

# CH 1

A **network** is a system that connects multiple devices, such as computers, smartphones, or servers, allowing them to communicate with each other. These devices are called **nodes**. The main purpose of a network is to share information and resources like files, internet access, and printers. Networks help people and businesses work more efficiently by enabling quick and easy communication between devices.

There are different types of networks, depending on their size and scope. A **Local Area Network (LAN)** connects devices within a small area, like an office or home. A **Wide Area Network (WAN)**, on the other hand, connects devices over large distances, like the internet, which is the largest network in the world.

Networks can be connected through **wired connections**, like cables, or **wireless connections**, such as Wi-Fi. Wireless networks use radio waves to transmit data between devices, making them more convenient for mobile use.

Each device on the network follows rules, called **protocols**, to ensure that data is sent and received properly. The most common protocol for networks is **TCP/IP**, which is used for internet communication. Networks help to improve productivity, enable collaboration, and allow for faster and more efficient sharing of resources.

## What is a Network?

A **network** is a group of interconnected devices, such as computers, phones, servers, and other hardware, that communicate and share resources with each other. These devices are connected using either wired (cables) or wireless (Wi-Fi, Bluetooth) methods. The main purpose of a network is to enable devices to exchange information, like files, data, or messages, and to share resources like printers or internet connections.

## Why is a Network Required?

Networks are essential because they allow for:

1. **Resource Sharing:** Devices can share printers, storage drives, and internet connections, reducing the need for duplicate resources.
2. **Efficient Communication:** Networks allow fast and easy communication between devices through email, chat, and file transfers, improving collaboration.
3. **Data Access and Sharing:** Users can access and share files from different locations on the network, increasing convenience and productivity.
4. **Centralized Management:** In business networks, administrators can control and monitor all devices from a central location, making it easier to manage updates, security, and troubleshooting.
5. **Cost Savings:** By sharing resources and data, companies can save on equipment costs, streamline processes, and improve workflow efficiency.

## **<span style="color:green">Advantages of Networks:</span>**

1. **Resource Sharing:** Devices can share printers, files, and internet access, saving time and money.
2. **Easy Communication:** People can quickly send emails, messages, or files to each other.
3. **Centralized Storage:** All important files can be stored in one place and accessed by everyone.
4. **Remote Work:** You can access the network from anywhere, which is great for working from home.
5. **Data Backup:** Data can be backed up centrally, reducing the risk of losing important files.
6. **Cost-Effective:** Businesses save money by sharing resources instead of buying separate ones for each user.
7. **Collaboration:** Teams can work together easily by sharing documents and resources on the network.
8. **Easier Management:** A network allows for easier control and management of all connected devices.
9. **Flexible Access:** Access to data and applications is available from any device on the network.
10. **Software Sharing:** Multiple users can access the same software without needing to install it on every device.

## **<span style="color:green">Disadvantages of Networks:</span>**

1. **Security Issues:** Networks can be targets for hackers, viruses, or cyberattacks.
2. **Setup Costs:** Creating a network can be expensive due to hardware and software costs.
3. **Complicated to Fix:** When something goes wrong, fixing the network can take time and expertise.
4. **Risk of Data Loss:** If the network fails or is attacked, data can be lost or corrupted.
5. **Requires Maintenance:** Networks need regular updates and monitoring to function properly.
6. **Slower Speeds:** When many people use the network at the same time, it can become slower.
7. **Dependence on the Network:** If the network goes down, productivity can stop because people can't access their files or tools.
8. **Needs Skilled Personnel:** You need skilled IT professionals to manage and maintain the network.
9. **Software Costs:** Sometimes, businesses need special software to run the network, which can be costly.
10. **Hardware Failures:** If a critical device like a server breaks down, the whole network can be affected.

## NETWORK TYPES :

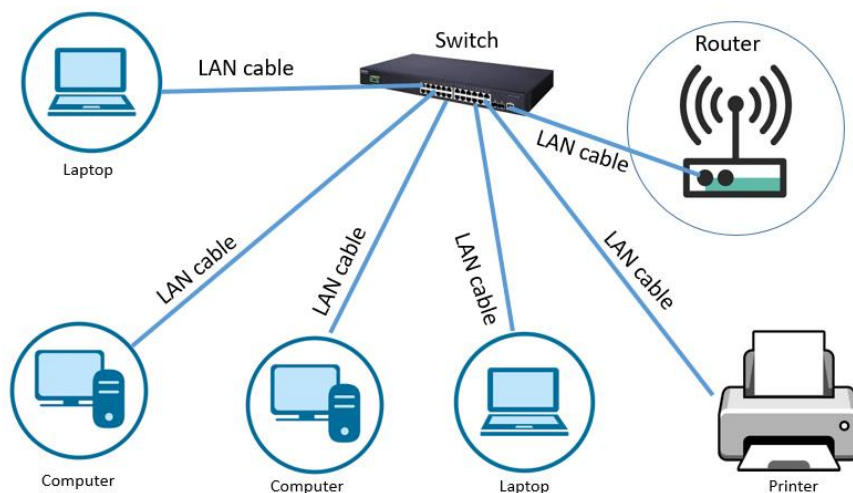
### PERSONAL AREA NETWORK



### PAN (Personal Area Network)

A Personal Area Network (PAN) is a small network designed for an individual, typically covering just a few meters around a person. It connects personal devices like smartphones, laptops, tablets, and smartwatches. A PAN is often used for personal tasks such as transferring files, syncing data between devices, or connecting to wireless headphones.

For example, when you connect your smartphone to your laptop via Bluetooth or Wi-Fi, you're creating a PAN. It's the smallest type of network and is very limited in range, usually just a few meters. PANs are common in homes or small workspaces where the network needs to cover only a single person or device.

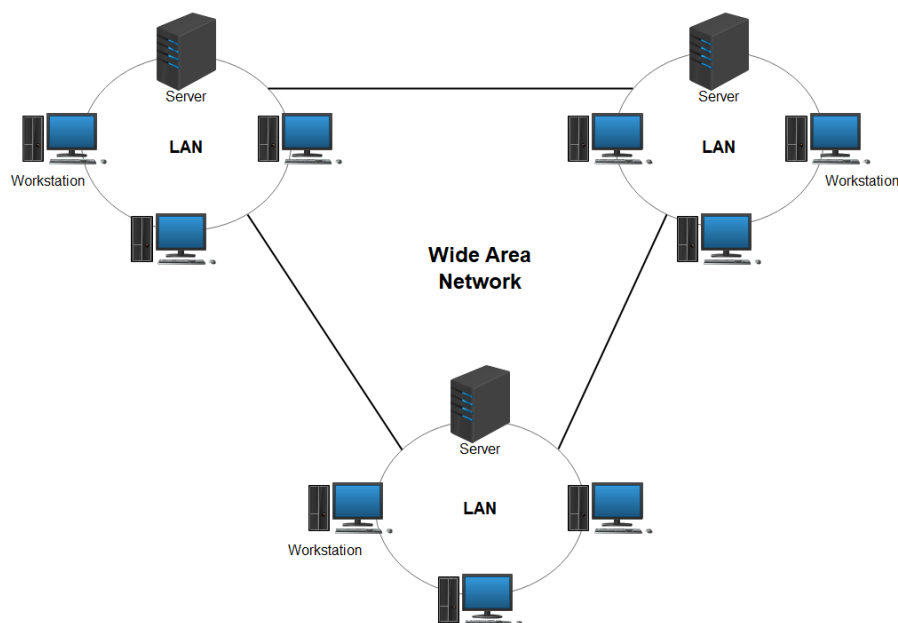


## Local Area Network

## LAN (Local Area Network)

A **Local Area Network (LAN)** connects devices within a small, specific area, like a single building, office, or home. It is the most common type of network used in businesses, schools, or homes. LANs are fast, reliable, and allow multiple users to share resources like printers, files, or internet connections.

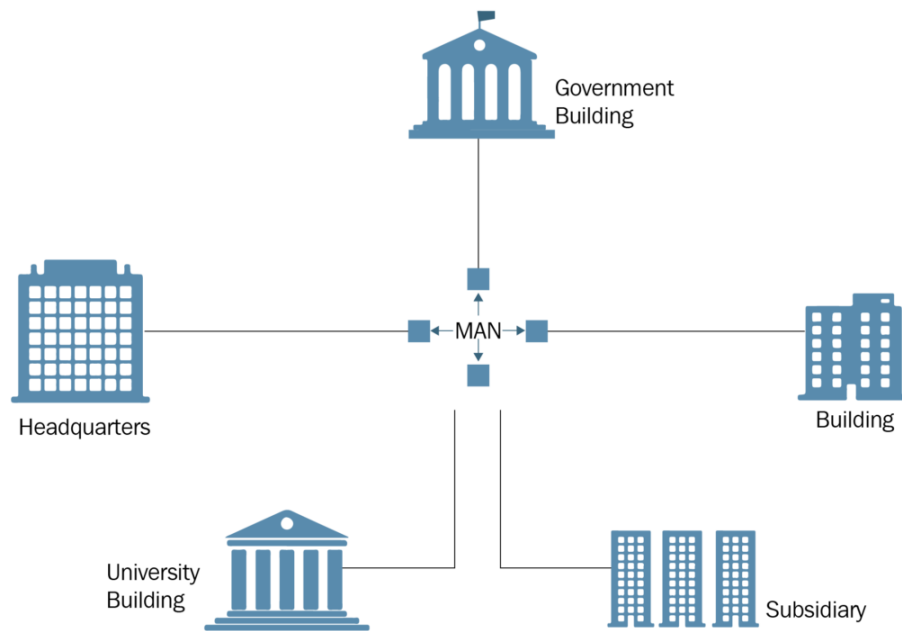
For example, in a school or office building, all the computers connected to each other through a LAN can share files and access the internet through a central router. A LAN typically covers a small area, usually within one building, and is cost-effective to set up.



