

Unit III

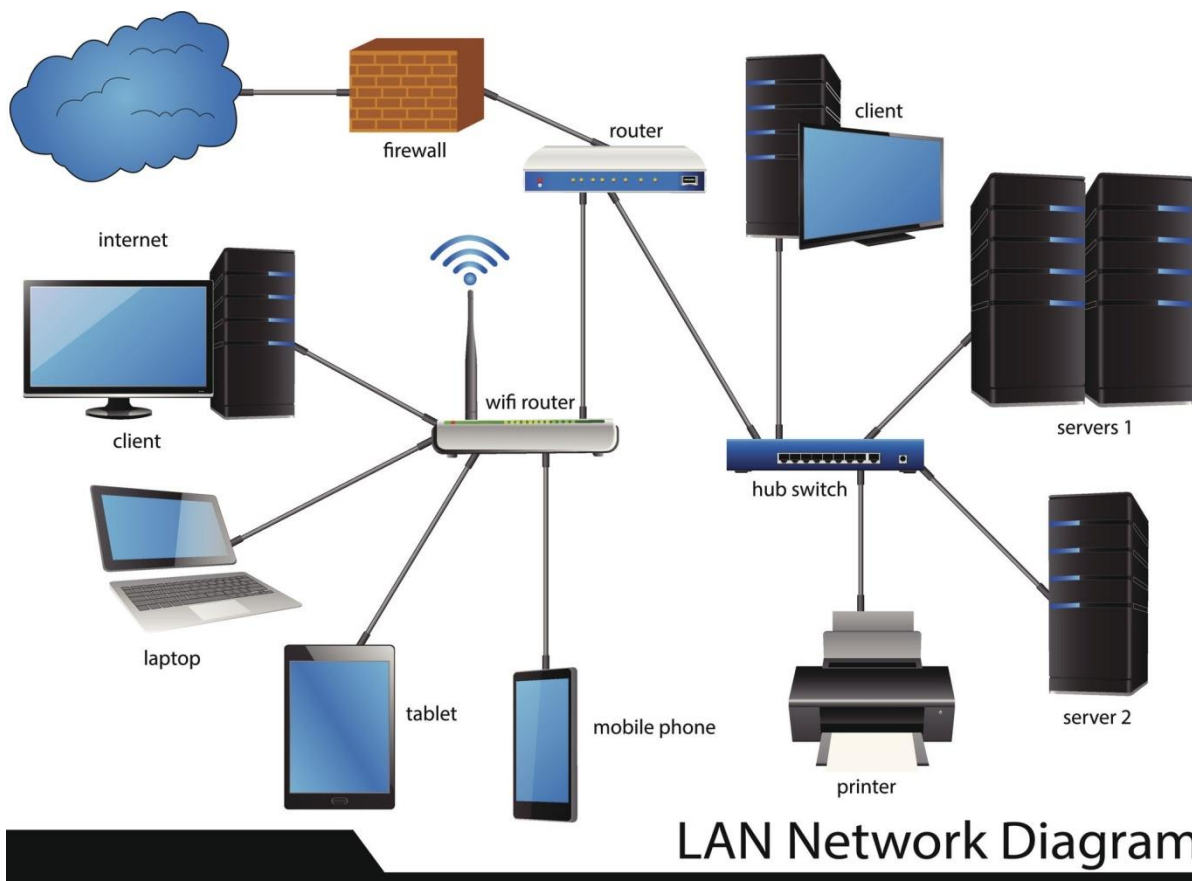
INTERNET AND ITS APPLICATIONS IN EDUCATION

A **computer network** is a system of interconnected computing devices that can communicate and share resources with one another. It enables the transmission and exchange of information, forming the backbone of modern digital life.

