

MCA 1ST SEM



**Dr. Ambedkar Memorial Institute of
Information Technology & Management Science**

LECTURE NOTES

ON

COMPUTER NETWORK

MCPC1002 MCA (1st Sem)

Prepared By

Prof. Alisha Nayak

MCA 1ST SEM

COMPUTER NETWORK

MODULE - 1

Overview of the Internet: introduction to data communication, network application, Network hardware, Protocol, Layering Scenario, **reference models**: The OSI Model, TCP/IP model, Internet history, standards and administration; Comparison of the OSI and TCP/IP reference model.

Physical Layer: data and signals: analog and digital, periodic analog signals, digital signals, transmission impairments, data rate limit, Guided transmission media, unguided transmission media, Wireless transmission, mobile telephone system.

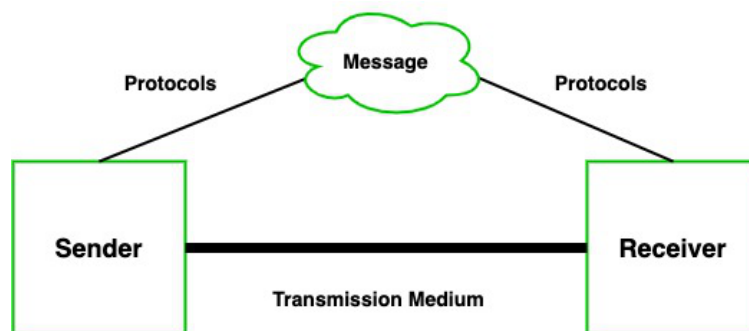
Introduction to Data Communication

- Data communication is the exchange of data between two devices (computer, phone, IoT device) through a transmission medium (wired or wireless).

A communication system is made up of the following components:

- Message**: A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
- Sender**: It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
- Receiver**: It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
- Transmission Medium / Communication Channels**: Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
- Set of rules (Protocol)**: When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless.

Real-life example: Sending a WhatsApp message → Your phone (sender) encodes data → Wi-Fi/mobile network (medium) → WhatsApp server → friend's phone (receiver).



Type of data communication :

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

- Simplex Communication**: It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices use their entire capacity in transmission. For example, IoT, entering data using a keyboard, listening music using a speaker, etc.
- Half Duplex communication**: It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.

MCA 1ST SEM

3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

Network Applications :

Network Applications are **software programs or services** that use a **computer network (like the Internet or LAN)** to enable **communication, resource sharing, or online services** between devices and users. They rely on **network protocols** (such as HTTP, SMTP, FTP, TCP/IP) to work properly.

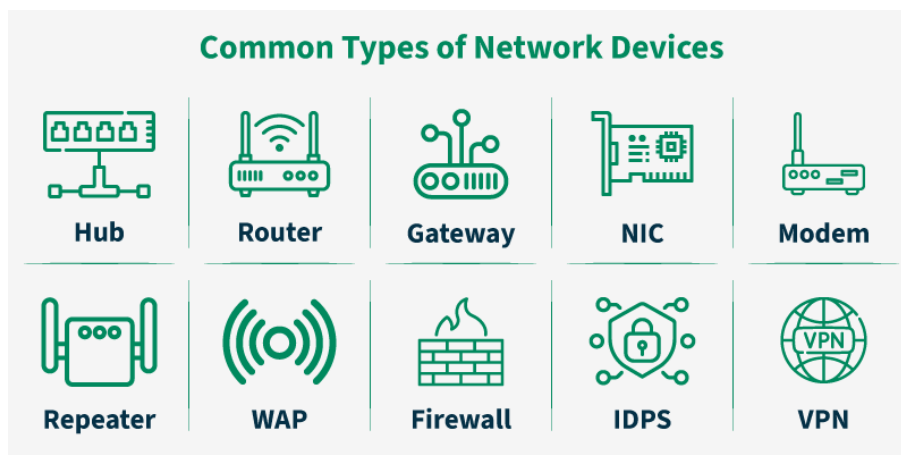
Without network applications, the Internet would just be a physical connection with no useful services.

Examples of Network Applications

1. **Email (Gmail, Outlook)** → send & receive electronic messages.
2. **Web Browsing (Google Chrome, Safari)** → access websites using HTTP/HTTPS.
3. **File Transfer (FTP, Google Drive, WeTransfer)** → share documents & files.
4. **Instant Messaging (WhatsApp, Telegram, Messenger)** → real-time chatting.
5. **Video Conferencing (Zoom, Google Meet)** → online meetings & classes.
6. **E-Commerce (Amazon, Flipkart)** → online shopping.
7. **Online Gaming (PUBG, Free Fire, Fortnite)** → multiplayer gaming.
8. **Social Networking (Facebook, Instagram, Twitter/X)** → connect & share with people.
9. **Cloud Services (Google Drive, Dropbox, AWS)** → store & access data online.

Network Hardware :

Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other. Network devices like hubs, repeaters, bridges, switches, routers, gateways, and brouter help manage and direct data flow in a network. They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks. Each device serves a specific role, from simple data forwarding to complex routing between networks.



Access Point

An [access point](#) in networking is a device that allows wireless devices, like smartphones and laptops, to connect to a wired network. It creates a Wi-Fi network that lets wireless devices communicate with the internet or other devices on the network. Access points are used to extend the range of a network or provide Wi-Fi in

MCA 1ST SEM

areas that do not have it. They are commonly found in homes, offices, and public places to provide wireless internet access.

Modems

Modem is also known as modulator/demodulator is a network device that is used to convert digital signal into analog signals of different frequencies and transmits these signals to a modem at the receiving location. These converted signals can be transmitted over the cable systems, telephone lines, and other communication mediums. A modem is also used to convert an analog signal back into digital signal. Modems are generally used to access the internet by customers of an Internet Service Provider (ISP).

Types of Modems

There are four main types of modems:

- **DSL Modem:** Uses regular phone lines to connect to the internet but it is slower compared to other types.
- **Cable Modem:** Sends data through TV cables, providing faster internet than DSL.
- **Wireless Modem:** Connects devices to the internet using Wi-Fi relying on nearby Wi-Fi signals.
- **Cellular Modem:** Connects to the internet using mobile data from a cellular network not Wi-Fi or fixed cables.

Firewalls

A firewall is a network security device that monitors and controls the flow of data between your computer or network and the internet. It acts as a barrier, blocking unauthorized access while allowing trusted data to pass through. Firewalls help protect your network from hackers, viruses, and other online threats by filtering traffic based on security rules. Firewalls can be physical devices (hardware), programs (software), or even cloud-based services, which can be offered as SaaS, through public clouds, or private virtual clouds.

Repeater

A repeater operates at the physical layer. Its main function is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Hub

A hub is a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. A bridge is not strictly limited to two ports, it can have multiple ports to connect and manage multiple network segments. Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Switch

A switch is a multiport bridge with a buffer designed that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

MCA 1ST SEM

Gateway

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

Router

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as a bridge, it is capable of filtering local area network traffic.

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Protocols :

A **protocol** is a set of **rules and standards** that define how data is transmitted, received, and interpreted over a network. It ensures proper communication between devices, regardless of their hardware or software differences.

Example: When you open a website, **HTTP protocol** defines how your browser communicates with the web server.

Important Network Protocols (with examples)

1. **HTTP/HTTPS (HyperText Transfer Protocol / Secure)**
 - Used for web browsing.
 - HTTPS adds encryption (secure communication).
 - *Example:* Opening Google.com.
2. **FTP (File Transfer Protocol)**
 - Used to transfer files between client and server.
 - *Example:* Uploading files to a website.
3. **SMTP (Simple Mail Transfer Protocol)**
 - Used for sending emails.
 - *Example:* Sending an email via Gmail.
4. **POP3 / IMAP (Post Office Protocol / Internet Message Access Protocol)**
 - Used for receiving emails.
 - *Example:* Outlook using IMAP to fetch emails.
5. **TCP (Transmission Control Protocol)**
 - Provides reliable, connection-oriented communication.
 - *Example:* File download where accuracy is needed.
6. **UDP (User Datagram Protocol)**
 - Fast, connectionless communication (less reliable).
 - *Example:* Online gaming, video calls.
7. **IP (Internet Protocol)**
 - Responsible for addressing and routing data packets.
 - *Example:* Every device has an IP address (192.168.1.1).
8. **DNS (Domain Name System)**
 - Converts domain names into IP addresses.
 - *Example:* Converting www.youtube.com → IP address.
9. **DHCP (Dynamic Host Configuration Protocol)**

MCA 1ST SEM

- Automatically assigns IP addresses to devices.
- *Example:* When your phone connects to Wi-Fi, it gets an IP from DHCP.

10. HTTPS + SSL/TLS

- Encrypts communication for secure transactions.
- *Example:* Online banking, shopping.

Layering Scenario :

• In networking, **layering** means dividing the communication process into multiple layers, where each layer has a **specific role**. Each layer **only communicates with the layer directly above or below it**.

- **Advantages:** modularity, troubleshooting, standardization.
- *Example:* Sending an email → Application layer (email app) → Transport (TCP ensures reliable delivery) → Network (IP addresses) → Data link (Ethernet/Wi-Fi) → Physical (electric/optical signals).