## WAN (Wide Area Network)

A **Wide Area Network (WAN)** covers a large geographical area, connecting multiple smaller networks (like LANs) over long distances. WANs are often used by large companies, governments, or organizations that need to connect offices or branches in different cities or even countries. The internet itself is the largest WAN in the world, connecting computers across the globe.

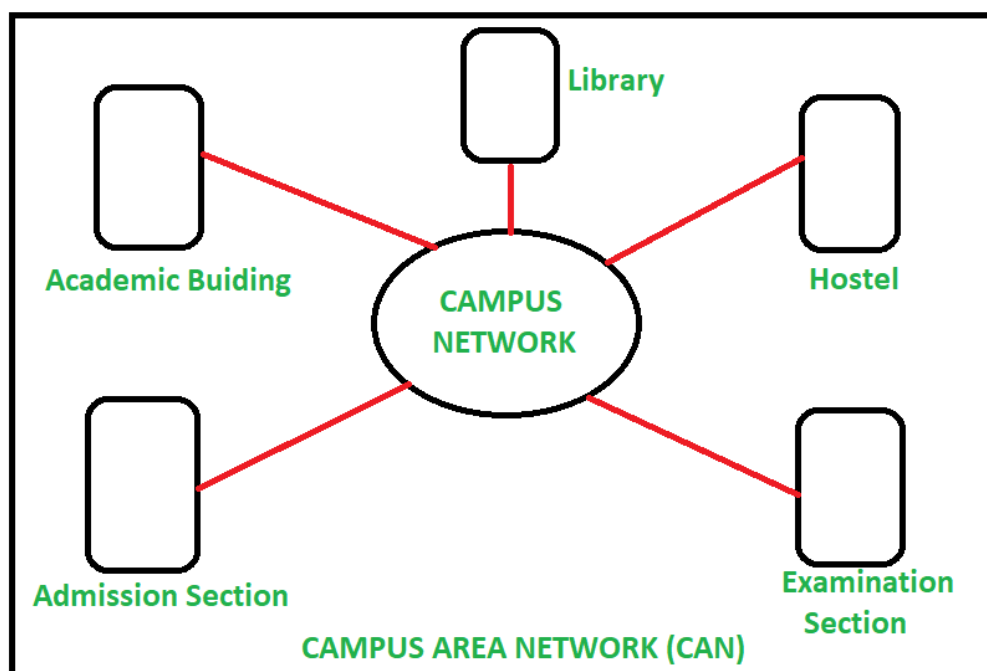
For example, a company with offices in different cities like New York, London, and Tokyo might use a WAN to allow employees in each office to share data and communicate with each other. WANs are more complex and expensive to maintain than LANs due to the need for specialized equipment and services.



## MAN (Metropolitan Area Network)

A Metropolitan Area Network (MAN) connects multiple LANs across a larger area, like a city or a large campus. It is larger than a LAN but smaller than a WAN. MANs are commonly used by organizations like universities, government agencies, or large corporations to connect different buildings within a city.

For example, a university might use a MAN to connect all its campuses spread across a city, allowing students and staff in different locations to share data, use the internet, and access university resources. MANs are usually faster than WANs and can cover distances of up to 50 kilometers.

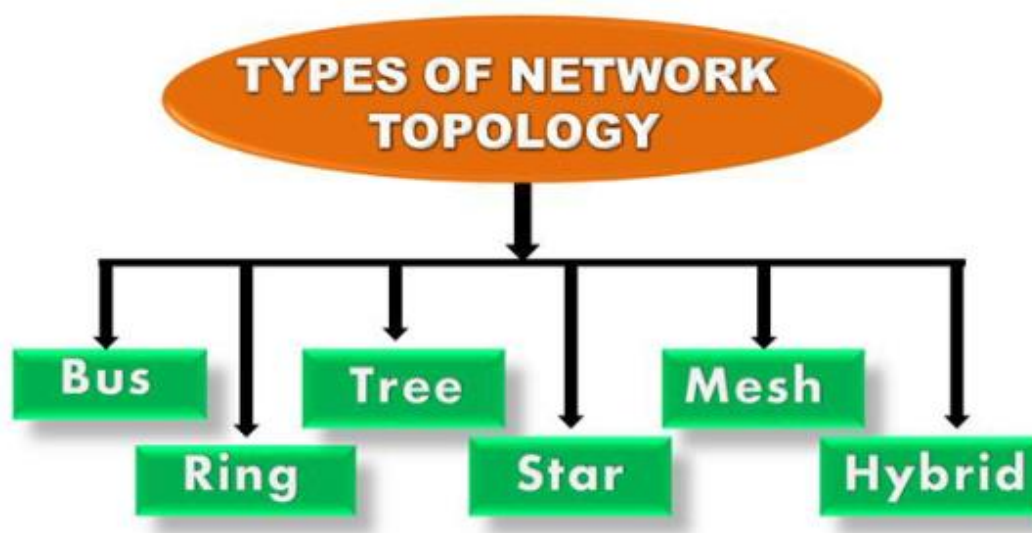


## CAN (Campus Area Network)

A Campus Area Network (CAN) is a network that connects multiple buildings within a specific area like a university campus, corporate office, or hospital. It's similar to a LAN but covers a larger area and is used to connect multiple LANs together. A CAN allows easy communication and data sharing between the buildings in a specific campus or area.

For example, a company might use a CAN to connect all the departments in different buildings across its corporate campus. This allows employees to share files and resources without needing an internet connection. CANs are designed to be fast and secure, making them ideal for places that need reliable connectivity over a small geographic area.

## Network Topology :



### BUS Topology

Bus topology is a simple network setup where all devices (nodes) are connected to a single, central cable called a "bus." Data is transmitted along this bus, and each device checks the data to see if it's intended for them. If not, the data moves on to the next device. Only one device can send data at a time to prevent collisions.

For example, imagine a classroom where every computer is connected to the same cable. When one computer sends data, it travels along the cable until it reaches the correct destination. Bus topology is easy and cheap to set up, but it has limitations. If the central cable (bus) fails, the entire network stops working. It's best suited for small networks where only a few devices are connected.

## RING Topology

In Ring topology, each device is connected to exactly two other devices, forming a circular path for data to travel. Data moves in one direction around the ring until it reaches the intended device. Every device acts as a repeater, boosting the signal as it passes through.

For example, imagine several computers arranged in a circle, each one passing data to the next. In a ring topology, data moves in a predictable direction, so there's less chance of data collisions. However, if one device in the ring fails, the whole network can break down. Ring topology is used in some older types of networks but isn't as common today because of this weakness.

---

## TREE Topology

Tree topology is a hierarchical structure that combines elements of both Bus and Star topologies. It starts with a root node, which is usually the main computer or server, and branches out into smaller networks. Each branch can have its own devices connected in a bus or star configuration.

For example, a university network might use tree topology, with the main server at the top (root), and different departments (branches) connected to it. Each department can have its own smaller LAN (Local Area Network). The advantage of tree topology is that it's scalable, meaning you can add more branches as the network grows. However, if the root node (main server) fails, the entire network can be disrupted.

---

## STAR Topology

In Star topology, every device is connected to a central hub or switch. The hub manages all data traffic, ensuring that information gets from one device to another. If a device wants to send data, it first sends it to the hub, which then forwards it to the correct destination.

For example, in an office, every computer might be connected to a central server. If one computer fails, it doesn't affect the others, but if the central hub or server goes down, the entire network stops functioning. Star topology is commonly used because it's easy to manage and troubleshoot. It's more reliable than bus or ring topologies, but it can be more expensive due to the need for a central hub.



## MESH Topology

Mesh topology is a setup where each device is connected to every other device in the network. This creates a web of connections, allowing data to take multiple paths to reach its destination. There are two types of mesh topology: **full mesh**, where every device connects to every other device, and **partial mesh**, where only some devices have multiple connections.

For example, in a military or emergency services network, a mesh topology ensures that communication can still happen even if some connections fail. It's highly reliable because there's always another route for the data to travel. However, setting up a full mesh network can be expensive and complicated due to the number of connections required.

---

## HYBRID Topology

Hybrid topology is a combination of two or more different types of network topologies, like star, bus, or ring. It takes the best features from each topology to create a more flexible and efficient network. A hybrid network can be designed to meet specific needs, making it adaptable and scalable as the network grows.

For example, a large company might use a star topology for each department's local network and then connect these star networks using a bus topology. This setup allows the network to grow and change without affecting the entire system. Hybrid topology is widely used because it offers the strengths of multiple topologies while minimizing their weaknesses, though it can be more expensive and complex to manage.





## Internet

The Internet is a global network that connects millions of computers and devices around the world. It allows people to share information, communicate, and access a wide variety of online services like websites, email, and social media. The internet uses standard protocols like TCP/IP to ensure that data can move between different networks seamlessly.

