Root element of the HTML page
- Contains all other elements

3. <head> Section

- Contains **information about the page** (not shown directly on screen)
- Includes:
  - Title of the page
  - Meta information
  - Links to CSS or scripts

4. <title> Tag

- Sets the title shown in the browser tab

5. <body> Section

- Contains **visible content** of the web page
- Includes text, images, links, tables, etc.

Common Elements Used in HTML Documents

- Headings: <h1> to <h6>
- Paragraphs: <p>
- Links: <a>
- Images: <img>
- Line break:

Example:

```
<h1>Main Heading</h1>
<p>This is a paragraph.</p>
<a href="https://example.com">Visit Site</a>
```

Steps to Build an HTML Document

1. Open a text editor (Notepad or Visual Studio Code)
2. Write HTML code
3. Save file with .html extension
4. Open file in a web browser like Google Chrome
5. View the webpage

Features of HTML Documents

- Simple to create
- Works in all browsers
- Platform independent
- Easy to modify and update

4.6 Use of Font Size and Attributes

1. Font Size in HTML

Font size defines how big or small the text appears on a web page.

Methods to set font size:

1. Using <font> tag (Old method – not recommended in modern HTML)

```
<font size="5">This is large text</font>
```

- size="1" = very small
- size="7" = very large

This method is outdated.

2. Using CSS (Modern method – recommended)

```
<p style="font-size:20px;">This is styled text</p>
```

Advantages:

- More control over appearance
- Used in modern web design
- Works with all browsers like Google Chrome

2. HTML Attributes

Attributes provide extra information about HTML elements. They are always written inside the opening tag.

Common HTML Attributes

1. href (Link Attribute)

```
<a href="https://example.com">Click Here</a>
```

- Used to define link destination

2. src (Source Attribute)

```
<img src="image.jpg">
```

- Used to display images

3. alt (Alternative Text)

```
<img src="image.jpg" alt="Nature Image">
```

- Shows text if image fails to load

4. style (Design Attribute)

```
<p style="color:blue;">Blue Text</p>
```

- Used to apply CSS styling

5. title Attribute

```
<p title="This is a tooltip">Hover over me</p>
```

- Shows extra information when mouse is placed over text

Importance of Font Size and Attributes

- Improves readability of web pages
- Enhances user experience
- Helps in designing attractive websites
- Provides structure and meaning to content

4.7 Backgrounds, Formatting tags, Images, Hyperlinks, div tag

In **HTML (HyperText Markup Language)**, different elements are used to design and structure web pages on the Internet. These elements help make web pages attractive, readable, and interactive.

1. Backgrounds in HTML

Backgrounds are used to set the visual appearance behind content on a web page.

Types:

Background Color

<body style="background-color:lightblue;">

- Changes the background color of the page

Background Image

<body style="background-image:url('bg.jpg');">

- Adds an image as background

Importance:

- Improves design and appearance
- Makes web pages visually attractive

2. Formatting Tags in HTML

Formatting tags are used to style text in a web page.

Common Formatting Tags:

- → Bold text
- → Italic text
- <u> → Underlined text
- → Important bold text
- → Emphasized text
- <mark> → Highlighted text

Example:

This is bold and italic text.

3. Images in HTML

Images are added using the <img> tag.

Syntax:

<img src="image.jpg" alt="Sample Image">

Attributes:

- src → image file path
- alt → alternative text if image does not load
- width and height → size control

Importance:

- Makes web pages more attractive
- Helps in visual communication

4. Hyperlinks in HTML

Hyperlinks connect one page to another.

Syntax:

Visit Website

Types:

- External links (to other websites)
- Internal links (within same website)
- Email links

Importance:

- Helps navigation between pages
- Builds connectivity on the web

5. Tag in HTML

The tag is a **container element** used to group other HTML elements.

Syntax:

```
<div style="background-color:yellow;">
  <h2>Section Title</h2>
```

```
  <p>This is inside a div.</p>
</div>
```

Features:

- Used for grouping content
- Helps in page layout design
- Works with CSS for styling
- Does not display anything by itself

4.8 List Type and its Tags, Table Layout

1. Types of Lists in HTML

A. Ordered List

- Displays items in a **numbered format**
- Used when order is important

**Tag: **

Example:

```
<ol>
  <li>Apple</li>
  <li>Banana</li>
  <li>Mango</li>
</ol>
```

B. Unordered List

- Displays items with **bullets**
- Used when order is not important

**Tag: **

Example:

```
<ul>
  <li>Pen</li>
  <li>Pencil</li>
  <li>Book</li>
</ul>
```

C. Description List

- Used to describe terms and their meanings

Tags: <dl>, <dt>, <dd>

Example:

```
<dl>
  <dt>HTML</dt>
  <dd>Markup language for web pages</dd>
</dl>
```

2. Table Layout in HTML

A **table** is used to display data in rows and columns.