Real-life Example of Layering

Sending a WhatsApp Message

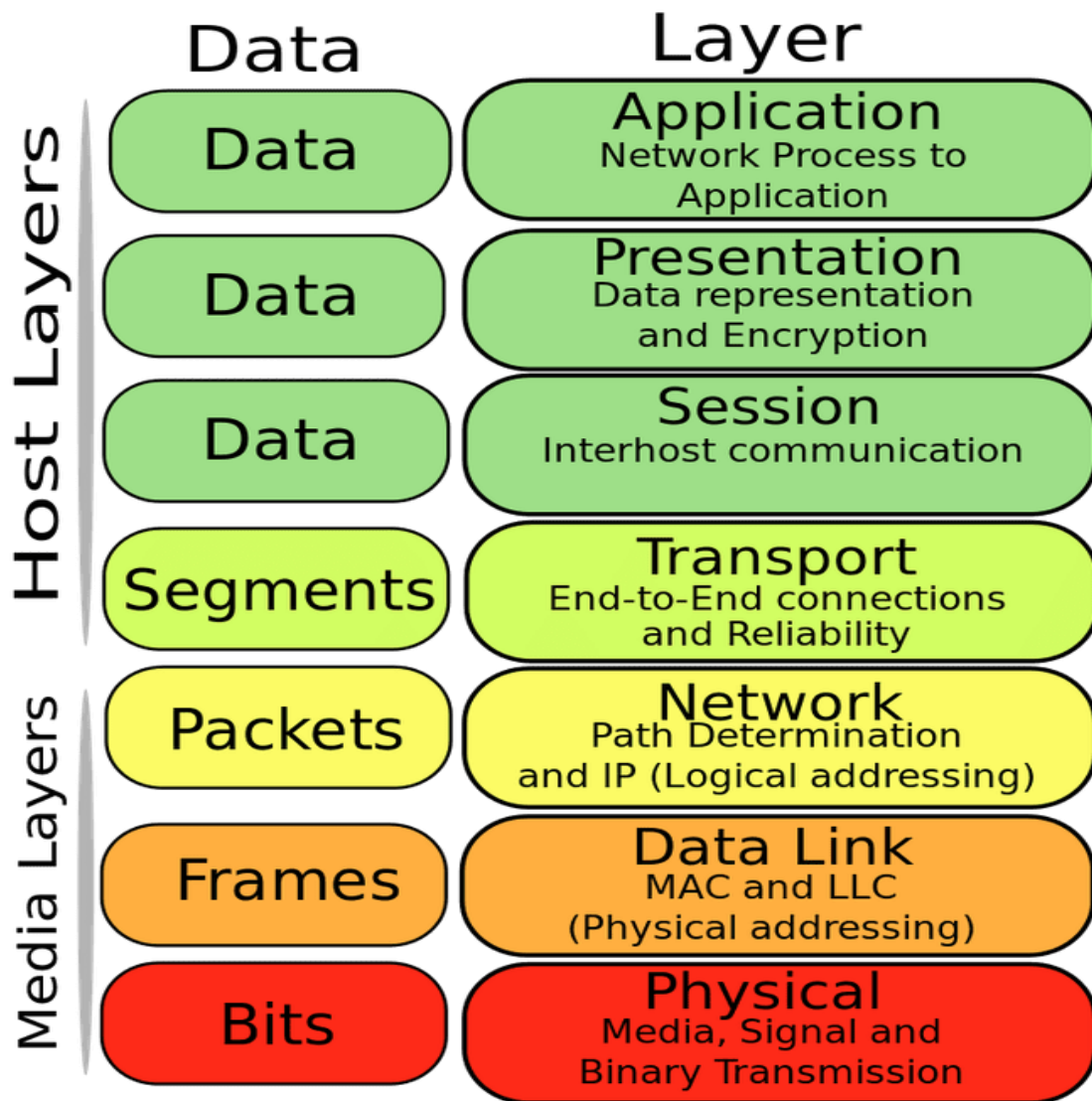
1. **Application layer:** You type "Hi" in WhatsApp.
2. **Transport layer (TCP/UDP):** Breaks message into small packets.
3. **Network layer (IP):** Adds sender & receiver IP addresses.
4. **Data Link layer (Wi-Fi/4G/5G):** Adds MAC addresses for local delivery.
5. **Physical layer:** Converts data into Wi-Fi or mobile signals → sends.

On the receiver's phone → the reverse process happens → "Hi" appears in chat.

The OSI Model :

The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the International Organization for Standardization (ISO). The OSI Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together.

OSI Model



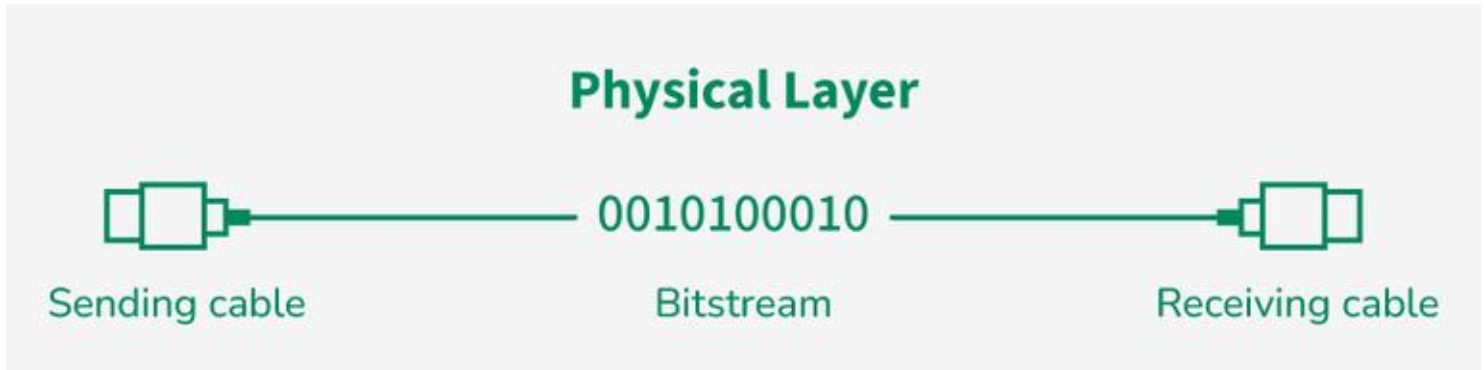
Layer 1: Physical Layer

The lowest layer of the OSI reference model is the Physical Layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits.

- Physical Layer is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
- Common physical layer devices are Hub, Repeater, Modem, and Cables.
- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

MCA 1ST SEM

- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. [bus topology](#), [star topology](#), or [mesh topology](#).
- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are [Simplex](#), [half-duplex](#) and [full duplex](#).



Layer 2: Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its [MAC address](#).
- Packet in the Data Link layer is referred to as Frame. [Switches and Bridges](#) are common Data Link Layer devices.
- The packet received from the Network layer is further divided into frames depending on the frame size of the NIC ([Network Interface Card](#)). DLL also encapsulates Sender and Receiver's MAC address in the header.
- The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

Layer 3: Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

- The sender and receiver's [IP address](#) are placed in the header by the network layer. Segment in the Network layer is referred to as Packet.
- Network layer is implemented by networking devices such as [routers and switches](#).
- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4: Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the end-to-end delivery of the complete message.

- The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
- Protocols used in Transport Layer are [TCP](#), [UDP](#), [NetBIOS](#), [PPTP](#).
- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Layer 5: Session Layer

- Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.
- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.

Layer 6: Presentation Layer

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are [TLS/SSL](#) (Transport Layer Security / Secure Sockets Layer). [JPEG](#), [MPEG](#), [GIF](#), are standards or formats used for encoding data, which is part of the presentation layer's role.

- For example, [ASCII to EBCDIC](#).
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- Reduces the number of bits that need to be transmitted on the network.

Layer 7: Application Layer

MCA 1ST SEM

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network.

- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- Protocols used in the Application layer are [SMTP](#), [FTP](#), [DNS](#), etc.

How Data Flows in the OSI Model?

Let us suppose, Person A sends an e-mail to his friend Person B.

- **Step 1: Person A** interacts with e-mail application like Gmail, outlook, etc. Writes his email to send. (This happens at Application Layer).
- **Step 2: At Presentation Layer**, Mail application prepares for data transmission like encrypting data and formatting it for transmission.
- **Step 3: At Session Layer**, there is a connection established between the sender and receiver on the internet.
- **Step 4: At Transport Layer**, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.
- **Step 5: At Network Layer**, addressing of packets is done in order to find the best route for transfer.
- **Step 6: At Data Link Layer**, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.
- **Step 7: At Physical Layer**, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

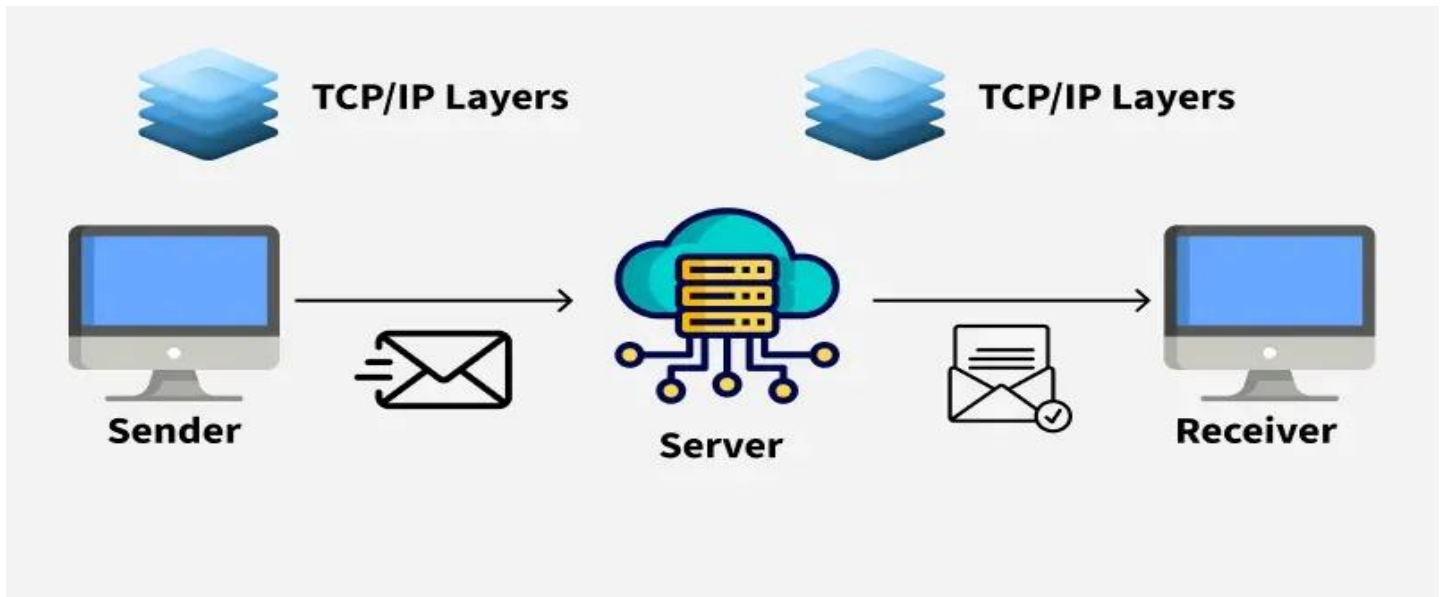
After the email reaches the receiver i.e. Person B, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Person B email client.