For example, when you use your phone to search something on Google, your device connects to the internet to communicate with Google's servers. The servers send the search results back to your device, and you see them on your screen. The internet is open to everyone, making it a public network that anyone can access with the right device and connection.

The internet has become essential for everyday life, enabling everything from online shopping to video calls. However, since it's a public network, it's vulnerable to security risks like hacking and viruses, which is why protecting your data online is so important.

---

## Intranet

An Intranet is a private network that's used within an organization, like a company or school. Unlike the internet, which is open to everyone, an intranet is only accessible to authorized users, such as employees or students. It's often used to share company information, collaborate on projects, and communicate internally.

For example, a business might have an intranet where employees can access internal documents, company policies, or a private chat system. Employees must log in to the intranet with a username and password, ensuring that only they can access the company's resources. Intranets often use similar technology as the internet (like web browsers), but they're closed off from the public.

The main advantage of an intranet is security. Since only authorized people can access it, sensitive information stays within the organization. Intranets can also boost productivity by providing a centralized place for resources and communication.

## Unicast

Unicast is a one-to-one communication method in networking where data is sent from one device (sender) to another specific device (receiver). This is the most common type of data transfer, especially when browsing the web or sending emails. Only the intended recipient receives the data, and other devices on the network are not involved.

For example, when you send an email to a friend, that's unicast communication. The email goes from your computer to your friend's email server without involving other users. Unicast is efficient for direct communication but may not be the best option when you need to send the same data to multiple recipients.

Unicast is widely used because it provides a private and direct form of communication. However, it can use more bandwidth if the same data needs to be sent to multiple people, as the sender would need to repeat the process for each recipient.

---

## Broadcast

Broadcast is a one-to-all communication method in which data is sent from one device to all devices on a network. Every device on the network receives the same data, regardless of whether it was intended for them. This method is often used in local area networks (LANs) to share important information with all connected devices.

For example, in a school network, if the administrator sends an announcement to all computers in the building, that's a broadcast. Every computer receives the same message at the same time. Broadcasts are useful when information needs to reach everyone at once, but they can also flood the network with unnecessary data.

Broadcasting is efficient for sending the same message to many people quickly, but it can slow down the network if overused. Only certain types of data (like network management information) are typically sent this way because most communication needs to be more targeted.

---

## Multicast

Multicast is a one-to-many communication method, where data is sent from one device to a specific group of devices on a network, not to all devices. It's more efficient than broadcast because only the intended recipients receive the data. Multicast is commonly used for services like live streaming, video conferencing, and online gaming, where many people are watching or interacting at the same time.

For example, in a webinar, the presenter's video is sent to everyone who signed up to view it. Instead of sending individual copies of the video to each viewer, multicast sends a single stream that's shared among the group. This reduces the bandwidth required while still reaching all participants.

Multicast helps save network resources by ensuring that data is only sent to the group of devices that need it, rather than broadcasting to everyone. It's especially useful in applications where many users need to receive the same data at the same time.



### What is the Internet?

The Internet is a vast global network that connects millions of computers and devices all over the world. It allows people to communicate, share information, and access various services like websites, emails, and social media. You can think of it as a giant web that links countless devices, making it possible for them to exchange data with one another.

At its core, the Internet is made up of numerous smaller networks that communicate using standard protocols, primarily **TCP/IP** (Transmission Control Protocol/Internet Protocol). These protocols ensure that data is sent and received correctly between devices, regardless of their location or type. The Internet is not owned by any single organization; instead, it's a collective of interconnected networks operated by various service providers, governments, and institutions.

One of the most significant features of the Internet is that it's constantly evolving. New technologies and applications are developed all the time, which can change how we use the Internet. From online shopping to video streaming, the Internet has become an essential part of daily life for billions of people around the globe.

---

### Why is the Internet Called a Network?

The Internet is called a **network** because it consists of many interconnected devices that communicate with each other. A network, in simple terms, is a group of two or more devices that can share information. The Internet takes this concept to a much larger scale, linking millions of devices across different locations.

Each device connected to the Internet can send and receive data, allowing for the sharing of resources and information. This can include anything from websites and applications to files and videos. The ability to connect different types of devices, whether they are computers, smartphones, or servers, makes the Internet a versatile and powerful network.

Moreover, the Internet allows for various types of communication, such as **unicast** (one-to-one), **multicast** (one-to-many), and **broadcast** (one-to-all). This flexibility in communication methods is one of the reasons the Internet is such a robust network. By linking various devices and enabling different types of data exchange, the Internet has transformed how we interact and share information globally.

---

## How Does the Internet Work?

The Internet works through a combination of hardware and software that facilitates data transmission. When you want to access a website, your device sends a request through your Internet Service Provider (ISP). The ISP connects you to the broader Internet, routing your request to the appropriate server that hosts the website you want to visit.

Once the server receives your request, it processes it and sends back the required data, such as the website's content. This data travels back to your device in small packets. Each packet contains a portion of the information, as well as the address of the sender and receiver. The Internet uses routers to direct these packets to their destination, ensuring they take the best possible path.

Once all the packets reach your device, your computer or smartphone reassembles them, and you see the website on your screen. This whole process happens in a matter of seconds, making it seem instantaneous. The Internet's design allows for efficient and reliable data transfer, which is why we can browse, communicate, and share information so easily today.



## Advantages of the Internet

### 1. Information Access

The Internet provides vast amounts of information on almost any topic imaginable. You can easily find articles, videos, and research papers to learn about anything.

### 2. Communication

It allows instant communication through emails, messaging apps, and social media, making it easy to stay in touch with friends and family anywhere in the world.

### 3. Online Shopping

You can buy products and services online from the comfort of your home, which saves time and offers a wider selection than physical stores.

### 4. Education and Learning

There are many online courses and educational resources available, allowing people to learn new skills and gain knowledge without attending traditional schools.

### 5. Remote Work

The Internet has made it possible for many people to work from home, providing flexibility and reducing commuting time.

### 6. Entertainment

You can stream movies, music, and games online, providing endless entertainment options.

## 7. Social Connections

Social media platforms help people connect with others who share similar interests, fostering community and friendship.

## 8. Research and Development

The Internet accelerates innovation by allowing researchers and developers to share ideas and collaborate across distances.

## 9. Banking and Finance

Online banking makes it easy to manage your finances, pay bills, and transfer money without needing to visit a bank.

## 10. Global Awareness

The Internet connects people worldwide, promoting cultural exchange and understanding of global issues.

# Disadvantages of the Internet

## 1. Cybersecurity Threats

The Internet can expose users to risks like hacking, identity theft, and viruses, putting personal information at risk.

## 2. Misinformation

There's a lot of false or misleading information online, which can lead to confusion and poor decision-making.

## 3. Addiction

Some people may spend excessive amounts of time online, leading to addiction that can affect mental health and relationships.

## 4. Privacy Issues

Personal data can be collected and misused by companies and malicious actors, raising concerns about privacy.

## 5. Social Isolation

While the Internet connects people, it can also lead to isolation, as individuals may prefer online interactions over real-life relationships.

## 6. Distraction

The abundance of content online can lead to distractions, making it hard for students and professionals to focus on their tasks.

## 7. Digital Divide

Not everyone has equal access to the Internet, leading to disparities in information and opportunities.



#### 8. Inappropriate Content

The Internet hosts content that may be harmful or inappropriate for certain audiences, especially children.

#### 9. Dependence on Technology

Over-reliance on the Internet can lead to issues when technology fails or is unavailable.

#### 10. Environmental Impact

The infrastructure that supports the Internet requires energy and resources, contributing to environmental concerns.



## What is Intranet?

An intranet is a private network that is used within an organization, such as a company, school, or government office. Unlike the Internet, which is open to everyone, an intranet is restricted to authorized users only. It provides a secure environment where employees or members of the organization can share information, collaborate on projects, and communicate efficiently.

Think of an intranet as a smaller version of the Internet, designed specifically for internal use. It typically includes features like internal websites, document sharing, and communication tools that help streamline workflows and improve productivity. Intranets can also host applications that are useful for the organization, such as HR systems or project management tools.

Intranets are often built using similar technology as the Internet, including web browsers and servers, making it easy for users to access information through familiar interfaces. Because it is private, sensitive information can be shared without the risk of exposure to outsiders, ensuring better security for the organization's data.

---

## How it Works?

An intranet works by connecting devices within a specific organization through a secure network. To access the intranet, users typically need a username and password to log in. This ensures that only authorized individuals can access the resources available on the intranet. Once logged in, users can access various tools and resources that are essential for their work.

The structure of an intranet often includes a central server that hosts all the applications and information. Users can interact with the intranet through web browsers, similar to how they would access websites on the Internet. Information can be stored in databases, and users can retrieve documents, submit requests, or communicate with colleagues using the intranet's tools.

Intranets may also include communication features like chat systems, forums, or email, allowing for real-time collaboration among team members. Regular updates and maintenance are essential to keep the intranet secure and functioning properly. Overall, an intranet enhances internal communication, improves access to information, and fosters a sense of community within the organization.

## Advantages of Intranet

### 1. Improved Communication

An intranet enhances communication within the organization, making it easier for employees to share information and collaborate.

### 2. Centralized Information

It provides a single location for important documents, resources, and company policies, making it easier for employees to find what they need.