Table Tags:

- <table> → Creates a table
- <tr> → Table row
- <th> → Table heading
- <td> → Table data

Example of Table Layout:

```
<table border="1">
  <tr>
    <th>Name</th>
    <th>Age</th>
  </tr>
  <tr>
```

```
  <td>Rahul</td>
  <td>20</td>
 </tr>
 <tr>
  <td>Sita</td>
  <td>18</td>
 </tr>
</table>
```

Features of HTML Tables:

- Organize data clearly
- Easy comparison of information
- Used in reports, results, and data display

Table Layout Structure

Basic Structure:

```
Table
├── Row (<tr>)
│    ├── Header (<th>)
│    └── Data (<td>)
```

4.9 Use of Frames and Forms in Web Pages

Frames are used to **divide a web page into multiple sections**, where each section can display a different HTML document.

Tags Used:

- <frameset> → Defines how the page is divided
- <frame> → Defines each section (frame)
- <iframe> → Used to embed another web page inside a page (modern method)

Example (Frameset – Old Method):

```
<frameset cols="50%,50%">
 <frame src="page1.html">
 <frame src="page2.html">
</frameset>
```

Example (Iframe – Modern Method):

```
<iframe src="https://example.com" width="300" height="200"></iframe>
```

Uses of Frames:

- Display multiple pages in one window
- Useful for menus, headers, and content sections
- Helps in separating navigation and content

Note:

- <frameset> is now outdated in modern HTML
- <iframe> is commonly used instead

2. Forms in Web Pages

What are Forms?

Forms are used to **collect user input** such as text, password, email, and selections.

Tag Used:

- <form> → Creates a form

Example:

```
<form>
 Name: <input type="text"><br>
 Email: <input type="email"><br>
```

```
 <input type="submit" value="Submit">
</form>
```

Common Form Elements:

- <input> → Text box, password, checkbox, radio button
- <textarea> → Multi-line text input
- <button> → Clickable button
- <select> → Drop-down list

Uses of Forms:

- User registration (sign up)
- Login pages
- Online surveys
- Contact forms
- Data submission

How Forms Work:

1. User enters data
2. Data is submitted using the form
3. Server processes the data
4. Response is sent back

4.10 Working with Style sheet: Elements and different Type of style sheet;

A **Style Sheet** is used to control the appearance and layout of web pages.
In web designing, **CSS (Cascading Style Sheets)** is used to add styles such as colors, fonts, spacing, borders, and positioning to HTML elements.
CSS helps in:

- Making web pages attractive
- Separating content from design
- Reducing repeated formatting
- Improving website maintenance

Elements of CSS

A CSS rule contains the following parts:

```
selector {
   property: value;
}
```

Example

```
h1 {
   color: blue;
   font-size: 30px;
}
```

Explanation

- **Selector** → h1
- **Property** → color, font-size
- **Value** → blue, 30px

Different Types of Style Sheets

There are mainly **3 types of CSS Style Sheets**:

1. Inline Style Sheet
2. Internal (Embedded) Style Sheet
3. External Style Sheet

1. Inline Style Sheet

Inline CSS is written directly inside the HTML element using the style attribute.
Example

```
<p style="color:red; font-size:20px;">
  Welcome to CSS
</p>
```

Advantages

- Easy for small changes
- Useful for testing

Disadvantages

- Difficult to manage large websites
- Repeats code

2. Internal (Embedded) Style Sheet

Internal CSS is written inside the <style> tag within the <head> section of the HTML document.

Example

```
<!DOCTYPE html>
<html>
<head>
<style>
h1 {
  color: green;
}

p {
  font-size: 18px;
}
</style>
</head>

<body>

<h1>Welcome</h1>
<p>This is Internal CSS.</p>

</body>
</html>
```

Advantages

- Easy to manage one webpage
- No separate CSS file required

Disadvantages

- Cannot be reused for multiple pages

3. External Style Sheet

External CSS is written in a separate .css file and linked to the HTML page.