TCP/IP Model

TCP/IP Model stands for **Transmission Control Protocol / Internet Protocol Model**.

The TCP/IP model is a framework that is used to model the communication in a network. It is mainly a collection of network protocols and organization of these protocols in different layers for modeling the network.

- It has four layers, Application, Transport, Network/Internet and Network Access.
- While the [OSI model](#) has seven layers, the 4 layer TCP/IP model is simpler and commonly used in today's Internet and networking systems.



1. Application Layer

The Application Layer is the top layer of the TCP/IP model and the one closest to the user. This is where all the apps you use like web browsers, email clients, or file sharing tools connect to the network.

- It acts like a bridge between your software (like Chrome, Gmail, or WhatsApp) and the lower layers of the network that actually send and receive data.
- It supports different protocols like HTTP (for websites), FTP (for file transfers), SMTP (for emails), and DNS (for finding website addresses).
- It also manages things like data formatting, so both sender and receiver understand the data, encryption to keep data safe, and session management to keep track of ongoing connections.

2. Transport Layer

The Transport Layer is responsible for making sure that data is sent reliably and in the correct order between devices. It checks that the data you send like a message, file, or video arrives safely and completely.

- **This layer uses two main protocols:** TCP and UDP, depending on whether the communication needs to be reliable or faster.
- TCP is used when data must be correct and complete, like when loading a web page or downloading a file.
- It checks for errors, resends missing pieces, and keeps everything in order. On the other hand, UDP (User Datagram Protocol) is faster but doesn't guarantee delivery useful for things like live video or online games where speed matters more than perfect accuracy.

3. Internet Layer

The Internet Layer is used for finding the best path for data to travel across different networks so it can reach the right destination. It works like a traffic controller, helping data packets move from one network to another until they reach the correct device.

- This layer uses the Internet Protocol (IP) to give every device a unique IP address, which helps identify where data should go.
- The main job of this layer is routing deciding the best way for data to travel.

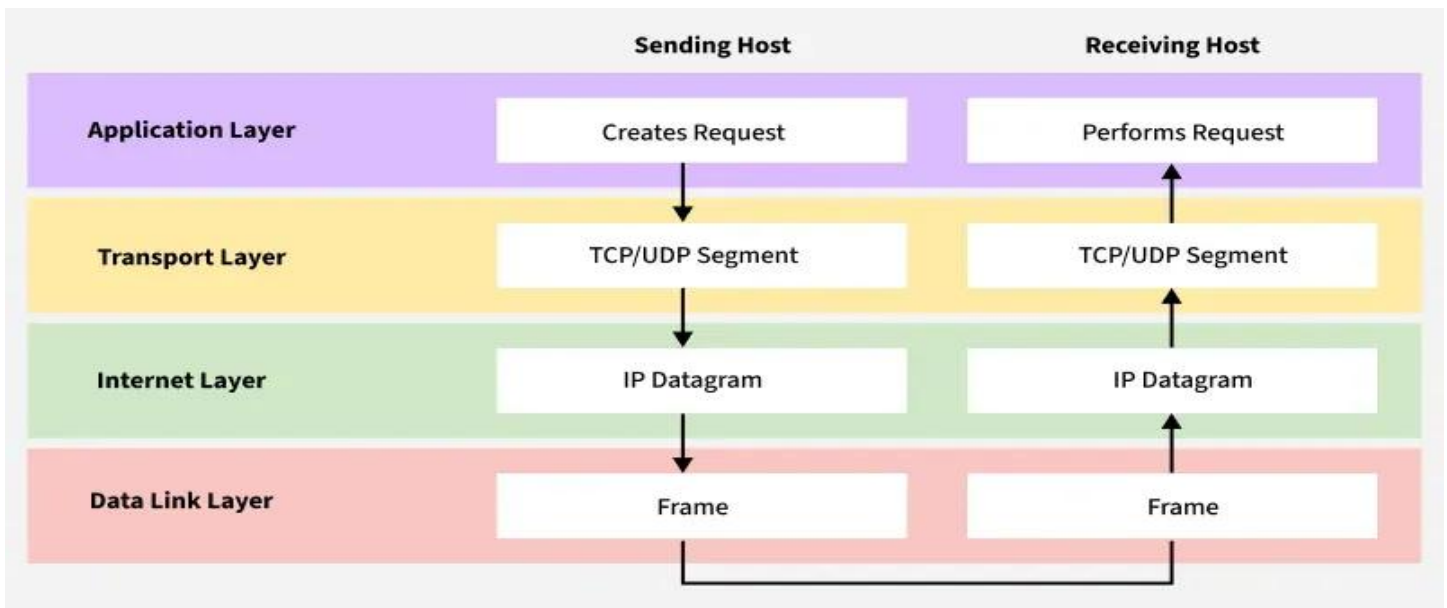
MCA 1ST SEM

- It also takes care of packet forwarding (moving data from one point to another), fragmentation (breaking large data into smaller parts), and addressing.

4. Network Access Layer

The Network Access Layer is the bottom layer of the TCP/IP model. It deals with the actual physical connection between devices on the same local network like computers connected by cables or communicating through Wi-Fi.

- This layer makes sure that data can travel over the hardware, such as wires, switches, or wireless signals.
- It also handles important tasks like using MAC addresses to identify devices, creating frames (the format used to send data over the physical link), and checking for basic errors during transmission.



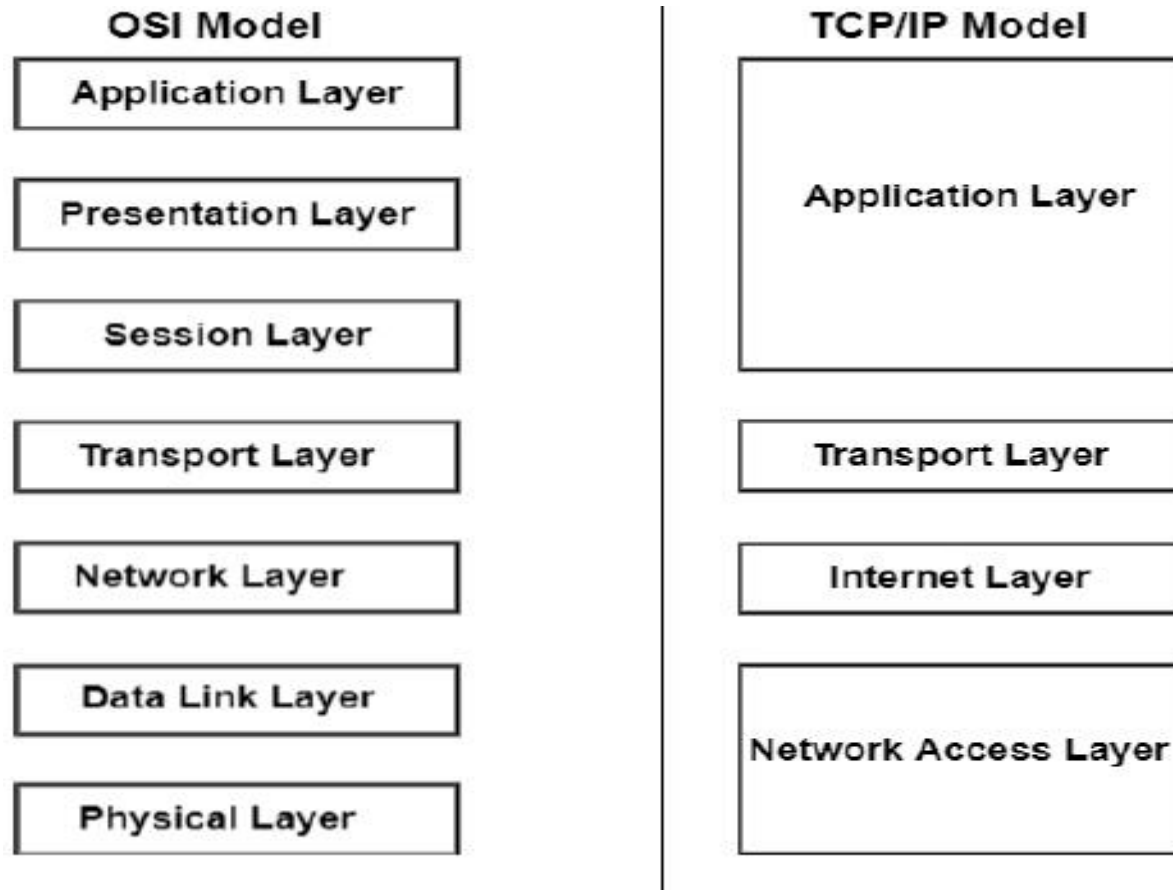
Following are the differences between OSI and TCP/IP Reference Model

OSI	TCP/IP
OSI represents Open System Interconnection .	<u>TCP/IP</u> model represents the Transmission Control Protocol / Internet Protocol.
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.
The OSI model was developed first, and	The protocols were created first and then

MCA 1ST SEM

OSI	TCP/IP
then protocols were created to fit the network architecture's needs.	built the TCP/IP model.
It provides quality services.	It does not provide quality services.
The OSI model represents defines administration, interfaces and conventions. It describes clearly which layer provides services.	It does not mention the services, interfaces, and protocols.
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly.	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer.	It provides connectionless transmission in the network layer and supports connecting and connectionless-oriented transmission in the transport layer.
It uses a vertical approach.	It uses a horizontal approach.
The smallest size of the OSI header is 5 bytes.	The smallest size of the <u>TCP/IP header</u> is 20 bytes.
Protocols are unknown in the OSI model and are returned while the technology modifies.	In TCP/IP, returning protocol is not difficult.

MCA 1ST SEM



History of the Internet

The Internet has evolved over decades, starting from a small research project to the vast global network we know today.