### 3. Enhanced Security

Since an intranet is private, it offers better security for sensitive information compared to the public Internet.

### 4. Increased Productivity

With easy access to tools and information, employees can work more efficiently and effectively, leading to higher productivity.

### 5. Cost-Effective

Using an intranet can reduce costs related to printing and distributing physical documents, as most resources can be accessed digitally.

### 6. Customizable

Organizations can tailor their intranet to meet specific needs, adding features and tools that are relevant to their operations.

### 7. Facilitates Training

Intranets can host training materials and resources, making it easier for employees to learn new skills and improve their knowledge.

### 8. Project Management Tools

Intranets can include project management features that help teams coordinate tasks, set deadlines, and track progress.

### 9. Employee Engagement

Intranets can foster a sense of community by allowing employees to share news, updates, and achievements within the organization.

### 10. Version Control

Intranet systems can keep track of document versions, ensuring that employees always access the most up-to-date information.

## Disadvantages of Intranet

### 1. Initial Setup Costs

Creating an intranet can require significant initial investment in technology, software, and training.

### 2. Maintenance Requirements

Regular updates and maintenance are necessary to keep the intranet running smoothly, which can require dedicated IT resources.

### 3. Limited Access

Since intranets are private, employees may not have access to the same information and resources they would find on the Internet.

### 4. User Resistance

Some employees may be hesitant to adopt a new intranet system, preferring traditional communication methods instead.

### 5. Technical Issues

Like any technology, intranets can experience technical problems that may disrupt access to information and tools.

### 6. Overload of Information

If not organized properly, an intranet can become cluttered with too much information, making it hard for users to find what they need.

### 7. Dependence on Technology

Employees may become overly reliant on the intranet for information, leading to reduced face-to-face communication.

### 8. Limited Mobility

Intranets are often accessible only within the organization, making it challenging for remote employees to access necessary resources.

### 9. Security Risks

While intranets are generally secure, they can still be vulnerable to internal threats or unauthorized access if not properly managed.

### 10. Lack of Updates

If not regularly updated, information on the intranet can become outdated, leading to confusion and misinformation among employees.

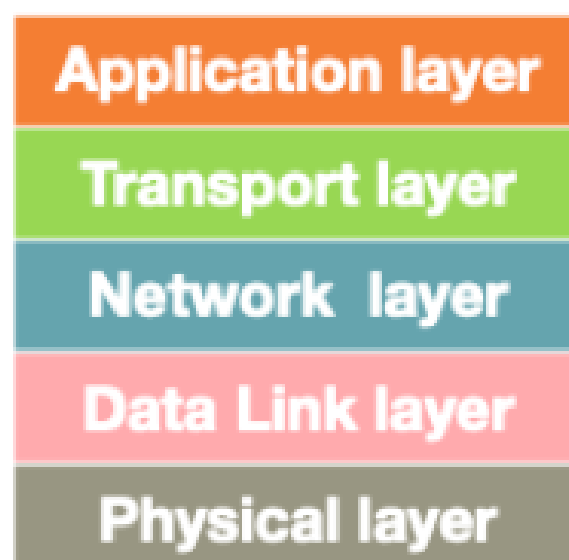
## WORKING WITH INTERNET AND ARCHITECTURE

### Working of the Internet

The Internet works by connecting millions of computers and devices to form a global network. When you want to access a website or send data, your device communicates with other devices through a series of steps. Here's how it typically works:

1. **Request Initiation:** When you type a website address (URL) into your browser and hit enter, your computer sends a request to a Domain Name Server (DNS). The DNS translates the website name into an IP address, which is a unique address for the server that hosts the website.
2. **Data Transmission:** Once the IP address is identified, your request travels through your Internet Service Provider (ISP) and over various networks to reach the server hosting the website. This journey may involve multiple routers and switches that direct the data along the fastest available path.
3. **Server Response:** The server receives your request and processes it. It then sends back the requested data, such as the website's content, in small packets. These packets travel back through the network, often taking different routes to reach your device.
4. **Reassembly:** Once the packets arrive at your device, your browser reassembles them into a complete webpage, which you can then view. This entire process happens in seconds, making it seem instantaneous.

### Five-layered Internet Protocol Stack



## 1. Physical Layer

**What it does:** This is the foundation of the Internet architecture. It includes the hardware components like cables, routers, and switches that physically connect devices.

**How it works:** When you send data, this layer converts it into electrical signals, light pulses, or radio waves for transmission over various mediums.

## 2. Data Link Layer

**What it does:** This layer ensures that data packets are transferred reliably between devices on the same local network.

**How it works:** It frames the data packets, checks for errors, and manages how devices on the network communicate. It's like ensuring that messages are properly packaged and addressed before being sent.

## 3. Network Layer

**What it does:** This layer is responsible for routing data packets between different networks.

**How it works:** It determines the best path for data to travel from the sender to the receiver. The Internet Protocol (IP) operates at this layer, assigning unique IP addresses to devices, which helps in locating them on the network.

## 4. Transport Layer

**What it does:** This layer ensures that data is delivered reliably and in the correct order.

**How it works:** It breaks down large messages into smaller packets and reassembles them at the destination. Protocols like TCP (Transmission Control Protocol) function here, providing error-checking and ensuring that all packets are received.

## 7. Application Layer

**What it does:** This is the topmost layer where users interact with the Internet through applications.

**How it works:** It includes web browsers, email clients, and other software that allow users to send and receive data. This layer provides the interface for all Internet services, enabling users to access websites, send emails, and more.



# WORKING WITH INTRANET AND ARCHITECTURE

## Working of Intranet

An intranet functions as a private network that allows users within an organization to share information and resources securely. Here's how it typically works:

1. **Access Control:** To access the intranet, users need to log in with a username and password. This ensures that only authorized employees can view or interact with the resources available on the intranet.
2. **Central Server:** The intranet is hosted on a central server that stores all the applications, documents, and resources needed by the organization. When a user requests information or a specific application, their device communicates with this server.
3. **Data Transmission:** Similar to the Internet, data is sent in packets. When a user requests a document or application, the server processes the request and sends the necessary data back to the user's device. This happens over the organization's internal network, which is usually faster and more secure than external networks.
4. **Accessing Resources:** Once the data arrives at the user's device, it is displayed through a web browser or specific application. Users can access shared documents, use company-specific software, or communicate with colleagues through the intranet.

## Architecture of Intranet

The architecture of an intranet is designed to facilitate efficient communication and resource sharing within an organization. Here are the main components:

1. **Client-Server Model:** Intranet architecture typically follows a client-server model. Clients (users' devices) request resources, and the server (central system) responds with the needed data. This separation helps manage and secure information effectively.
2. **Network Layer:** This layer consists of the physical and data link layers that connect all devices within the organization. It includes routers, switches, and cables that ensure data can be transmitted across the internal network.
3. **Application Layer:** The application layer includes the software and tools used on the intranet, such as document management systems, project management tools, and communication platforms. These applications are designed to help employees collaborate and access information easily.
4. **Database Management:** Intranets often use databases to store and manage information securely. Databases help organize data, making it easier for users to search for and retrieve information.
5. **Security Features:** Since intranets contain sensitive organizational information, they include security measures like firewalls, encryption, and access controls to protect data from unauthorized access and cyber threats.



## 1. Hub

A **hub** is a basic network device that connects multiple computers or devices within a local area network (LAN). It acts as a central point for data transmission, allowing devices to communicate with each other. When a device sends data to the hub, the hub broadcasts that data to all other connected devices, regardless of whether they need it or not.

For example, imagine a classroom where all students (devices) are sharing notes. If one student passes a note (data) to the teacher (hub), the teacher reads it and then shouts the contents to everyone in the class. This method can create confusion since not every student needs the information, leading to unnecessary traffic on the network.

Hubs are considered outdated and inefficient compared to more advanced devices like switches, as they do not manage data traffic intelligently. They work at a lower speed and can slow down the network when many devices are connected.

---

## 2. Modem


A **modem** (short for modulator-demodulator) is a device that connects your home or office network to the Internet. It converts digital signals from your computer into analog signals for transmission over telephone lines or cable systems, and vice versa. This process enables data to be sent and received over long distances.

Think of a modem like a translator between two different languages. For instance, if your computer speaks a digital language and the telephone line speaks an analog language, the modem translates messages back and forth, allowing them to understand each other. Without a modem, your devices wouldn't be able to access the Internet.

In everyday life, when you subscribe to an Internet service provider (ISP), they often provide a modem. You connect it to your home network to enable Internet access for all your devices, like laptops, smartphones, and smart TVs.

---

## 3. Switch

A **switch** is a more advanced network device compared to a hub. It connects multiple devices on a LAN and intelligently manages data traffic. When a device sends data to the switch, the switch examines the destination address and sends  data only to the specific device that needs it, rather than broadcasting it to all devices.



### 3. Switch

A switch is a more advanced network device compared to a hub. It connects multiple devices on a LAN and intelligently manages data traffic. When a device sends data to the switch, the switch examines the destination address and sends the data only to the specific device that needs it, rather than broadcasting it to all devices.

For example, imagine a post office (the switch) that sorts mail (data) to deliver it only to the intended recipients (devices). If a letter arrives for a specific person, the post office ensures it goes directly to that person's mailbox, avoiding confusion and speeding up the process.

Switches enhance network performance by reducing unnecessary traffic and collisions. They operate at a higher speed and are essential for modern networks where multiple devices need to communicate efficiently.