Types of Networks

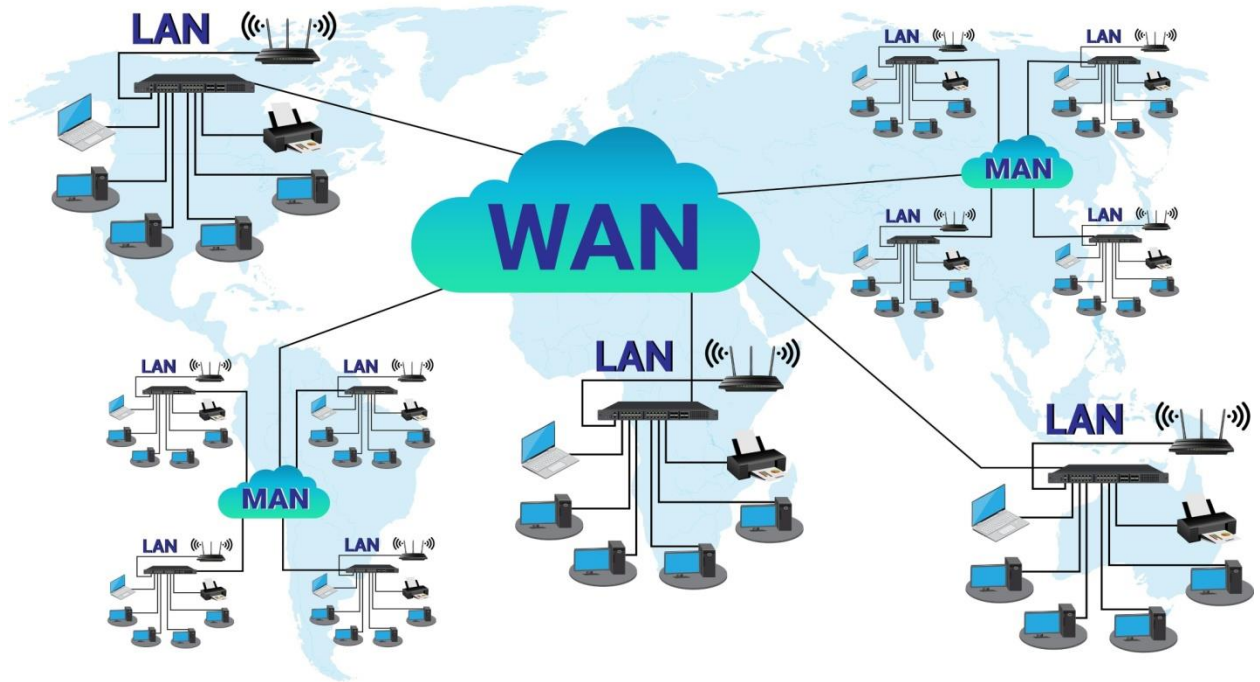
Networks are typically classified by their geographical area.

- **Local Area Network (LAN):** Connects devices within a small, confined area like a home, office building, or school. LANs are known for their high data transfer speeds and are used for sharing resources such as printers and files. A home Wi-Fi network is a common example of a LAN.



- **Metropolitan Area Network (MAN):** Larger than a LAN but smaller than a WAN, a MAN connects devices across an entire city or a large campus. It's often used to connect multiple LANs together and is commonly seen in cable television networks or city-wide wireless connections.
- **Wide Area Network (WAN):** Spans a large geographical area, such as a state, country, or even the world. The internet is the most well-known example of a WAN, connecting countless smaller networks together. WANs are used for long-distance communication and data transmission.

WAN Wide Area Network



- **Personal Area Network (PAN):** The smallest type of network, connecting devices within a person's immediate workspace. A PAN has a very limited range and is often used for devices like a wireless mouse, keyboard, or Bluetooth headphones.

Modes of Connection

Computer networks can be connected using two primary modes: wired and wireless.

Wired Connection

A **wired connection** uses physical cables to transfer data between devices.

- **How it works:** Data is sent through electrical signals or light pulses over physical media like Ethernet cables, coaxial cables, or fiber-optic cables.
- **Characteristics:**
 - **Speed & Reliability:** Generally faster and more stable than wireless connections because they are not subject to radio frequency interference.
 - **Security:** Considered more secure since data transmission is contained within a physical cable, making it harder to intercept.
 - **Mobility:** Lacks mobility, as devices must be physically connected to the network.

Wireless Connection

A **wireless connection** transmits data through the air without the use of physical cables.

- **How it works:** Devices communicate using electromagnetic waves, such as radio waves (Wi-Fi, Bluetooth) or infrared signals.
- **Characteristics:**
 - **Speed & Reliability:** Typically slower and less reliable than wired connections due to potential interference from physical obstructions (walls) and other electronic devices.
 - **Security:** Less secure than wired connections as the signal can be intercepted, although modern encryption methods have significantly improved security.
 - **Mobility:** Offers great mobility and convenience, allowing devices to connect from anywhere within the signal range.

The **Internet** is a global system of interconnected computer networks that allows devices worldwide to communicate and share resources. It is often described as a "network of networks" because it links millions of private, public, academic, and government networks together, enabling the transfer of a vast range of data and services.