HTML File

```
<!DOCTYPE html>
<html>
<head>
<link rel="stylesheet" href="style.css">
</head>

<body>

<h1>DAV College</h1>
<p>External CSS Example</p>
```

```
</body>
</html>
```

CSS File (style.css)

```
h1 {
  color: blue;
}

p {
  font-size: 20px;
  color: red;
}
```

Advantages

- Reusable for many webpages
- Easy maintenance
- Cleaner HTML code

Disadvantages

- Requires separate CSS file

Comparison of Style Sheets

Type	Location	Reusability	Best Use
Inline CSS	Inside HTML element	No	Small changes
Internal CSS	Inside <style> tag	Limited	Single webpage
External CSS	Separate .css file	Yes	Large websites

4.11 Introduction to Java Script: Identifier & operator, control structure, functions, Predefined functions, numbers & string functions, Array in Java scripts.

JavaScript is a **scripting language** used to make web pages interactive and dynamic.
It is mainly used for:

- Form validation
- Calculations
- Animation
- Pop-up messages
- Dynamic webpage content

JavaScript works together with **HTML** and **CSS**.

Features of JavaScript

- Lightweight scripting language
- Object-based language
- Platform independent
- Supports event handling
- Used in web development

Identifiers in JavaScript

Identifiers are the **names** used for variables, functions, and objects.

Rules for Identifiers

- Must begin with a letter, _, or $
- Cannot start with a number
- Cannot use reserved keywords

Example

```
var studentName = "Rahul";
var marks = 85;
```

Here:

- studentName and marks are identifiers.

Operators in JavaScript

Operators are symbols used to perform operations.

1. Arithmetic Operators

Operator	Meaning	Example
+	Addition	a + b
-	Subtraction	a - b
*	Multiplication	a * b
/	Division	a / b
%	Modulus	a % b

Example

```
var a = 10;
var b = 5;

console.log(a + b);
console.log(a * b);
```

2. Comparison Operators

Operator	Meaning
==	Equal to
!=	Not equal
>	Greater than
<	Less than

3. Logical Operators

Operator	Meaning
&&	AND
||	OR
!	NOT

Control Structures in JavaScript

Control structures control the flow of execution.

1. if Statement

```
var age = 18;

if(age >= 18){
   console.log("Eligible to vote");
}
```

2. if-else Statement

```
var number = 10;

if(number % 2 == 0){
   console.log("Even Number");
}
else{
```

```
   console.log("Odd Number");
}
```

3. switch Statement

```
var day = 2;

switch(day){
   case 1:
      console.log("Monday");
      break;

   case 2:
      console.log("Tuesday");
      break;

   default:
      console.log("Invalid");
}
```

4. Looping Statements

for Loop

```
for(var i=1; i<=5; i++){
   console.log(i);
}
```

while Loop

```
var i = 1;

while(i <= 5){
   console.log(i);
   i++;
}
```

Functions in JavaScript

Functions are reusable blocks of code.

Syntax

```
function functionName(){
   // code
}
```

Example

```
function greet(){
   console.log("Welcome to JavaScript");
}

greet();
```

Function with Parameters

```
function add(a, b){
   return a + b;
}

console.log(add(5, 3));
```

Predefined Functions in JavaScript

JavaScript provides many built-in functions.

Example 1: alert()
alert("Welcome");
Example 2: prompt()
var name = prompt("Enter your name");
Example 3: confirm()
confirm("Are you sure?");

Number Functions in JavaScript
JavaScript provides methods for number operations.
Example
var num = 12.567;

console.log(num.toFixed(2));
Common Number Functions

Function	Purpose
toFixed()	Rounds number
parseInt()	Converts string to integer
parseFloat()	Converts string to decimal

String Functions in JavaScript
Strings are sequences of characters.
Example
var text = "JavaScript";

console.log(text.length);
console.log(text.toUpperCase());
console.log(text.toLowerCase());
Common String Functions

Function	Purpose
length	Returns string length
toUpperCase()	Converts to uppercase
toLowerCase()	Converts to lowercase
charAt()	Returns character at position

Arrays in JavaScript
An array stores multiple values in a single variable.
Creating an Array
var fruits = ["Apple", "Banana", "Mango"];

Accessing Array Elements
console.log(fruits[0]);
console.log(fruits[1]);

Array Functions
var colors = ["Red", "Blue"];

colors.push("Green");

console.log(colors);
Common Array Methods

Method	Purpose

Method	Purpose
push()	Add element
pop()	Remove last element
shift()	Remove first element
unshift()	Add element at beginning

Unit V

5.1 Basic of Cyber Security and Cyber Crime: Computer Ethics and Application Programs

Introduction

With the rapid growth of computers and the internet, protecting digital information has become very important.