---

### 4. Router

A router is a device that connects different networks, such as your home network to the Internet. It directs data traffic between these networks, ensuring that information reaches its correct destination. Routers also assign local IP addresses to devices within the network, allowing them to communicate with each other.


Think of a router as a traffic officer at a busy intersection. Just as the officer directs vehicles (data) to their appropriate destinations (networks), the router manages data packets, deciding the best route for them to travel. This process involves analyzing the destination IP address and determining the most efficient path.

In real life, when you connect to your home Wi-Fi, you're using a router. It allows all your devices to access the Internet while keeping them connected to each other, enabling things like file sharing and online gaming.

---

### 5. Gateway

A gateway is a device that serves as a "gate" between two different networks, often translating protocols so that they can communicate. It can connect a local network to the Internet or link networks that use different communication protocols, allowing them to work together.

Imagine a gateway as a customs officer at an international border. Just as the customs officer checks and processes goods coming from different  ntries (networks), the gateway ensures that data

## 5. Gateway

A gateway is a device that serves as a "gate" between two different networks, often translating protocols so that they can communicate. It can connect a local network to the Internet or link networks that use different communication protocols, allowing them to work together.

Imagine a gateway as a customs officer at an international border. Just as the customs officer checks and processes goods coming from different countries (networks), the gateway ensures that data moving between distinct networks is properly formatted and routed. It handles conversions and translations that allow smooth communication.

In a typical home setting, the gateway may be integrated into a modem or router, allowing your local network to connect to the broader Internet while managing differences in data formats and protocols.

---

## 6. Access Point

An access point (AP) is a device that extends a wired network by providing wireless connectivity. It allows wireless devices, like laptops and smartphones, to connect to the network without needing physical cables. Access points can be used to increase the range of a Wi-Fi network or to connect different wireless devices within a larger network.

Think of an access point as a Wi-Fi hotspot in a coffee shop. Customers (devices) can connect to the Internet without needing to plug in. The access point receives data from the wired network and transmits it wirelessly, making it easy for multiple users to access the Internet simultaneously.

In larger buildings or campuses, multiple access points may be deployed to ensure strong and consistent Wi-Fi coverage. This setup enables users to move around freely while staying connected, making it essential for modern workplaces and public spaces.

## 1. Coaxial Cable

Coaxial cable is a type of electrical cable that consists of a central conductor surrounded by insulation, a metallic shield, and an outer plastic sheath. This design helps protect the signal from interference, making coaxial cables effective for transmitting data over moderate distances.

A common real-life example of coaxial cable is the cable TV connection in your home. When you connect your TV to a cable service, the coaxial cable carries the television signal from the wall outlet to your TV set. This type of cable can transmit both video and audio signals, providing a reliable connection for viewing channels.

Coaxial cables are also used in some Internet connections. They can carry high-frequency signals, making them suitable for cable modems. However, they are less flexible compared to other types of cables and can be bulkier, which may limit their use in certain situations.

---

## 2. Unshielded Twisted Pair (UTP) Cable

Unshielded twisted pair (UTP) cable consists of pairs of insulated copper wires twisted together. This twisting helps reduce electromagnetic interference and crosstalk from adjacent pairs. UTP cables are widely used for networking and telecommunications.

A familiar example of UTP cable is the Ethernet cable you might use to connect your computer to a router or switch. When you set up a home network, the UTP cable allows your devices to communicate with each other and access the Internet. The twisted pairs help maintain a clear signal over relatively short distances, making UTP cables suitable for local area networks (LANs).

UTP cables are categorized into different types based on their performance, such as Cat5e, Cat6, and Cat6a, which indicate the maximum speed and bandwidth they can support. They are popular due to their affordability, ease of installation, and versatility in various networking environments.

### 3. Fiber Optic Cable

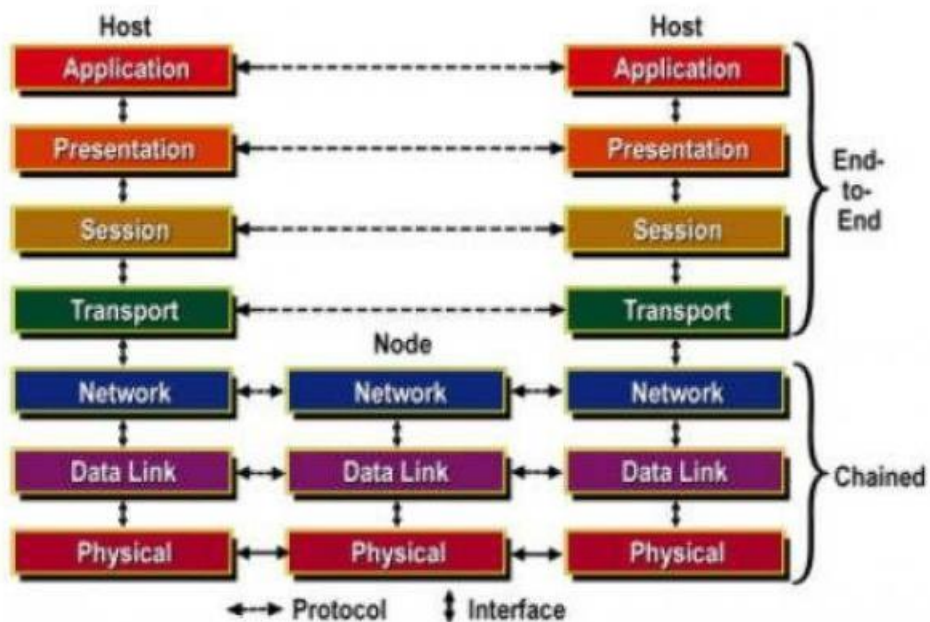
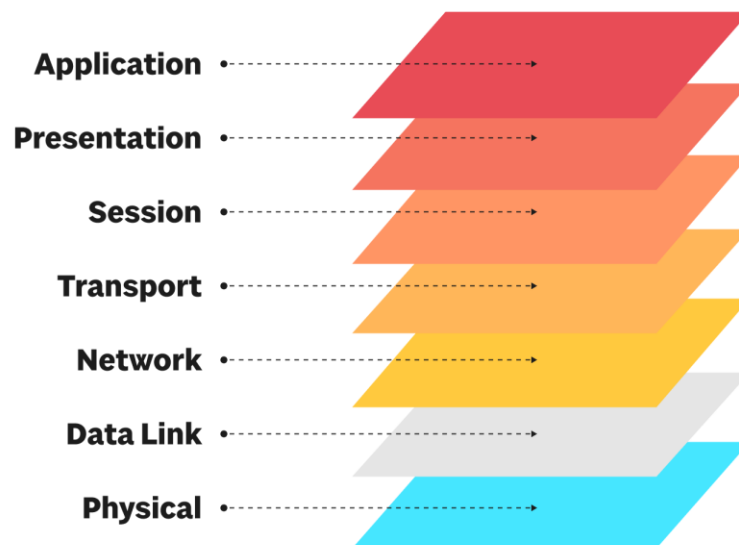
Fiber optic cable uses thin strands of glass or plastic to transmit data as light signals. This technology allows for extremely high-speed data transmission over long distances without significant loss of signal quality. Fiber optic cables are less susceptible to interference compared to copper cables.

A real-life example of fiber optic cable is the high-speed Internet connections offered by many service providers. When you subscribe to a fiber optic Internet service, the data travels through these cables as light pulses, enabling fast download and upload speeds. This is especially beneficial for activities like streaming videos, online gaming, and video conferencing.

Fiber optic cables are also used in telecommunications, medical instruments, and various industrial applications due to their ability to transmit large amounts of data quickly and reliably. Although they can be more expensive to install than copper cables, their advantages in speed and capacity make them increasingly popular for modern networks.

## UNIT 3

# The OSI Model



THE OSI REFERENCE MODEL:

# What Is the OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

---

## 7. Application Layer


The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the [Hypertext Transfer Protocol](#) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

## 6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

## 5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.





## **4. Transport Layer**

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

## **3. Network Layer**

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

## **2. Data Link Layer**

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media [Access Control](#) (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

## **1. Physical Layer**

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.



## Concepts of OSI Model

The **OSI (Open Systems Interconnection) Model** is a conceptual framework that helps us understand how data travels from one computer to another over a network. It breaks down the communication process into seven different layers, each with its specific role. This model ensures that different networking systems and technologies can work together by standardizing the way they communicate.

Each layer in the OSI Model has a specific task, such as handling data, managing connections, or converting signals, which helps in the smooth transfer of data across networks. By organizing tasks into layers, it simplifies troubleshooting and allows for better communication between different devices and systems.