Educational Applications of the Internet

The Internet has revolutionized education by making knowledge more accessible and transforming traditional learning methods. Here are some key applications:

- **Online Learning and E-learning:** The Internet enables distance education through online courses and entire degree programs. Platforms like Coursera, Udemy, and Khan Academy offer a wide variety of subjects, allowing students to learn at their own pace and from anywhere in the world.



- **Access to Information and Research:** The Internet serves as a massive digital library. Students and researchers can access a wealth of information through academic databases, digital libraries, online encyclopedias, and countless websites. This makes research faster and more comprehensive than ever before.
- **Collaborative Tools:** The Internet facilitates collaboration between students and educators. Tools like Google Classroom, Microsoft Teams, and other learning management systems (LMS) allow for virtual classrooms, group projects, shared document editing, and real-time communication.

- **Interactive Learning and Gamification:** Websites and apps use interactive quizzes, games, and simulations to make learning more engaging. Platforms like Kahoot! and Duolingo use gamification to motivate students and reinforce concepts in a fun way.
- **Digital Content Creation:** The Internet empowers students to become creators, not just consumers. They can create blogs, websites, podcasts, and videos to showcase their work, develop digital literacy skills, and share their knowledge with a global audience.

Here are some fundamental internet terms and their definitions.

Basic Internet Terms

- **Browser:** A software application used to access and view websites and webpages. Popular examples are Google Chrome, Mozilla Firefox, and Microsoft Edge.
- **ISP (Internet Service Provider):** A company that provides you with access to the internet. They own the infrastructure that connects you to the global network. Examples include Comcast, AT&T, and Verizon.
- **Website:** A collection of related webpages, typically identified by a common domain name (like google.com).
- **Webpage:** A single document on the web, often a part of a larger website. It is identified by a unique URL.
- **Homepage:** The main or first page of a website. It serves as the entry point and provides an overview and navigation links to other parts of the site.
- **URL (Uniform Resource Locator):** The unique address that specifies the location of a webpage or file on the internet. For example, <https://www.google.com/> is a URL.
- **Wi-Fi:** A technology that uses radio waves to provide a wireless internet connection.
- **Hotspot:** A physical location where you can get a wireless internet connection, typically provided by a Wi-Fi router. A mobile hotspot uses your phone's cellular data to create a personal Wi-Fi network.
- **Client:** A computer or device that requests information or services from a **server**. Your laptop or smartphone is a client when you browse the web.
- **Server:** A powerful computer or program that stores data and serves it to clients. When you visit a website, the server sends the webpage's data to your browser (the client).
- **Download & Upload:**
 - **Download:** The process of receiving data from a server to your device (e.g., saving a movie or a file from the internet).
 - **Upload:** The process of sending data from your device to a server (e.g., posting a photo on social media or sending an email).
- **Online & Offline:**
 - **Online:** Being actively connected to a network, like the internet.
 - **Offline:** Not being connected to any network.
- **Cloud (Cloud Computing):** A system that delivers computing services—including servers, storage, databases, and software—over the internet. It allows you to access and store data on remote servers instead of your local device.
- **Hacking:** The act of compromising digital devices and networks by gaining unauthorized access. While the term is often associated with malicious activity, some "ethical hackers" legally test systems to find vulnerabilities.

Communication and collaboration tools are digital platforms and software that enable individuals and groups to interact, share information, and work together, regardless of their physical location. In education, they are transforming traditional learning by creating connected, interactive, and flexible environments.

E-learning Platforms and E-schooling Services

These are comprehensive online systems that deliver educational content and manage the entire learning process. They serve as a digital version of a school or classroom.

- **Communication:** They provide various tools for communication, such as discussion forums, internal messaging systems, and announcement boards, which allow for asynchronous communication between students and teachers.
- **Collaboration:** They support collaborative projects by offering shared document spaces, wikis, and group assignment tools that allow students to work together on tasks. Examples include **Google Classroom** and **Moodle**.

E-mail (Electronic Mail)

E-mail is a fundamental tool for sending and receiving digital messages over a computer network. It is a cornerstone of professional and academic communication.

- **Communication:** It is used for formal one-on-one or group communication. Teachers use it to send announcements and assignments, while students use it to ask questions, submit work, and seek clarification.
- **Collaboration:** While not a real-time tool, e-mail is crucial for coordinating group projects, sharing files, and keeping a documented history of communication.

Online Conferencing (Audio and Video)

This involves conducting live, real-time meetings over the internet. These tools simulate face-to-face interaction, which is essential for remote learning and meetings.