- **1960s: ARPANET (Advanced Research Projects Agency Network)**
 - The precursor to the modern Internet, ARPANET, was developed by the U.S. Department of Defense in the late 1960s.
 - The key innovation was packet switching, which allowed data to be broken into packets and sent across different routes, making the network more resilient and efficient.
 - ARPANET connected universities and research institutions, enabling them to share information.
- **1970s: TCP/IP and Expansion**
 - In 1973, Vinton Cerf and Bob Kahn developed the **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**, which became the foundation for the Internet's architecture.
 - The protocol allowed different networks to connect, creating the first global inter-network.
- **1980s: The Rise of the Internet and the Domain Name System (DNS)**
 - The Domain Name System (DNS) was introduced in 1983, allowing users to access websites using human-readable domain names (e.g., `www.example.com`) instead of numerical IP addresses.
 - The U.S. National Science Foundation (NSF) funded NSFNET, which connected universities and research centers and served as a backbone for the Internet.
- **1990s: The World Wide Web (WWW)**
 - In 1991, **Tim Berners-Lee** developed the World Wide Web, a system that used hypertext to enable users to access documents and resources via the Internet.
 - The first web browser, **Mosaic**, was developed in 1993, followed by **Netscape Navigator**, which popularized the Internet in the mid-1990s.
 - The 1990s saw a boom in websites, online services, and e-commerce.

MCA 1ST SEM

- **2000s and Beyond: Commercialization and Global Expansion**

- By the early 2000s, the Internet became widely commercialized, with search engines (e.g., Google), social media platforms (e.g., Facebook, Twitter), and e-commerce giants (e.g., Amazon, eBay) becoming dominant players.
 - The development of broadband connections and wireless technologies like Wi-Fi helped bring the Internet to more users worldwide.
-

Internet Standards

Internet standards are crucial to ensuring that the various technologies and protocols used to operate the Internet work together seamlessly.

- **IETF (Internet Engineering Task Force):**

- A global community of network designers and engineers that develops and promotes voluntary Internet standards.
- The IETF produces **Request for Comments (RFCs)**, which are documents that define standards, protocols, and practices used on the Internet. For example, **RFC 791** defines IPv4, while **RFC 2616** defines HTTP 1.1.

- **Key Protocols:**

- **IP (Internet Protocol):** The main protocol for routing and addressing packets of data across the Internet.
- **TCP (Transmission Control Protocol):** Ensures reliable data transmission by establishing connections and managing the flow of data.
- **UDP (User Datagram Protocol):** A faster, connectionless protocol used for real-time applications like video streaming and gaming.
- **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):** The protocol used for transferring web pages.
- **FTP (File Transfer Protocol):** A protocol for transferring files between computers over the Internet.
- **DNS (Domain Name System):** The system that translates domain names (like www.example.com) into IP addresses.

- **W3C (World Wide Web Consortium):**

- Responsible for developing web standards such as **HTML**, **CSS**, and **XML** to ensure consistency and interoperability of web content across different platforms and browsers.
-

Internet Administration

Internet administration involves managing and coordinating the technical and organizational aspects of the Internet.

- **ICANN (Internet Corporation for Assigned Names and Numbers):**

- ICANN is a non-profit organization responsible for overseeing domain name registrations, IP address allocation, and the overall functioning of the DNS system.
- It ensures that domain names are unique and resolve to the correct IP addresses.

- **IANA (Internet Assigned Numbers Authority):**

- A part of ICANN, IANA is responsible for coordinating IP address allocation, Autonomous System Number (ASN) assignment, and protocol parameter assignments.

MCA 1ST SEM

- It maintains a global registry of IP address space and assigns blocks to regional internet registries (RIRs).
 - **Regional Internet Registries (RIRs):**
 - There are five RIRs that allocate IP address space within specific geographic regions:
 - **ARIN (American Registry for Internet Numbers)** for North America.
 - **RIPE NCC (Réseaux IP Européens Network Coordination Centre)** for Europe, the Middle East, and parts of Central Asia.
 - **APNIC (Asia-Pacific Network Information Centre)** for Asia and the Pacific.
 - **LACNIC (Latin American and Caribbean Network Information Centre)** for Latin America and the Caribbean.
 - **AFRINIC (African Network Information Centre)** for Africa.
 - **Internet Service Providers (ISPs):**
 - ISPs are organizations that provide Internet access to users and businesses. They are often involved in domain name registration, email services, and the management of broadband networks.
 - **Internet Governance:**
 - Internet governance refers to the policies, regulations, and frameworks that guide the development and use of the Internet. It involves multiple stakeholders, including governments, private companies, civil society, and technical bodies.
 - Key issues include **net neutrality**, **privacy**, **cybersecurity**, and **accessibility**.
-

Important Terms in Internet Administration

- **IP Address:** A unique identifier for a device connected to the Internet (e.g., 192.168.1.1).
 - **DNS Server:** A server that translates domain names into IP addresses.
 - **Bandwidth:** The amount of data that can be transmitted over a network in a given period (usually measured in bits per second).
 - **Latency:** The time it takes for data to travel from the sender to the receiver.
 - **Firewall:** A security system that controls incoming and outgoing network traffic.
-

Evolution and Future Trends

- **IPv6 Adoption:** With IPv4 addresses running out, IPv6 (which uses a 128-bit address space) is gradually being adopted, offering a far larger pool of addresses.
- **5G and IoT:** The advent of 5G technology promises faster internet speeds, lower latency, and the ability to support the growing number of connected devices (Internet of Things).
- **Decentralized Internet:** Concepts like blockchain-based Internet and distributed web technologies aim to decentralize Internet services and give more control back to users.

Data and Signals

- **Data:** Information that needs to be transmitted. It can be in the form of **binary data (1s and 0s)** or **analog signals** depending on the medium of transmission.

MCA 1ST SEM

- **Signal:** A signal is the representation of data in a form that can be transmitted over the physical medium. Signals can be of two types:
 - **Analog Signals:** Continuous signals that vary smoothly over time (e.g., sound waves, light waves).
 - **Digital Signals:** Discrete signals that represent data as binary numbers (1s and 0s).

Difference Between Analog And Digital Signal

- The difference between analog signal and digital signal could be understood from the table given below:

Basis	Analog Signal	Digital Signal
Definition	Analog signals represent continuous variations in magnitude over time.	Digital signals are Discrete and quantized, with specific values.
Signal Type	Continuous waveforms	Discrete Signals
Processing	Requires complex processing for manipulation.	Easier to process and manipulate digitally.
Storage	Less efficient for storage due to continuous nature.	More efficient for storage due to discrete values.
Bandwidth	Typically requires more bandwidth.	Requires less bandwidth for transmission.
Examples	Analog audio signals, analog radio waves, Human voice, etc.	Digital audio signals, digital data streams, computers, etc.
Errors	Susceptible to noise and distortion	More resistant to noise and distortion
Circuit Component	Amplifiers, filters, continuous-wave oscillators	Microprocessors, binary counters, logic gates
Signal Values	Infinite range of values	Limited to discrete values
Conversion	No conversion required	Analog-to-digital conversion (ADC) required
Applications	Analog signals are used in electric fan, landlines, radio frequency communications, etc.	Digital signals are used in computers, smartphones, digital sensors, digital imaging, etc.

MCA 1ST SEM

- **Periodic Analog Signals:**

- A periodic signal repeats itself after a fixed period.
- Commonly represented as a **sine wave**.
- Can be characterized by:
 - **Amplitude:** The peak value of the signal.
 - **Frequency:** The number of cycles (or oscillations) per second (measured in Hertz, Hz).
 - **Phase:** The initial angle or shift of the wave.

Examples: Radio signals, electrical power transmission.

- **Digital Signals:**

- Discrete signals, where the data is represented by a series of voltage pulses corresponding to binary values.
- Each voltage level represents a distinct binary value (e.g., "high" for 1 and "low" for 0).
- These signals are less affected by noise and interference than analog signals, which makes them suitable for data communication over long distances.

Examples: Computer data, digital audio, and video signals.

Transmission Impairments

Transmission impairments refer to the degradation of the signal quality during transmission. There are several types of impairments:

- **Attenuation:** The loss of signal strength as it travels through a medium.
 - This is often caused by the resistance in the transmission medium (e.g., copper wires) or distance.
- **Noise:** Any unwanted electrical signals that interfere with the transmission of the signal.
 - Types of noise include thermal noise (due to heat), impulse noise (sudden spikes), and cross-talk (signals from adjacent channels).
- **Distortion:** The change in the waveform of the signal during transmission, leading to loss of fidelity in the original data.
 - This is caused by imperfections in the transmission medium.

Data Rate Limit

The data rate (or bandwidth) refers to the amount of data transmitted in a given amount of time (usually measured in bits per second, bps). The **Shannon-Hartley Theorem** defines the theoretical maximum data rate (C) of a communication channel:

$$C = B \cdot \log_2(1 + NS)$$

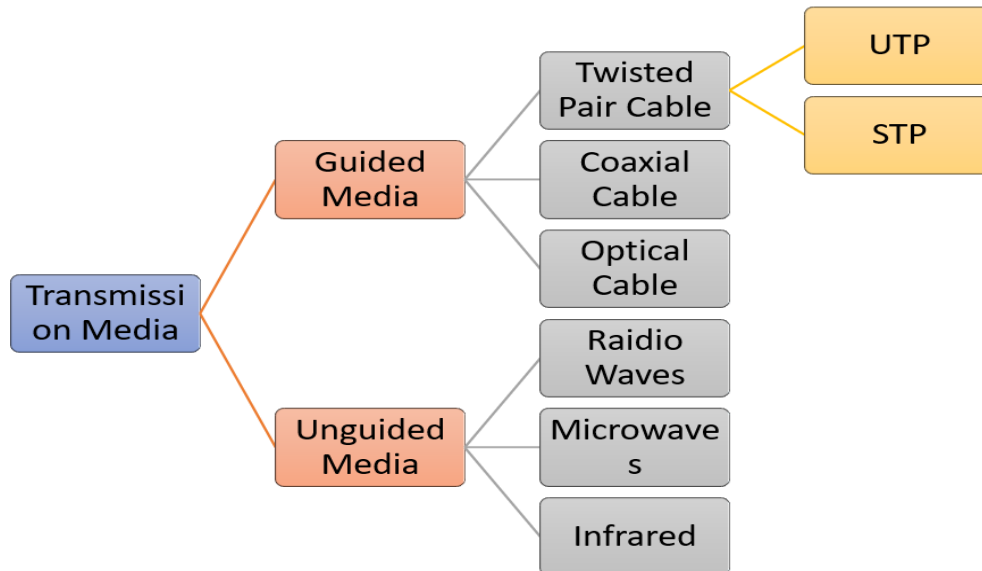
Where:

- C is the maximum data rate.