## Introduction of OSI Layers and Their Purpose

1. **Physical Layer:** This layer is all about the hardware. It handles sending the actual data through wires, cables, or wirelessly. Imagine it's like talking on a phone – this layer is responsible for making sure the voice is carried through the phone lines.
2. **Data Link Layer:** After data is sent, this layer makes sure it's packed neatly into "frames" and checks for mistakes during transmission. It's like putting a letter into an envelope and double-checking that it's sealed properly before mailing.
3. **Network Layer:** This layer figures out the best route to send your data. Just like how a GPS finds the best path for your car, the network layer finds the best way to deliver the data using IP addresses to identify the destination.
4. **Transport Layer:** The transport layer ensures all the pieces of data arrive correctly. Think of sending a package – it ensures all parts of your shipment arrive safely and in the right order. TCP and UDP work here to manage this.
5. **Session Layer:** This layer sets up, manages, and ends communication between devices. If you're making a call, the session layer opens the line, keeps the call going, and hangs up when the conversation is over.
6. **Presentation Layer:** The presentation layer makes sure that the data is in a readable format. For example, if you're sending a picture, this layer ensures both devices see it as an image instead of random code. It also handles encryption and compression.
7. **Application Layer:** This is the layer you directly interact with. When you browse the web, send an email, or transfer a file, you're using the application layer. It communicates with the software (like your web browser) to exchange data between networks.

### Data Packets

A **data packet** is a small piece of information that is sent over a network. When you send something like an email or a file, that information gets broken down into these packets. Each packet contains part of the data and important details like where it's coming from and where it's going. This way, even large messages can be sent efficiently.

Think of data packets like envelopes in the mail. Each envelope holds a piece of your message (the data) and has an address on it (the destination). When all the packets arrive at the receiver's device, they are put back together to recreate the original message. If one packet gets lost or damaged, only that packet needs to be resent, making the whole process faster and more reliable.

Using data packets allows networks to handle lots of information at once. It's easier to send many small packets rather than one big message, which helps prevent delays and ensures that data reaches its destination quickly.

---

### Datagram

A **datagram** is a specific type of data packet that is used in certain network protocols, like UDP (User Datagram Protocol). Unlike regular packets that make sure everything is received correctly, a datagram is sent without checking if the receiver is ready. This means there's no guarantee that the datagram will arrive or that it will arrive in the right order.

You can think of a datagram like sending a postcard. Once you drop it in the mailbox, you have no way of knowing if it gets to the recipient or if it gets lost along the way. If it doesn't arrive, you can't track it down or automatically resend it unless you send another one. This makes datagrams faster but less reliable.

Datagrams are useful for activities where speed is more important than accuracy, such as live video streaming or online gaming. In these cases, it's better to send data quickly, even if some of it might not make it to the other end, rather than waiting to confirm that everything is received perfectly.

## Purpose of the Presentation Layer

The **Presentation Layer** is the 6th layer in the OSI Model, and its main job is to make sure data is presented in a way that both the sending and receiving devices can understand. It acts like a translator, ensuring that the format of the data is correct for both devices. This layer is responsible for things like data formatting, data encryption, and data compression.

For example, if you're sending an image, the presentation layer ensures that the file is converted into a format that can be read by the recipient's device. It also makes sure that the data is secure by handling encryption (scrambling the data) and decryption (unscrambling it back).

In simple terms, the presentation layer ensures that the data is clean, secure, and ready to be used by the next layer (the application layer) or sent across the network.

---

## Presentation Layer Protocols and Their Purpose

The Presentation Layer uses several protocols to perform its tasks, including:

1. **SSL/TLS (Secure Sockets Layer / Transport Layer Security):** These protocols ensure secure data transmission over a network. SSL/TLS encrypts the data before sending it so that hackers cannot read it. When you visit secure websites (like those with "https" in the URL), SSL/TLS is working to keep your data private.
2. **MIME (Multipurpose Internet Mail Extensions):** MIME is used for formatting email messages. It allows emails to contain more than just plain text, like images, videos, and other files. Without MIME, you wouldn't be able to send attachments in your emails.
3. **JPEG, GIF, PNG:** These are image compression protocols that the presentation layer uses to ensure images are transferred in a smaller size without losing too much quality. This helps make sure images are sent quickly over the network.

In short, presentation layer protocols make sure that data is correctly formatted, secure, and optimized for network transfer, ensuring smooth communication between devices.

## SSL (Secure Sockets Layer)

SSL is a security technology that keeps your data safe when you're browsing the web. It works by encrypting (scrambling) the information that travels between your web browser and the website you're visiting. This way, even if someone tries to intercept the data, they won't be able to understand it because it's scrambled.

When you visit a website with **https** in the address, it means SSL (or its updated version, TLS) is being used to secure your connection. For example, when you enter your credit card information on an online shopping site, SSL makes sure that your sensitive details are protected from hackers.

SSL uses something called a **certificate** to ensure that the website you're visiting is legitimate. Websites with SSL certificates show a padlock symbol next to the URL in your browser. This lets you know that your connection is secure and encrypted.

In short, SSL is essential for protecting private information, such as passwords and credit card details, during online communication. It ensures that data exchanged between users and websites remains confidential and secure.

---

## HTTP (Hypertext Transfer Protocol)

HTTP is the basic communication protocol that web browsers and servers use to exchange information. When you visit a website, HTTP helps your browser request and receive the data (like text, images, and videos) from the server hosting the site. It's the foundation of the web, allowing browsers to display web pages.

However, HTTP itself doesn't offer any security features. This means that any information you send or receive over an HTTP connection is unprotected and can be intercepted. That's why **HTTPS** was created, which is HTTP combined with SSL/TLS for secure communication.

For example, when you type "google.com" into your browser, HTTP requests the web page, and the server sends it back. Without security, any data shared through HTTP could be accessed by others, which is why sensitive sites, like banks, always use HTTPS.

In summary, **HTTP** enables the basic functioning of the web by allowing web browsers and servers to communicate, but it lacks the security needed for sensitive information exchanges, which is why **HTTPS** is preferred for secure browsing.

## FTP (File Transfer Protocol)

FTP is a standard network protocol used to transfer files between two computers. It allows users to upload or download files to and from a server. For example, if you're a web developer, you might use FTP to upload files (like images or code) from your computer to a web server where your website is hosted.

FTP requires a **client** (the user's computer) and a **server** (the host). You log into the server using credentials, and then you can transfer files between the two. It's similar to copying files on your computer, but over a network, which can be anywhere in the world.

One downside of FTP is that it's not secure by default. Data, including your username and password, is sent in plain text, meaning it can be intercepted by others. To solve this, secure versions of FTP like **FTPS** and **SFTP** are used, which encrypt the connection to protect the data during transfer.

Overall, **FTP** is a simple and widely-used way to move files between computers, especially for tasks like website management, though users often rely on secure versions for sensitive transfers.

---

## TELNET (Teletype Network)

**TELNET** is an older network protocol that allows you to control a remote computer by typing commands from your own system. It's like opening a command-line interface (CLI) on a distant machine, letting you run programs, manage files, and configure settings on the remote system.

When using **TELNET**, you connect to another computer over a network (like the internet) and are able to access it as if you were sitting right in front of it. For example, network administrators used **TELNET** to troubleshoot and manage remote servers.

However, the biggest drawback of **TELNET** is that it's not secure. Everything you type, including passwords, is sent as plain text, meaning anyone with access to the network can read it. This is why **TELNET** has largely been replaced by more secure protocols like **SSH (Secure Shell)**, which encrypts your connection.

In summary, **TELNET** was a useful tool for remote computer management, but because it lacks encryption, it has been replaced by more secure alternatives for most modern applications.



## Application Layer Protocol

The **Application Layer** is the top layer in the OSI model and the **Internet Protocol Suite (TCP/IP)**. This layer provides a way for applications (like web browsers, email clients, and file-sharing programs) to communicate over a network. It's responsible for **interfacing directly with the end-user applications**, making sure that the data needed by these applications is transmitted correctly.

Unlike the lower layers that deal with raw data transmission, the Application Layer focuses on providing **specific services** that people use every day, such as sending emails, transferring files, or browsing websites. The protocols in this layer ensure that different applications on various devices can communicate smoothly over the network.

## Examples of Application Layer Protocols

There are many protocols in the Application Layer, each with a specific role, such as:

1. **HTTP (Hypertext Transfer Protocol)**: Used by web browsers to load web pages from servers. It allows users to communicate with websites and access their content.
2. **SMTP (Simple Mail Transfer Protocol)**: Used for sending emails from one server to another. SMTP ensures that emails can be delivered from a sender's email server to the recipient's server.
3. **DNS (Domain Name System)**: Converts human-readable domain names (like [www.example.com](http://www.example.com)) into IP addresses that computers use to identify each other on the network.
4. **FTP (File Transfer Protocol)**: Used for transferring files between computers over the internet. FTP allows users to upload or download files to and from servers.

---


## Why the Application Layer Is Important

The Application Layer ensures that **applications and services** that users interact with daily, such as emails, websites, and file-sharing systems, function properly. It makes network communication easy by allowing users to send messages, share files, and browse the internet without needing to know how the network operates beneath the surface.

For instance, when you type a URL in your browser, the Application Layer protocols handle the request, contact the server, and retrieve the website data for you. It's what makes the **internet user-friendly** and accessible.

---

## How Application Layer Protocols Work

When you perform tasks like sending an email  loading a webpage, the Application Layer protocols

## How Application Layer Protocols Work

When you perform tasks like sending an email or loading a webpage, the Application Layer protocols spring into action. They **package the data** (like a webpage or an email) into a format that can be understood by the receiver. The data is then passed down through the lower layers of the network, where it is transmitted over the internet.

For example, if you're sending an email, the SMTP protocol will ensure that the email is properly sent from your server to the recipient's server. When browsing a website, HTTP ensures that your browser can fetch and display the website's content.