- **Communication:** Platforms like **Zoom** and **Google Meet** enable live lectures, office hours, and one-on-one meetings. The use of audio and video helps participants see and hear each other clearly.
- **Collaboration:** Features like screen sharing, digital whiteboards, and breakout rooms facilitate collaboration. A teacher can share a presentation, a student can work on a problem on the virtual whiteboard, or a group can work on a project in a separate digital room.

E-library

An e-library (or digital library) is a collection of digital resources, such as e-books, journals, and multimedia, that can be accessed online.

- **Communication and Collaboration:** While not a direct communication tool, e-libraries support collaboration by providing a centralized repository of resources that all students can access

simultaneously. This enables them to share research, discuss materials, and work on projects using the same reference points.

Virtual Classrooms

A virtual classroom is a specific type of online learning environment that closely mimics a physical classroom.

- **Communication and Collaboration:** It provides a platform for live, synchronous sessions with features like a teacher-led lecture space, chat functionality, and interactive tools for real-time engagement. Students can "raise their hands" and participate in polls, while teachers can manage the class and facilitate discussions.

Educational Websites and Portals

These are websites that provide educational content and services. They range from simple repositories of information to sophisticated learning hubs.

- **Communication and Collaboration:** Many educational websites provide forums and comment sections for students to discuss topics. Educational portals, in particular, serve as a single point of access to various school resources (e.g., student grades, schedules, assignments), improving communication between students, teachers, and parents. Examples include Khan Academy for learning materials and school-specific portals for academic management.

Concepts of Digital Safety and Cyber Hygiene

Digital Safety refers to the practices and precautions you take to protect your information and privacy while using the internet. It is about being aware of the risks and knowing how to navigate the digital world securely.

Cyber Hygiene is the routine and regular maintenance of your digital health, similar to how personal hygiene maintains your physical health. It involves a set of good habits that help you mitigate online threats.

Key practices of cyber hygiene include:

- **Strong Password Management:** Using long, complex, and unique passwords for every account. Using a password manager is highly recommended.
- **Multi-Factor Authentication (MFA):** Enabling an extra layer of security beyond a password, such as a code sent to your phone, to verify your identity.
- **Regular Software Updates:** Keeping your operating systems, applications, and web browsers updated to patch security vulnerabilities that hackers can exploit.
- **Data Backup:** Regularly backing up your important files to an external drive or cloud service to protect against data loss from hardware failure or a ransomware attack.
- **Awareness and Caution:** Being able to recognize and avoid threats like phishing emails, suspicious links, and deceptive pop-up ads.

Threats: Viruses and Malware

Malware (malicious software) is a broad term for any software designed to harm or exploit a computer system. **Viruses** are a specific type of malware.

- **Viruses:** A type of malware that attaches itself to a legitimate file or program. When the infected file is executed, the virus replicates and spreads to other files on the system, often corrupting data or causing system instability.
- **Malware:** This category includes a wide range of threats:
 - **Ransomware:** Encrypts a user's files and demands a ransom payment to restore access.
 - **Spyware:** Secretly monitors user activity to steal personal information like passwords or banking details.
 - **Trojans:** Malicious software disguised as a harmless or useful program. When you run the program, the Trojan secretly performs harmful actions in the background.

Management of Threats

Managing these threats involves both prevention and mitigation:

- **Prevention:** The best defense is to prevent an infection in the first place by practicing good cyber hygiene. Avoid clicking suspicious links, be careful with email attachments, and only download software from trusted sources.
- **Mitigation:** If a system is infected, you must disconnect it from the network to prevent the malware from spreading. Then, you need to use specialized software to identify and remove the threat.

Use of Antivirus Software and Firewalls

Antivirus software and **firewalls** are two essential components of a layered security strategy. They work together to protect a computer system.

- **Antivirus Software:** A program designed to detect, prevent, and remove malicious software.
 - **Function:** It scans files and programs on your computer, compares them against a database of known malware signatures, and uses behavioral analysis to identify new or unknown threats. When a threat is found, it quarantines or deletes the malicious file.
 - **Analogy:** Think of antivirus as an internal security guard that patrols the inside of your house, looking for intruders that have already made it inside.
- **Firewall:** A security system that acts as a barrier between your computer and the outside network, such as the internet. It can be a hardware device or a software program.
 - **Function:** It monitors and filters all incoming and outgoing network traffic based on a set of predefined security rules. It blocks unauthorized access attempts and prevents malicious data packets from entering your system.
 - **Analogy:** A firewall is like a gatekeeper at the entrance of your property, checking every person and package before allowing them to enter or leave.

While an antivirus can't stop an external attack, and a firewall can't remove a virus once it's inside, using them together provides robust protection by defending both the perimeter and the interior of your system