- **B** is the bandwidth of the channel.
- **S** is the signal power.
- **N** is the noise power.

This formula illustrates that the maximum data rate depends on both the bandwidth and the signal-to-noise ratio (SNR).

Transmission Media in Computer Networks



1. Guided Media

Guided Media is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. There are 3 major types of Guided Media: Twisted Pair, Coaxial and Optical Fiber Cables

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

1.1 Twisted Pair Cable

It consists of 2 separately insulated conductor wires twisted about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

(a) Unshielded Twisted Pair (UTP): UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- Least expensive
- Easy to install
- High-speed capacity

Disadvantages:

MCA 1ST SEM

- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

(b) Shielded Twisted Pair (STP): Shielded Twisted Pair (STP) cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast data rate Ethernet and in voice and data channels of telephone lines.

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

Disadvantages:

- Comparatively difficult to install and manufacture
- More expensive
- Bulky

1.2 Coaxial Cable

Coaxial cable has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.

The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- Coaxial cables has high bandwidth .
- It is easy to install.
- Coaxial cables support multiple channels

Disadvantages:

- Coaxial cables are expensive.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.

1.3 Optical Fiber Cable

Optical Fibre Cable uses the concept of total internal reflection of light through a core made up of glass. The core is surrounded by a less dense glass or plastic covering called the coating. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost

2. Unguided Media

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals. There are 3 types of Signals transmitted through unguided media: Radio wave, Microwave and Infrared Wave.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

2.1 Radio Waves

Radio waves are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3KHz - 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

Types of Radio Waves:

- Short Wave: AM Radio
- VHF (Very High Frequency): FM Radio/TV
- UHF (Ultra High Frequency): TV

Radio Wave Components:

- Transmitter: Responsible for encoding the signal.
- Receiver: Responsible for decoding the signal.

2.2 Microwaves

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz - 300GHz. Micro waves are majorly used for mobile phone communication and television distribution.

Advantages:

- Cheaper than using cables
- Freedom from land acquisition
- Ease of communication in difficult terrains
- Communication over oceans

Disadvantages:

- Insecure communication.
- Out of phase signal.
- Susceptible to weather conditions.
- Bandwidth is limited.
- High cost of design, implementation, and maintenance.

2.3 Infrared

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300GHz - 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Wireless Transmission

Wireless transmission refers to the use of radio waves or other forms of electromagnetic waves to transmit data without physical cables. Some key aspects of wireless transmission include:

- **Radio Waves:** These are used for broadcast and mobile communication (e.g., Wi-Fi, Bluetooth, cellular networks).
- **Microwave Transmission:** High-frequency radio waves used in long-distance communications such as satellite links or ground-based microwave systems.
- **Infrared:** Short-range wireless communication used in devices like remote controls, infrared communication between devices, and certain sensors.
- **Bluetooth & Wi-Fi:** Two popular standards for wireless local area networks (WLANs) and personal area networks (PANs).

Applications of Transmission Media in Computer Networks

Transmission Media	Application
Unshielded Twisted Pair (UTP)	Local Area Networks (LAN), telephones
Shielded Twisted Pair (STP)	Industrial networks, environments with high interference
Optical Fiber Cable	Long-distance communication, internet backbones
Coaxial Cable	Cable TV, broadband internet, CCTV
Stripline	Printed Circuit Boards (PCBs), microwave circuits
Microstripline	Antennas, satellite communication, RF circuits
Radio	Wireless communication, AM/FM radio, mobile phones
Infrared	Remote controls, short-range communication
Microwave	Satellite communication, radar, long-distance links

Mobile Telephone System

A **Mobile Telephone System** is a wireless communication system that allows users to make voice calls, send messages, and access data services using **cellular networks**.

- It uses **radio frequencies** to connect mobile devices to base stations (cell towers).

MCA 1ST SEM

- The system is divided into "**cells**" (geographic areas), each served by a base station.
 - As users move, the network hands over the connection to the next cell (**handover/handoff**).
-
- **1G (First Generation)**: Analog mobile systems, such as the **AMPS (Advanced Mobile Phone System)**, which provided basic voice services.
 - **2G (Second Generation)**: Introduced digital mobile networks (e.g., **GSM** and **CDMA**) with better voice quality and the introduction of SMS (Short Message Service).
 - **3G (Third Generation)**: Allowed mobile broadband, faster data speeds, and the ability to access the internet on mobile devices (e.g., **UMTS**, **CDMA2000**).
 - **4G (Fourth Generation)**: Enhanced mobile broadband with high-speed data, enabling HD video, high-speed internet, and seamless communication (e.g., **LTE**).
 - **5G (Fifth Generation)**: Provides ultra-fast data speeds, low latency, and the ability to connect more devices simultaneously, driving innovations in IoT, autonomous vehicles, and smart cities.

MCA 1ST SEM

MODULE - 2

Data Link Layer: Design issues, error detection and correction design issues, elementary ,data link protocols, CRC codes, sliding window protocols, HDLC, the data link layer in the internet. Elementary Data Link Layer Protocols, sliding window protocols, noisy and noiseless channels. THE MEDIUM ACCESS SUBLAYER: Channel allocations problem, multiple access protocols, Ethernet, Data Link Layer switching, Wireless LAN, Broadband Wireless, Bluetooth.

Introduction to Data Link Layer

The Data Link Layer is the second layer in the OSI model and plays a crucial role in establishing reliable communication between adjacent network nodes. This layer ensures error-free transmission of data frames over the physical medium and provides essential services for network communication.

The Data Link Layer operates between the Physical Layer and Network Layer, acting as a bridge that transforms raw transmission facilities into reliable communication channels. It handles the complexities of the physical medium while providing standardized services to the upper layers.

Functions of Data Link Layer

1. Framing

Framing is the fundamental process of organizing raw data bits into structured units called frames. The Data Link Layer encapsulates network layer packets into frames by adding header and trailer information.

Key Aspects of Framing:

Frame Delimitation: Identifying the beginning and end of each frame

Frame Synchronization: Ensuring proper timing between sender and receiver

Frame Size Management: Controlling the maximum transmission unit (MTU)

Address Information: Including source and destination MAC addresses

Types of Framing:

Fixed-Size Framing: All frames have identical length

Variable-Size Framing: Frame length varies based on data content

Delimiter-Based Framing: Special characters mark frame boundaries

2. Error Detection and Correction

The Data Link Layer implements sophisticated mechanisms to identify and correct transmission errors that may occur during data transfer.

Error Detection Mechanisms:

Redundancy Addition: Extra bits added for error checking

MCA 1ST SEM

Mathematical Algorithms: Complex calculations to detect corruption

Real-time Monitoring: Continuous verification of data integrity

Statistical Analysis: Pattern recognition for error identification

Error Correction Capabilities:

Forward Error Correction (FEC): Automatic error correction without retransmission

Automatic Repeat Request (ARQ): Requesting retransmission of corrupted data

Hybrid Approaches: Combining detection and correction techniques

Flow Control Mechanisms

Flow control ensures that the sender does not overwhelm the receiver with data faster than it can be processed. This mechanism maintains optimal data transfer rates and prevents buffer overflow.

Stop-and-Wait Protocol

The Stop-and-Wait protocol is the simplest flow control mechanism where the sender transmits one frame and waits for acknowledgment before sending the next frame.

Operational Characteristics:

Sequential Transmission: One frame at a time

Acknowledgment Dependency: Sender waits for ACK signal

Timeout Mechanism: Retransmission after specified time

Simplicity: Easy implementation and understanding

Advantages Disadvantages

- Simple implementation Low bandwidth utilization
- Reliable data transfer High latency for long distances
- Minimal buffer requirements Inefficient for high-speed networks
- Easy error recovery Susceptible to network delays

Sliding Window Protocol

The Sliding Window protocol allows multiple frames to be transmitted before receiving acknowledgments, significantly improving network efficiency.

Sliding Window Protocol allows sending multiple packets before receiving acknowledgments.

- Using a "window" to manage packet flow, it improves network efficiency and throughput, especially over long-distance or high-latency connections.
- Sliding window protocols are used where reliable and ordered delivery of packets is needed, such as in the Data Link Layer and the Transmission Control Protocol in Transport Layer.

Terminologies Related to Sliding Window Protocol

1. Transmission Delay (Tt): Time to transmit the packet from the host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

$$T_t = \text{Data Size (D)} / \text{Bandwidth (B)} \quad T_t = \text{Bandwidth (B)} / \text{Data Size (D)}$$

2. Propagation Delay (Tp): It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

$$T_p = \text{Distance (d)} / \text{Propagation Speed (s)} \quad T_p = \text{Propagation Speed (s)} / \text{Distance (d)}$$

3. Efficiency: It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

$$\begin{aligned} \text{Total time (TT)} &= T_t(\text{data}) + T_p(\text{data}) + \\ &T_t(\text{acknowledgement}) + T_p(\text{acknowledgement}) \\ &= T_t(\text{data}) + T_p(\text{data}) + T_p(\text{acknowledgement}) \\ &= T_t + 2 * T_p \end{aligned}$$

Since acknowledgements are very less in size, their transmission delay can be neglected.

$$\text{Efficiency} = \frac{T_t}{T_t + 2T_p} = \frac{1}{1 + 2a}, a = \frac{T_p}{T_t} \quad \text{Efficiency} = \frac{T_t}{T_t + 2T_p} = \frac{1}{1 + 2a}, a = \frac{T_p}{T_t}$$

4. Effective Bandwidth(EB) or Throughput - Number of bits sent per second.

$$EB = \text{Data Size (D)} / \text{Total Cycle time (Tt + 2 * Tp)}$$

Multiplying and dividing by Bandwidth (B),

$$\begin{aligned} &= (1 / (1 + 2a)) * B \quad [\text{Using } a = T_p / T_t] \\ &= \text{Efficiency} * \text{Bandwidth} \end{aligned}$$

5. Capacity of link - If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.

$$\text{Capacity} = \text{Bandwidth (B)} * \text{Propagation (Tp)}$$

For Full Duplex channels,

$$\text{Capacity} = 2 * \text{Bandwidth (B)} * \text{Propagation (Tp)}$$

Concept of Pipelining

In Stop and Wait protocol, only 1 packet is transmitted at a time. After sending a packet, the sender must wait for an acknowledgement from the receiver before transmitting the next one.