Cyber Security helps protect computers, networks, and data from unauthorized access and cyber attacks.

Cyber Crime refers to illegal activities performed using computers or the internet.

Cyber Security

Definition

Cyber Security is the practice of protecting computer systems, networks, software, and data from cyber attacks, damage, or unauthorized access.

Objectives of Cyber Security

- Protect data and information
- Maintain privacy
- Prevent hacking and malware attacks
- Ensure safe internet usage
- Protect online transactions

Types of Cyber Security

1. Network Security

Protects computer networks from unauthorized access.

Example

Using firewalls and antivirus software.

2. Information Security

Protects confidential information from theft or misuse.

3. Application Security

Protects software and applications from threats.

Example

Password protection in applications.

4. Internet Security

Protects online activities such as email, browsing, and online banking.

Common Cyber Threats

Threat	Description
Virus	Malicious program that damages files
Malware	Harmful software
Phishing	Fake emails or websites to steal data
Hacking	Unauthorized access to systems
Ransomware	Locks files and demands money

Safety Measures in Cyber Security

- Use strong passwords
- Install antivirus software
- Avoid suspicious links
- Update software regularly
- Use secure websites (https)
- Backup important data

Cyber Crime
Definition
Cyber Crime means illegal activities carried out using computers, mobile devices, or the internet.

Types of Cyber Crime
1. Hacking
Accessing computer systems without permission.

2. Identity Theft
Stealing personal information such as passwords or bank details.

3. Online Fraud
Cheating people through fake websites or online scams.

4. Cyber Bullying
Harassing or threatening people online.

5. Software Piracy
Illegal copying or distribution of software.

Effects of Cyber Crime
- Financial loss
- Data theft
- Loss of privacy
- Damage to reputation
- System failure

Computer Ethics
Definition
Computer Ethics refers to moral principles and proper behavior while using computers and the internet.

Rules of Computer Ethics
1. Do not access others' files without permission.
2. Do not spread viruses or harmful software.
3. Respect copyright laws.
4. Do not use computers for illegal activities.
5. Use the internet responsibly.

Importance of Computer Ethics
- Promotes safe technology use
- Protects privacy
- Prevents cyber crime
- Encourages responsible behavior

Application Programs
Definition
Application Programs are software designed to perform specific tasks for users.

Types of Application Programs

Application Program	Purpose
Word Processor	Create documents
Spreadsheet	Perform calculations

Application Program	Purpose
Presentation Software	Create presentations
Web Browser	Access internet
Media Player	Play audio/video

Examples of Application Programs

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Google Chrome
- VLC Media Player

5.2 Cyber Law, Introduction to IT laws & Cyber Crimes – Internet, Hacking, Cracking, Viruses, Virus Attacks, Software Piracy

Introduction

With the growth of computers and the internet, many online activities such as banking, shopping, communication, and data sharing are performed digitally. To control illegal activities and ensure safe use of technology, **Cyber Laws** and **IT Laws** were introduced.

Cyber Law

Definition

Cyber Law is the branch of law that deals with legal issues related to computers, digital communication, the internet, and cyber crimes.

It provides rules and regulations for:

- Internet usage
- Online transactions
- Data protection
- Digital signatures
- Cyber crimes

Objectives of Cyber Law

- Protect internet users
- Prevent cyber crimes
- Secure electronic transactions
- Protect privacy and data
- Promote safe digital communication

IT Laws

Introduction to IT Laws

IT Laws (Information Technology Laws) are laws related to the use of information technology and digital communication.

In India, the major law related to cyber activities is the:

Information Technology Act 2000

This law was introduced to:

- Give legal recognition to electronic records
- Control cyber crimes
- Support e-commerce and digital communication

Features of IT Act 2000

- Legal recognition of digital signatures
- Electronic record protection
- Punishment for cyber crimes
- Regulation of online activities

- Data protection provisions

Cyber Crimes
Definition
Cyber Crime means illegal activities performed using computers, mobile devices, networks, or the internet.