---

## Real-World Use of Application Layer Protocols

1. **Web Browsing (HTTP/HTTPS):** Every time you visit a website, your browser uses HTTP or HTTPS (the secure version) to communicate with the server and load the web pages.
2. **Email (SMTP/IMAP/POP3):** When you send an email, SMTP is used to send the message, while POP3 or IMAP is used to retrieve emails from the server and display them in your inbox.
3. **File Transfer (FTP/SFTP):** Developers and users often use FTP to upload files to a server (e.g., when building websites) or download files from a remote server.

The **Application Layer** protocols make sure that communication between different software applications on various devices is seamless, allowing us to use the internet in the way we are familiar with today.



## SMTP (Simple Mail Transfer Protocol)

**SMTP** is the protocol used to send emails over the Internet. It acts like the "mailman" for email services, making sure your messages are delivered from your computer (or email client) to the recipient's email server. SMTP only handles sending emails, not receiving them.

When you hit "send" in your email application (like Gmail or Outlook), SMTP takes over. It checks the destination address and sends your email to the recipient's mail server. From there, another protocol (like POP or IMAP) is used to retrieve the email from the server when the recipient opens their inbox.

SMTP works by transferring your email through different mail servers until it reaches the recipient. It's designed for text-based messages but can handle attachments (like images or files) by encoding them. However, SMTP is a "push" protocol, meaning it only pushes emails to the server but doesn't fetch or retrieve them.

In summary, **SMTP** is essential for sending emails, ensuring that messages get from one email server to another, but it doesn't handle the retrieval of emails, which is where protocols like POP and IMAP come in.

---

## DNS (Domain Name System)

**DNS** is like the phonebook of the internet. It translates human-readable domain names (like "[www.google.com](https://www.google.com)") into numerical IP addresses that computers use to identify each other on the network. Without DNS, you would have to type in long strings of numbers (like 192.168.0.1) instead of easy-to-remember names to visit websites.

When you type a domain name into your browser, DNS steps in and finds the corresponding IP address of the server where the website is hosted. For example, when you type "google.com," DNS resolves this name to the correct IP address so that your browser can load the website.

DNS works behind the scenes and is crucial to the functioning of the web. It uses a hierarchical system of servers to manage this massive "phonebook." If one DNS server doesn't know the IP address of a domain, it can ask another until it finds the correct one.

In short, **DNS** makes the internet user-friendly by allowing us to use simple domain names instead of confusing IP addresses, enabling faster and easier access to websites.

---

## POP (Post Office Protocol)

POP is a protocol used to receive emails from a mail server. Specifically, POP3 (the most recent version) downloads the emails from the server to your device and usually deletes them from the server once they are downloaded. This means that your emails are stored locally on your computer or phone after being retrieved.

For example, if you're using an email client like Outlook or Thunderbird, when you connect to the internet, POP3 will download your new emails and store them on your device. Once the emails are downloaded, you can read, delete, or manage them even when you're offline because they are stored locally.

However, one limitation of POP is that it doesn't sync emails across multiple devices. If you check your emails on one device, the messages may no longer be available on another device since they were downloaded and possibly deleted from the server.

In summary, POP is great for people who prefer to store their emails locally on their devices, but it can be less useful if you want to access your email on multiple devices, which is why protocols like IMAP are often preferred for syncing across devices.



## Concept of IP Address

An **IP address (Internet Protocol address)** is a unique identifier assigned to every device connected to a computer network that uses the Internet Protocol for communication. Think of an IP address as a **digital home address** for your device on the internet. Just like your home address lets mail be delivered to you, an IP address allows data to find its way to your device.

An IP address ensures that devices like computers, smartphones, and servers can communicate with each other over the internet. Without IP addresses, devices wouldn't know where to send or receive information.

---

## Why IP Addresses Are Important

The internet is a massive network of devices, and each device needs a way to be identified so it can send and receive data. IP addresses solve this problem by providing a **unique identity** for every device. For instance, when you visit a website, your computer sends a request to the web server using the IP address of the server. The server, in turn, responds to your computer's IP address, delivering the requested webpage.

Without IP addresses, there would be no way to identify and communicate with other devices on the network, making internet use impossible.

## Types of IP Addresses

There are two types of IP addresses: IPv4 and IPv6.

### 1. IPv4:

- The most common type, which consists of four numbers separated by dots (like 192.168.1.1).
- IPv4 can provide around 4.3 billion unique addresses, but due to the rapid growth of the internet, these addresses are running out.

### 2. IPv6:

- Created to replace IPv4, it uses a much larger address space, allowing for a virtually unlimited number of unique IP addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- IPv6 was introduced because the world needed more IP addresses than IPv4 could provide.

Both IPv4 and IPv6 perform the same task: identifying devices and allowing them to communicate on the internet.

---

## How IP Addresses Work

When you connect to the internet, your Internet Service Provider (ISP) assigns your device an IP address. This address may be **static** (never changing) or **dynamic** (changing each time you connect). Here's how IP addresses work in practice:

1. **Sending Data:** When you type a website's address (like [www.google.com](http://www.google.com)), your browser doesn't actually understand the domain name. It first consults the **DNS (Domain Name System)** to find the IP address of that website. Then, it sends a request to that IP address asking for the webpage.
2. **Receiving Data:** The server hosting the website receives the request and sends the webpage data back to your device's IP address. This way, the correct data finds its way back to your computer.

In this way, an IP address acts like a postal address, ensuring that the information gets delivered to the right place.

HTTP	HTTPS
<ul style="list-style-type: none"> <li>• HTTP stands for 'HyperText Transfer Protocol'.</li> </ul>	<ul style="list-style-type: none"> <li>• HTTPS stands for 'HyperText Transfer Protocol Secure'.</li> </ul>
<ul style="list-style-type: none"> <li>• HTTP works at the application layer.</li> </ul>	<ul style="list-style-type: none"> <li>• HTTPS works at the transport layer.</li> </ul>
<ul style="list-style-type: none"> <li>• The default port number is 80, for communication.</li> </ul>	<ul style="list-style-type: none"> <li>• Here, the default port number is 443.</li> </ul>
<ul style="list-style-type: none"> <li>• No encryption is present in HTTP websites.</li> </ul>	<ul style="list-style-type: none"> <li>• Both encryption and decryption exist on HTTPS websites.</li> </ul>

## ❑ difference between HTTP and HTTPs

S.NO	HTTP	HTTPs
1.	It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
2.	It is not secure & unreliable.	It is secure & reliable.
3.	HTTP URLs begin with <a href="#">http://</a> .	HTTPs URLs begin with <a href="#">https://</a> .
4.	It uses port 80 by default .	It was use port 443 by default.
5.	It is subject to man-in-the-middle & eavesdropping attacks.	It is designed to withstand such attacks & is considered secure against such attacks.
<b>GENIUS</b>		





## MANET (Mobile Ad-hoc Network)

A **Mobile Ad-hoc Network (MANET)** is a type of wireless network where devices (like smartphones, laptops, or sensors) communicate directly with each other without relying on any fixed infrastructure like routers or base stations. The devices in this network are mobile and can move freely, which makes MANETs highly flexible.

In a MANET, each device acts both as a **node** (device) and a **router**. This means that not only do the devices send and receive data for themselves, but they also help forward data to other devices in the network. This creates a **self-configuring** and **dynamic network**, where the communication between devices is maintained even when the devices are moving.

---

## Why MANET is Important

MANETs are important because they allow devices to create a network without any pre-existing infrastructure. This makes them useful in situations where traditional networks are unavailable or not practical, such as:

1. **Disaster recovery:** During natural disasters (like earthquakes or floods), communication networks might be down. MANETs can be quickly deployed to allow rescue teams to communicate and share information.
  2. **Military operations:** Soldiers on the battlefield can use MANETs to create an instant communication network, even in remote or hostile areas where there is no other network available.
  3. **Remote areas:** In regions where it's difficult to set up traditional network infrastructure, MANETs can provide a way to create communication links.
- 

## How MANET Works

In a MANET, devices communicate using **radio signals** (like Wi-Fi or Bluetooth) instead of cables or fixed access points. Here's how it works:

1. **No central control:** There is no central device (like a router) managing the network. Instead, each device communicates directly with nearby devices. If a device wants to communicate with another device that is out of range, it sends the data through intermediate devices, which act as routers.
2. **Dynamic routing:** Because the devices are mobile, the network constantly changes as devices move in and out of range. The devices must constantly update their routing information to ensure that the data finds the correct path through the network. This process is called **dynamic routing**.

## How MANET Works

In a MANET, devices communicate using **radio signals** (like Wi-Fi or Bluetooth) instead of cables or fixed access points. Here's how it works:

1. **No central control:** There is no central device (like a router) managing the network. Instead, each device communicates directly with nearby devices. If a device wants to communicate with another device that is out of range, it sends the data through intermediate devices, which act as routers.
  2. **Dynamic routing:** Because the devices are mobile, the network constantly changes as devices move in and out of range. The devices must constantly update their routing information to ensure that the data finds the correct path through the network. This process is called **dynamic routing**.
  3. **Self-healing:** If one device moves out of range or fails, the network can automatically reconfigure itself and find a new route for the data. This makes MANETs very robust and adaptable.
- 

## Challenges in MANET

While MANETs offer flexibility and mobility, they also come with challenges:

1. **Security risks:** Since the devices communicate directly with each other, it can be easier for attackers to intercept data or inject malicious traffic.
2. **Power consumption:** Devices in MANETs need to work harder because they are constantly transmitting and forwarding data. This can drain battery power quickly, which is a concern for mobile devices.
3. **Unstable connections:** Since devices in a MANET are constantly moving, the network can become unstable, with frequent disconnections and reconnections.