The problem with this setup is low efficiency - the communication channel remains underutilized because only one packet is in transit, even though more packets could fit into the channel during the waiting time.

$$\text{The total cycle time is: } T_{\text{cycle}} = T_t + 2T_p \quad T_{\text{cycle}} = T_t + 2T_p$$

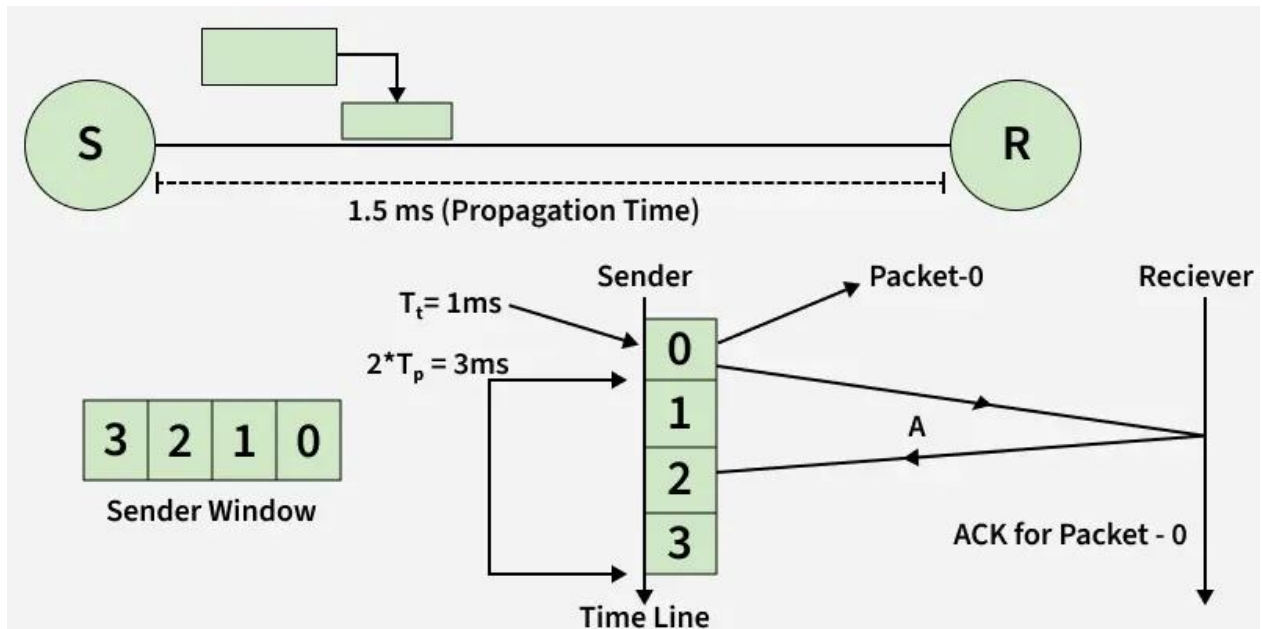
Now, let's calculate how many packets could ideally be transmitted during one cycle time:

- In T_t units → **1 packet** can be transmitted
- In 1 unit → $1/T_t$ packets can be transmitted
- In $(T_t + 2T_p)$ units → $T_t + 2T_p / T_t = 1 + 2T_p / T_t$

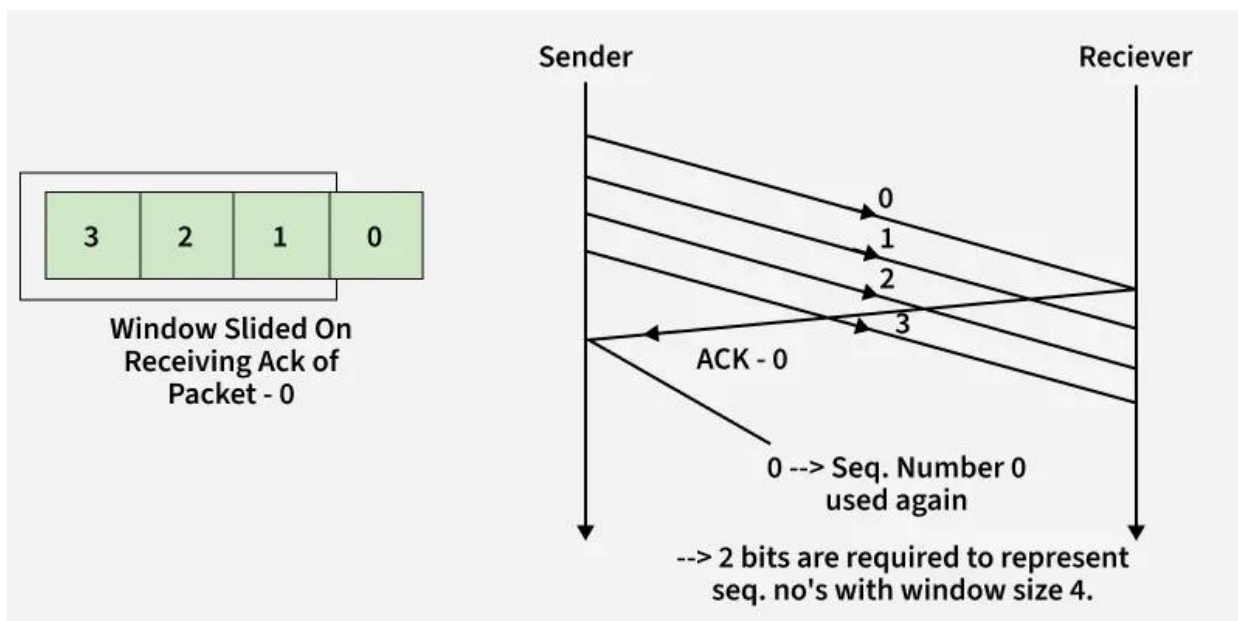
$$\text{If we use the notation } a = \frac{T_p}{T_t} \quad a = \frac{T_p}{T_t}$$

MCA 1ST SEM

- Packets per cycle = $1+2a$



Maximum packets that can be transmitted in a total cycle time: After we have received the Ack for packet 0, window slides and the next packet can be assigned sequence number 0. We reuse the sequence numbers which we have acknowledged so that header size can be kept minimum as shown in the diagram given below.



Maximum packets that can be transmitted in a total cycle time = $1+2a$

MCA 1ST SEM

Example: Let $T_t=1$ ms (transmission time per packet) and $T_p=1.5$ ms (propagation time).

- After the sender transmits packet 0, it immediately sends packets 1, 2, and 3.
- The acknowledgment for packet 0 arrives after:
- $2(T_p) = 3$ ms

In **Stop-and-Wait**, only 1 packet is transferred in:

- $T_t + 2(T_p)=4$ ms

With Sliding Window, a window of packets is maintained packets that have been sent but not yet acknowledged—allowing multiple packets to be transmitted efficiently.

Minimum Number of Bits For Sender Window

As we have seen above,

*Maximum window size = $1 + 2*a$ where $a = T_p/T_t$*

*Minimum sequence numbers required = $1 + 2*a$.*

Each packet in the current window is assigned a sequence number.

- **Sender window bits:** To represent the sender window, the number of bits required is:

$$\text{Bits} = \lceil \log_2(1+2a) \rceil$$

- **Protocol header constraint:** Sometimes, the sequence number field in the header is fixed. If the field has **N bits**, we can have **2^N sequence numbers**.

- **Window size:**

$$\text{Window Size (ws)} = \min(1+2a, 2^N)$$

- **Minimum bits to represent window:**

$$\text{Bits} = \lceil \log_2(ws) \rceil$$

This discussion covers sending windows only. Receiving windows, implemented using Go-Back-N or Selective Repeat for pipelining, will be discussed separately.

Key Features:

- Window Size: Number of frames that can be sent without acknowledgment
- Sequence Numbers: Unique identifiers for frame ordering
- Buffer Management: Efficient memory utilization
- Dynamic Adjustment: Window size adaptation based on network conditions


Types of Sliding Window:

- Go-Back-N: Retransmits all frames after error detection
- Selective Repeat: Retransmits only corrupted frames
- Adaptive Window: Dynamic window size adjustment

❑ Error Control Techniques

Error control mechanisms ensure data integrity by detecting and correcting

transmission errors through various mathematical and logical approaches.

Parity Check 

Parity checking is a simple error detection method that adds a single bit to

MCA 1ST SEM

make the total number of 1s either even or odd.

Types of Parity:

Even Parity: Total 1s must be even

Odd Parity: Total 1s must be odd

Two-Dimensional Parity: Row and column parity checking

Longitudinal Redundancy Check (LRC): Block-wise parity verification

Characteristics:

Detection Capability: Single-bit errors

Implementation: Simple hardware/software logic

Overhead: Minimal additional bits required

Limitations: Cannot detect even number of errors

Cyclic Redundancy Check (CRC)

CRC is a sophisticated error detection technique that uses polynomial division to generate check sequences for data verification.

CRC Process:

Generator Polynomial: Mathematical function for calculation

Division Algorithm: Systematic computation method

Remainder Generation: Check sequence creation

Verification Process: Error detection at receiver

Popular CRC Standards:

CRC-8: 8-bit check sequence

CRC-16: 16-bit check sequence

CRC-32: 32-bit check sequence (widely used)

CRC-64: 64-bit check sequence for critical applications

Hamming Code

MCA 1ST SEM

Hamming Code is an error correction technique that can detect and correct single-bit errors through strategic placement of parity bits.

Hamming Code Principles:

Parity Bit Positioning: Strategic placement at powers of 2

Syndrome Calculation: Error location identification

Single Error Correction: Automatic bit correction

Double Error Detection: Identification of multiple errors

Implementation Process:

Data Bit Organization: Systematic arrangement of information bits

Parity Bit Calculation: Mathematical determination of check bits

Error Syndrome: Pattern analysis for error location

Correction Mechanism: Automatic error fixing process



Data Link Layer Protocols

High-Level Data Link Control (HDLC) 🏢

HDLC is a comprehensive data link protocol that provides reliable communication over point-to-point and multipoint links.