Types of Cyber Crimes

1. Internet Crimes
Internet crimes are illegal activities committed through the internet.
Examples
- Online fraud
- Fake websites
- Cyber bullying
- Identity theft

2. Hacking
Hacking means gaining unauthorized access to a computer system or network.
Example
A person accessing someone's email account without permission.
Effects
- Data theft
- Privacy violation
- Financial loss

3. Cracking
Cracking means breaking security systems or software protections with malicious intent.
Example
Breaking software passwords or license protections.
Difference Between Hacking and Cracking

Hacking	Cracking
May be ethical or legal	Always illegal
Used for testing security	Used for harmful purposes

4. Viruses
A computer virus is a harmful program that damages computer files and systems.
Characteristics
- Self-replicating
- Spreads from one system to another
- Damages data and software

Virus Attacks
Definition
A virus attack occurs when malicious software infects a computer and causes harm.

Types of Virus Attacks

Virus Type	Description
Boot Sector Virus	Affects system boot files
File Virus	Infects files and programs
Macro Virus	Attacks documents
Worm	Spreads automatically through networks

Effects of Virus Attacks

- Slow computer performance
- Data corruption
- File deletion
- System crashes
- Information theft

Protection from Viruses

- Install antivirus software
- Avoid unknown email attachments
- Update software regularly
- Scan USB drives
- Use secure websites

Software Piracy
Definition
Software Piracy means illegal copying, installation, or distribution of software without permission from the owner.

Types of Software Piracy

1. Copying software illegally
2. Using fake software licenses
3. Downloading cracked software
4. Sharing paid software without permission

Effects of Software Piracy

- Financial loss to software companies
- Security risks
- Virus infections
- Legal punishment

Prevention of Software Piracy

- Use genuine software
- Buy licensed software
- Avoid illegal downloads
- Follow copyright laws

Importance of Cyber Security and Cyber Laws

- Protects digital information
- Ensures safe internet use
- Prevents cyber crimes
- Protects privacy and online transactions

5.3 Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits.
Intellectual Property (IP)
Definition
Intellectual Property refers to creations of the human mind such as inventions, software, designs, music, books, and trademarks that are protected by law.
It gives creators legal rights over their creations.

Types of Intellectual Property

Type	Description
Copyright	Protects books, music, software, and creative works
Patent	Protects inventions and new technologies
Trademark	Protects brand names, logos, and symbols
Trade Secret	Protects confidential business information

Importance of Intellectual Property

- Encourages innovation and creativity
- Protects original work from copying
- Gives legal ownership rights
- Promotes business growth

Intellectual Property in Information Technology

In Information Technology, IP protection is important for:

- Software programs
- Mobile applications
- Website designs
- Databases
- Digital content

Example

Software developed by a company is protected under copyright laws.

Legal System of Information Technology

Definition

The Legal System of Information Technology consists of laws and regulations related to computers, networks, software, digital communication, and cyber activities.

Objectives of IT Legal System

- Protect digital data
- Prevent cyber crimes
- Regulate online activities
- Provide legal recognition to electronic records
- Ensure safe electronic transactions

Features of IT Legal System

1. Recognition of electronic documents
2. Digital signature authentication
3. Cyber crime punishment
4. Data privacy protection
5. E-commerce regulation

Social Engineering

Definition

Social Engineering is a technique used by attackers to manipulate people into revealing confidential information such as passwords or bank details.

Instead of attacking systems directly, attackers exploit human emotions like trust, fear, or curiosity.

Common Types of Social Engineering

Type	Description
Phishing	Fake emails or messages to steal information

Type	Description
Impersonation	Pretending to be a trusted person
Baiting	Offering fake rewards or downloads
Shoulder Surfing	Watching someone enter passwords

Prevention of Social Engineering

- Never share passwords
- Verify unknown emails or calls
- Avoid suspicious links
- Use two-factor authentication
- Stay aware of online scams

Mail Bombs

Definition

A Mail Bomb is a cyber attack in which a large number of emails are sent to a person or server to overload the system.

The purpose is to:

- Slow down systems
- Crash email servers
- Harass users

Effects of Mail Bombs

- Server overload
- Email service disruption
- Reduced system performance
- Loss of important communication

Prevention of Mail Bombs

- Use spam filters
- Limit email traffic
- Use firewall protection
- Block suspicious email addresses

Bug Exploits

Definition

A Bug Exploit is the misuse of a software weakness or error (bug) to gain unauthorized access or cause damage.

Attackers take advantage of software vulnerabilities for illegal purposes.

Examples of Bug Exploits

- Accessing systems without permission
- Stealing information
- Crashing applications
- Spreading malware

Causes of Bug Exploits

- Programming errors
- Weak security testing
- Outdated software
- Poor system updates

Prevention of Bug Exploits