## VANET (Vehicular Ad-hoc Network)

VANET is a type of wireless network where **vehicles communicate with each other** and with roadside infrastructure to share information in real-time. This technology is designed to improve road safety, traffic management, and provide better driving experiences.

- **How it works:** In a VANET, each vehicle acts like a node in a network. Vehicles exchange data about road conditions, traffic jams, accidents, or weather conditions. They also communicate with infrastructure like traffic lights and road signs to get updates on speed limits, road closures, and more. This network is formed dynamically as vehicles move.
  - **Example:** Imagine you're driving on the highway, and there's an accident ahead. With VANET, your car could receive a warning message from other vehicles in the area, allowing you to slow down or take a different route.
  - **Purpose:** The main goal of VANET is to **improve road safety** by sharing real-time information between vehicles. It also helps reduce traffic congestion and makes driving more efficient by providing better navigation and traffic management.
- 

## SPAN (Smart Phone Ad-hoc Network)

SPAN stands for **Smartphone Ad-hoc Network**. In this type of network, **smartphones communicate directly with each other** without the need for mobile towers, Wi-Fi, or other fixed infrastructure.

- **How it works:** In SPAN, smartphones connect using Bluetooth or Wi-Fi Direct. Each smartphone in the network acts as a node that can send and receive data, and smartphones can forward data to each other, forming a **peer-to-peer network**.
  - **Example:** Imagine you're at a large music festival in a remote area with no mobile signal. With SPAN, people can still communicate by sending messages from one phone to another through the ad-hoc network, even without internet or cellular service.
  - **Purpose:** SPAN is useful in situations where **traditional networks are unavailable** or overloaded. It can be used in disaster zones, remote areas, or large events where mobile networks may fail. It allows people to stay connected even without regular internet access.
- 

## FANET (Flying Ad-hoc Network)

FANET refers to a network of drones or **UAVs (Unmanned Aerial Vehicles)** that communicate with each other. These drones are used for various tasks such as surveillance, search and rescue operations, and delivering goods.



- **How it works:** FANETs are formed when multiple drones communicate wirelessly to complete a

## FANET (Flying Ad-hoc Network)

FANET refers to a network of **drones** or **UAVs (Unmanned Aerial Vehicles)** that communicate with each other. These drones are used for various tasks such as surveillance, search and rescue operations, and delivering goods.

- **How it works:** FANETs are formed when multiple drones communicate wirelessly to complete a specific task. Each drone acts as a node in the network, sharing information like location, flight path, and mission details with other drones. This allows them to work together without the need for a central controller.
- **Example:** During a forest fire, drones equipped with cameras and sensors can create a FANET to monitor the fire's spread and relay real-time information to firefighters. The drones communicate with each other to cover a large area efficiently.
- **Purpose:** The primary purpose of FANET is to **enhance collaboration** between drones in tasks like **aerial surveillance, disaster management, and delivery services**. FANETs can operate in areas where traditional communication systems don't exist or are difficult to establish.



## Concepts of Email

Email, short for **Electronic Mail**, is a method of sending digital messages over the internet. It allows users to exchange messages with text, attachments, images, and links. Email has become an essential communication tool for personal, professional, and educational purposes.

- **How it works:** Email uses servers to **send, store, and deliver messages**. A sender writes an email, which is sent to the recipient's email server. The recipient's email client (such as Gmail, Outlook) retrieves the message from the server so it can be read.
- **Example:** When you send an email to your friend, the message is transferred through a series of mail servers until it reaches your friend's email account, where they can access it on their device.
- **Purpose:** Email provides **fast, reliable, and easy** communication across the world, allowing people to send messages, share documents, and collaborate in real-time.

---

## Working of Email Accounts and Services

To use email, you need an **email account**, which is typically provided by email services like Gmail, Yahoo Mail, or Outlook. Each account has a unique email address that identifies the user (e.g., [username@example.com](mailto:username@example.com)). Email services use several protocols to manage email transmission and retrieval:

- **SMTP (Simple Mail Transfer Protocol):** This protocol is used to **send emails** from your device to the recipient's mail server.
- **IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol):** These are used to **receive emails**. IMAP stores emails on the server, so they can be accessed from multiple devices, while POP3 downloads the emails to your device and usually removes them from the server.

**How it works step-by-step:**

1. **Composing:** You write the email and press "Send".
  2. **Sending:** The email goes to your email server using SMTP.
  3. **Delivery:** The email server finds the recipient's mail server and delivers the email.
  4. **Receiving:** The recipient retrieves the email using either IMAP or POP3.
- **Example:** When you send an email from your Gmail account to someone's Yahoo account, Gmail uses SMTP to send the message, and the Yahoo mail server receives it, storing it until the recipient reads it.

## URL (Uniform Resource Locator)

A URL is the address of a web page or resource on the internet. It's what you type into your browser's address bar to visit a website. URLs tell the browser where to find a specific page or file online.

- **Components of a URL:**
    - **Protocol:** (e.g., `http`, `https`) specifies how data is transferred.
    - **Domain name:** The website's address (e.g., `www.example.com`).
    - **Path:** Specifies a particular page or file on the website (e.g., `/about-us`).
    - **Query:** Optional parameters that can be passed to the web page (e.g., `?id=123`).
  - **Example:** In the URL "`https://www.example.com/about`", `https` is the protocol, `www.example.com` is the domain, and `/about` is the path leading to the "About" page.
- 

## URL Types: Absolute and Relative

**1. Absolute URL** An Absolute URL gives the complete address of a webpage, including the protocol (`http/https`), domain name, and the path to the page or resource. It is used to specify the location of a resource from any point on the internet.

- **Example:** "`https://www.example.com/products/shoes`" is an absolute URL that includes the entire path to the resource.
- **Purpose:** Absolute URLs are necessary when you need to access a resource or webpage from any location on the web.

**2. Relative URL** A Relative URL gives the path to a resource in relation to the current page or directory. It does not include the protocol or domain name. Relative URLs are often used within the same website.

- **Example:** "`/contact`" is a relative URL that directs to the contact page from the current website.
- **Purpose:** Relative URLs are shorter and easier to manage, making them ideal for internal website links where the domain remains the same.

## Case Study of Email: From Sender to Receiver

In this case study, we'll look at how an email travels from the sender to the receiver, involving various components such as the **Mailer (email client)**, **Mail Server**, and **Mailbox**, and how different protocols work together to ensure smooth delivery.

### 1. Sending an Email: Mailer (Email Client)

The journey begins when you (the sender) compose an email using a **Mailer**, also known as an **email client** (e.g., Gmail, Outlook, Thunderbird).

- **Step 1: Writing the email:** You write the email, add the recipient's email address, and click "Send".
  - **Step 2: SMTP kicks in:** When you hit send, the **SMTP (Simple Mail Transfer Protocol)** on your device sends the email to your **outgoing mail server**. SMTP ensures the message gets delivered to the correct mail server.
  - **Example:** If you're using Gmail to send an email to someone on Yahoo, your Gmail client uses SMTP to transfer your message to Gmail's outgoing mail server.
- 

### 2. Delivering the Email: Mail Servers

Once the email leaves your device, it travels through the internet to reach the **Mail Server**. Mail servers handle the routing and storage of emails until they reach their destination.

- **Step 3: SMTP (Continued):** The SMTP server at your mail provider (like Gmail) contacts the recipient's SMTP server (like Yahoo's mail server). The message is transferred over the internet.
  - **Step 4: Mail Queuing:** If the recipient's server is down or busy, the email is queued (saved temporarily) and tried again later.
  - **Step 5: DNS Lookup:** To deliver the email to the correct domain (e.g., yahoo.com), the sender's SMTP server performs a **DNS (Domain Name System)** lookup to find the recipient's mail server.
  - **Example:** Your Gmail SMTP server contacts Yahoo's SMTP server to deliver the email, which is then stored on Yahoo's mail server.
- 

### 3. Receiving the Email: Mailbox

After the email reaches the recipient's mail server, it needs to be stored in the **Mailbox**, where the receiver can access it using their email client.

- **Step 6: IMAP/POP3 Fetching:** The recipient's mail client uses either **IMAP (Internet Message Access Protocol)** or **POP3 (Post Office Protocol)** to download or access the message from the

### 3. Receiving the Email: Mailbox

After the email reaches the recipient's mail server, it needs to be stored in the Mailbox, where the receiver can access it using their email client.

- **Step 6: IMAP/POP3 Fetching:** The recipient's mail client uses either **IMAP** (Internet Message Access Protocol) or **POP3** (Post Office Protocol) to download or access the message from the server.
  - **IMAP:** If IMAP is used, the email stays on the server, and the recipient can access it from multiple devices (e.g., phone, laptop).
  - **POP3:** If POP3 is used, the email is downloaded to the device and often deleted from the server.
- **Step 7: Reading the Email:** The email is now in the recipient's inbox. The receiver can open and read the email on their device using their mailer (like Yahoo Mail or Outlook).
- **Example:** When the recipient opens their Yahoo Mail, the email is retrieved from Yahoo's mail server using IMAP or POP3.