HDLC Frame Structure:

Flag Field: Frame boundary identification (01111110)

Address Field: Station identification

Control Field: Frame type and sequence information

Information Field: Actual data payload

Frame Check Sequence: Error detection code

HDLC Frame Types:

Information Frames (I-frames): Carry user data

Supervisory Frames (S-frames): Flow and error control

Unnumbered Frames (U-frames): Link management and control

HDLC Operational Modes:

Normal Response Mode (NRM): Primary-secondary communication

Asynchronous Balanced Mode (ABM): Peer-to-peer communication

Asynchronous Response Mode (ARM): Secondary station initiation

MCA 1ST SEM

Point-to-Point Protocol (PPP)

PPP is a versatile data link protocol designed for direct connections between two network nodes, commonly used in dial-up and broadband connections.

PPP Components:

Link Control Protocol (LCP): Link establishment and configuration

Network Control Protocols (NCPs): Network layer protocol support

Authentication Protocols: Security and identity verification

Compression Protocols: Data optimization techniques

PPP Frame Format:

Flag: Frame delimiter (01111110)

Address: Broadcast address (11111111)

Control: Unnumbered information (00000011)

Protocol: Payload identification

Information: Data payload

Frame Check Sequence: Error detection

Feature HDLC PPP

- Application LANs, WANs Point-to-point links
- Authentication Limited PAP, CHAP support
- Network Layer Single protocol Multiple protocols
- Configuration Manual setup Automatic negotiation
- Error Recovery Go-Back-N ARQ Various methods

Advanced Data Link Layer Concepts

Quality of Service (QoS)

The Data Link Layer implements QoS mechanisms to prioritize different types of traffic and ensure optimal performance for critical applications.

Link Aggregation

Multiple physical links are combined to create a single logical link with increased bandwidth and redundancy.

Virtual LANs (VLANs)

MCA 1ST SEM

Logical segmentation of network traffic at the Data Link Layer level,
enabling flexible network management and security.

Spanning Tree Protocol (STP) 🌳

Prevention of network loops in switched environments through intelligent
path selection and redundant link management.

Performance Metrics and Optimization

Throughput Measurement 📊

- Effective Data Rate: Actual user data transmission speed
- Protocol Efficiency: Ratio of payload to total frame size
- Channel Utilization: Percentage of available bandwidth usage

Latency Considerations ⌚

- Propagation Delay: Signal travel time across medium
- Processing Delay: Frame handling time at nodes
- Queuing Delay: Buffer waiting time
- Transmission Delay: Frame serialization time

Future Trends and Technologies

- The Data Link Layer continues to evolve with emerging technologies such as:
- Software-Defined Networking (SDN): Programmable data link control
- Network Function Virtualization (NFV): Virtual data link services
- 5G and Beyond: Ultra-low latency requirements
- Internet of Things (IoT): Lightweight protocols for constrained devices
- Quantum Networking: Next-generation error correction techniques

Summary

The Data Link Layer serves as the foundation for reliable network communication by providing essential services including framing, error control, and flow control. Understanding these concepts is crucial for network professionals and forms the basis for more advanced networking topics.

The protocols and techniques discussed in this unit demonstrate the sophisticated engineering required to ensure data integrity and efficient communication in modern computer networks. As technology continues to advance, these fundamental principles remain relevant while adapting to new challenges and requirements.

THE MEDIUM ACCESS SUBLAYER (MAC Layer)

MCA 1ST SEM

The **Medium Access Control (MAC)** sublayer is part of the **Data Link Layer** in the OSI model. Its main function is to **control how multiple devices share a communication channel**.

1. Channel Allocation Problem

- **Goal:** Decide how users share the available bandwidth.
 - **Types:**
 - **Static Channel Allocation:**
 - Fixed assignment of channels (e.g., FDM, TDM).
 - Simple but inefficient when some users are idle.
 - **Dynamic Channel Allocation:**
 - Channels are assigned as needed.
 - Efficient use of bandwidth, used in LANs and wireless systems.
 - **Challenges:**
 - Collisions (two nodes transmit at the same time)
 - Fairness
 - Throughput optimization
-

2. Multiple Access Protocols

These define how multiple stations access the shared medium.

(a) Random Access Protocols

- **ALOHA:**
 - Nodes transmit whenever they have data.
 - **Pure ALOHA:** Collisions possible anytime.
 - **Slotted ALOHA:** Time divided into slots; transmissions start only at slot boundaries (improves efficiency).
- **CSMA (Carrier Sense Multiple Access):**
 - A station listens before transmitting.
 - Variants:
 - **1-persistent CSMA:** Transmit immediately if channel idle.
 - **Non-persistent CSMA:** Wait random time before retrying.
 - **p-persistent CSMA:** Transmit with probability p when idle.
 - **CSMA/CD (Collision Detection):** Used in Ethernet. Detects collisions and stops transmission.

(b) Controlled Access Protocols

- **Reservation:** Stations reserve the channel for future transmission.
- **Polling:** Central controller invites each station to transmit.
- **Token Passing:** A token circulates; only the holder can transmit (used in Token Ring).

(c) Channelization Protocols

- Divide the channel so multiple users can transmit simultaneously:

MCA 1ST SEM

- **FDMA (Frequency Division Multiple Access)**
 - **TDMA (Time Division Multiple Access)**
 - **CDMA (Code Division Multiple Access)**
-

3. Ethernet

- **Most widely used LAN technology.**
 - Based on **IEEE 802.3** standard.
 - Uses **CSMA/CD** for medium access (in older wired LANs).
 - **Frame Format:**
 - Preamble, Destination MAC, Source MAC, Type/Length, Data, CRC.
 - **Modern Ethernet:**
 - **Switched Ethernet:** No collisions, full duplex, high speed (1–100 Gbps).
 - **Uses MAC addresses** for device identification.
-

4. Data Link Layer Switching

- Used to improve LAN performance by segmenting traffic.

Types:

1. **Bridges:**
 - Connect multiple LAN segments.
 - Operate at Data Link Layer.
 - Use MAC addresses to forward frames.
 2. **Switches:**
 - Multiport bridges.
 - Maintain a **MAC address table**.
 - Provide dedicated bandwidth per port (reduces collision).
 3. **Learning Switches:**
 - Automatically learn which MAC addresses are on which ports.
-

5. Wireless LAN (WLAN)

- Based on **IEEE 802.11** standards.
 - Uses **CSMA/CA (Collision Avoidance)** since collision detection isn't possible in wireless.
 - **Components:**
 - **Access Point (AP):** Connects wireless stations to wired LAN.
 - **Stations (STA):** Wireless devices.
 - **Modes:**
 - **Infrastructure Mode:** Through AP.
 - **Ad Hoc Mode:** Devices communicate directly.
 - **Features:** Mobility, flexibility, and uses unlicensed frequency bands (2.4 GHz, 5 GHz).
-

6. Broadband Wireless

- Provides **high-speed wireless data access** over large areas.
 - Examples:
 - **WiMAX (IEEE 802.16)**: Up to several kilometers coverage.
 - **LTE/5G**: Cellular broadband systems.
 - **Features**:
 - High data rates.
 - QoS support.
 - Suitable for last-mile connectivity.
-

7. Bluetooth

- **IEEE 802.15.1** standard.
 - Short-range wireless technology (~10 meters).
 - Operates in **2.4 GHz ISM band**.
 - **Architecture**:
 - **Piconet**: 1 master + up to 7 active slaves.
 - **Scatternet**: Interconnected piconets.
 - **Applications**: Wireless headsets, IoT devices, file sharing.
 - **Protocol**: Uses **Frequency Hopping Spread Spectrum (FHSS)** to reduce interference.
-

Summary Table

Technology/Protocol	Standard	Access Method	Range/Usage
Ethernet	IEEE 802.3	CSMA/CD	Wired LAN
Wi-Fi	IEEE 802.11	CSMA/CA	Wireless LAN
WiMAX	IEEE 802.16	Scheduled Access	Broadband Wireless
Bluetooth	IEEE 802.15.1	FHSS	Short-range, personal area network

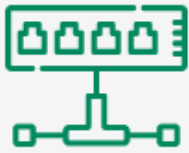
MODULE - 3

Connecting devices: learning bridges, spanning tree bridges, repeaters, hubs, bridges, switches, routers and gateways, definition of multiplexing and types.

Network Layer: Network Layer Design issues, store and forward packet switching, connectionless and connection oriented networks-routing algorithms-optimality principle, circuit and packet switching, definition of flooding and multicast.

Network Devices

Common Types of Network Devices



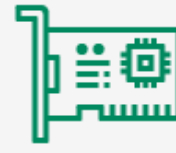
Hub



Router



Gateway



NIC



Modem



Repeater



WAP



Firewall



IDPS



VPN

Network devices are fundamental hardware components in computer networking that operate across different layers of the OSI and TCP/IP models. They facilitate data transmission, regulate traffic flow, provide interconnectivity between heterogeneous networks, and enforce security policies.

Functions of Network Devices

- Enable communication by transmitting and receiving data between devices.
- Allow devices to connect to networks efficiently and securely.
- Improve network performance by reducing congestion and managing traffic.
- Provide security by controlling access and preventing unauthorized activities.
- Extend network coverage and solve signal loss or attenuation problems.

Common Networking Devices

1. Access Point (AP)

- Creates a wireless local area network (WLAN).
- Allows wireless devices (smartphones, laptops, IoT devices) to connect to a wired network.
- Commonly used in offices, homes, and public areas to extend Wi-Fi coverage.

2. Modem

- Stands for Modulator/Demodulator.
- Converts digital signals from computers into analog signals for transmission over telephone lines, cable systems, or wireless media, and vice versa.
- Acts as the primary internet access device for users.

Types of Modems:

- **DSL Modem:** Uses telephone lines, slower than cable.
- **Cable Modem:** Uses TV cables, faster than DSL.
- **Wireless Modem:** Provides internet via Wi-Fi.
- **Cellular Modem:** Uses mobile data networks.

3. Firewall

- A security device that filters incoming and outgoing network traffic.
- Blocks unauthorized access while allowing trusted data.
- Can be hardware-based, software-based, or cloud-based.
- Protects against hackers, malware, and cyber threats.

MCA 1ST SEM

4. Repeater

- Operates at the Physical Layer of the OSI model.
- Regenerates and amplifies weak signals to extend network range.
- Commonly used in large LANs or WANs to solve signal attenuation issues.

5. Hub

- A multiport repeater used in star topology networks.
- Broadcasts data to all connected devices, regardless of the destination.
- Inefficient compared to switches due to collisions.

Types of Hubs:

- **Active Hub:** Boosts signals, acts as a repeater.
- **Passive Hub:** Relays signals without amplification.
- **Intelligent Hub:** Provides monitoring and management functions.

6. Bridge

- Operates at the Data Link Layer (Layer 2).
- Connects and filters traffic between two LAN segments.
- Uses MAC addresses to forward data only to the intended segment.

Types of Bridges:

- **Transparent Bridge:** Learns MAC addresses automatically.
- **Source Routing Bridge:** Follows routes specified by the sender.

7. Switch

- An advanced form of a bridge with multiple ports.
- Works at Layer 2 (Data Link Layer) and selectively forwards packets.
- Reduces collisions by creating separate collision domains.

Types of Switches:

- **Unmanaged Switches:** Plug-and-play, simple use.
- **Managed Switches:** Supports VLANs, QoS, link aggregation.
- **Layer 2 Switches:** Forward frames within the same network.
- **Layer 3 Switches:** Perform routing between different networks.
- **PoE Switches:** Provide power and data through the same cable.
- **Gigabit Switches:** Support high-speed Ethernet.
- **Modular Switches:** Expandable and customizable for large networks.

Read more about [Types of Switches](#)

8. Router

- Operates at the Network Layer (Layer 3).
- Uses IP addresses to route data between different networks (LAN to WAN).
- Maintains a routing table to decide the best path.
- Divides broadcast domains for better efficiency.

9. Gateway

- Acts as a protocol converter.
- Connects two networks using different architectures or protocols.
- Can work at any OSI layer depending on its function.
- **Examples:** connecting an enterprise LAN to the internet.

10. Brouter (Bridging Router)

- A hybrid device with features of both a Bridge and a Router.
- Works at Data Link Layer (as bridge) and Network Layer (as router).
- Routes packets between networks and filters traffic within LANs.

11. NIC (Network Interface Card)

- A hardware adapter that enables a computer to connect to a network.
- Works at Layer 2 (Data Link Layer).
- Has a unique MAC address for identification.
- Can be wired (Ethernet) or wireless (Wi-Fi).

MULTIPLEXING

Definition: Technique that allows **multiple signals to share a single communication channel**.

➤ Purpose:

- **Efficient** use of bandwidth.
 - Reduce cost of transmission media.
-

1. Frequency Division Multiplexing (FDM)

- Channel bandwidth divided into **frequency bands**.
- Each user gets a unique frequency range.
- Used in radio, TV, analog systems.

|---F1---|---F2---|---F3---|

→ Each band carries a separate signal

2. Time Division Multiplexing (TDM)

- Time divided into slots; each user gets a specific **time slot**.
- Types:
 - **Synchronous TDM:** Fixed time slots, even if user has no data.
 - **Statistical TDM:** Slots assigned dynamically based on demand.

Time → [A][B][C][A][B][C]...

Each user transmits in its slot

3. Wavelength Division Multiplexing (WDM)

- Used in **fiber optic networks**.
- Different signals transmitted at different **light wavelengths** (colors).

λ_1 | λ_2 | λ_3 | λ_4 → Combined in single fiber

4. Code Division Multiplexing (CDM / CDMA)

- Each user assigned a **unique code**.
- All transmit simultaneously over the same frequency band.
- Used in cellular systems.


MCA 1ST SEM

The Network Layer is the third layer in the OSI model and plays a crucial role in data communication across networks. It is responsible for delivering packets from source to destination across multiple networks.

Key Functions Overview

The Network Layer performs three primary functions that are essential for

internetworking:

1. Logical Addressing  Logical addressing provides a unique identification system for devices across different networks. Unlike physical addresses that are tied to hardware, logical addresses are hierarchical and can be assigned administratively.

Purpose: Identifies source and destination across multiple networks

Characteristics: Independent of physical network topology

Flexibility: Can be changed and reassigned as needed

Scope: Global addressing scheme for internetworking


2. Routing Routing is the process of determining the optimal path for data packets to travel from source to destination through interconnected networks.

Path Selection: Chooses the best route among multiple available paths

Dynamic Adaptation: Adjusts to network changes and failures

Efficiency: Optimizes network resource utilization

Scalability: Handles networks of varying sizes


3. Forwarding  Forwarding is the actual process of moving packets from input port to appropriate output port based on routing decisions.

Packet Processing: Examines destination address in packet headers

Table Lookup: Uses forwarding tables to determine output port

Header Modification: Updates necessary header fields

Quality of Service: Implements traffic management policies

 **IP Addressing** - Foundation of Internet Communication IP (Internet Protocol) addressing is the fundamental mechanism that enables communication across the global internet infrastructure.

IPv4 Addressing

MCA 1ST SEM

IPv4 (Internet Protocol version 4) uses 32-bit addresses represented in dotted decimal notation, providing approximately 4.3 billion unique addresses.

Address Structure:

Total Length: 32 bits (4 bytes)

Representation: Four octets separated by dots (e.g., 192.168.1.1)

Range: 0.0.0.0 to 255.255.255.255

Binary Format: Each octet represents 8 bits



IPv6 Addressing

IPv6 (Internet Protocol version 6) was developed to address IPv4 address exhaustion and provides enhanced features for modern networking requirements.

Key Improvements:

Address Space: 128-bit addresses (340 undecillion addresses)

Simplified Header: More efficient packet processing

Auto-configuration: Simplified network setup

Enhanced Security: Built-in IPSec support

Quality of Service: Better traffic flow handling

Address Format:

Representation: Eight groups of four hexadecimal digits

Separator: Colons (:) between groups

Compression: Consecutive zeros can be abbreviated

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Address Types:

Unicast: One-to-one communication

Multicast: One-to-many communication

Anycast: One-to-nearest communication



Subnetting and Supernetting

MCA 1ST SEM

Subnetting - Network Subdivision

Subnetting is the practice of dividing a large network into smaller, more manageable subnetworks (subnets).

Benefits of Subnetting:

Improved Security: Isolates network segments

Better Performance: Reduces broadcast domains

Efficient IP Usage: Minimizes address wastage

Administrative Control: Easier network management

Scalability: Supports network growth

Subnetting Process:

1. Determine Requirements: Identify number of subnets and hosts needed
2. Calculate Subnet Bits: Determine bits to borrow from host portion
3. Create Subnet Mask: Modify default mask to include subnet bits
4. Calculate Ranges: Determine network addresses for each subnet
5. Assign Addresses: Allocate IP ranges to network segments

Variable Length Subnet Masking (VLSM): VLSM allows different subnet masks within the same network, enabling more efficient IP address utilization by creating subnets of varying sizes based on actual requirements.

Supernetting - Route Aggregation

Supernetting, also known as Classless Inter-Domain Routing (CIDR), combines multiple smaller networks into a single larger network.

Advantages:

Reduced Routing Tables: Fewer routing entries

Improved Efficiency: Less memory and processing overhead

Simplified Management: Easier route administration

Scalability: Supports internet growth

CIDR Notation: Uses slash notation (/) to indicate the number of network bits (e.g., 192.168.0.0/24)

Routing Algorithms - Path Determination

Routing algorithms are mathematical procedures used by routers to determine the best path for packet delivery across networks.

Distance Vector Routing

Distance Vector algorithms use the Bellman-Ford algorithm principle, where each router maintains a table of distances to all known destinations.

Key Characteristics:

Information Sharing: Routers share their complete routing table with neighbors

Periodic Updates: Regular exchange of routing information

Hop Count Metric: Often uses number of hops as distance measure

Distributed Calculation: Each router calculates its own routes

Advantages:

Simplicity: Easy to implement and understand

Low Overhead: Minimal computational requirements

Automatic Updates: Self-configuring when topology changes

Memory Efficient: Stores only necessary routing information

Disadvantages:

Slow Convergence: Takes time to adapt to network changes

Count-to-Infinity Problem: May create routing loops

Limited Scalability: Performance degrades in large networks

Bandwidth Usage: Periodic updates consume network resources

Popular Protocols:

RIP (Routing Information Protocol): Uses hop count, maximum 15 hops

IGRP (Interior Gateway Routing Protocol): Cisco proprietary with enhanced metrics \

Link State Routing

Link State algorithms require each router to maintain a complete topology map of the network and use Dijkstra's shortest path algorithm.

Operation Process:

1. Topology Discovery: Each router learns about its directly connected neighbors
2. Link State Advertisement: Routers flood network with topology information

MCA 1ST SEM

3. Database Construction: Every router builds identical topology database
4. Shortest Path Calculation: Dijkstra's algorithm determines optimal routes
5. Routing Table Update: Calculated paths populate the routing table

Advantages:

Fast Convergence: Quickly adapts to network changes

Loop-Free: Algorithm prevents routing loops

Scalability: Performs well in large networks

Accurate Metrics: Uses precise link cost measurements

Disadvantages:

High Complexity: More difficult to implement and troubleshoot

Resource Intensive: Requires significant CPU and memory

Initial Overhead: Large topology databases need substantial storage

Flooding Traffic: Link state advertisements consume bandwidth

Popular Protocols:

OSPF (Open Shortest Path First): Widely used in enterprise networks

IS-IS (Intermediate System to Intermediate System): Common in ISP networks

Switching Techniques - Data Transfer Methods

Switching techniques determine how data is transmitted through network infrastructure, each with distinct characteristics and applications.

Circuit Switching

Circuit Switching establishes a dedicated communication path between sender and receiver for the entire duration of the communication session.

Operational Phases:

1. Circuit Establishment: Sets up dedicated path through network
2. Data Transfer: Information flows through established circuit
3. Circuit Termination: Releases resources when communication ends

MCA 1ST SEM

Characteristics:

Dedicated Bandwidth: Guaranteed data rate throughout session

Connection-Oriented: Requires session establishment before data transfer

Resource Reservation: Network resources allocated for entire session

Predictable Performance: Consistent delay and throughput

Applications:

Traditional Telephony: PSTN (Public Switched Telephone Network)

Video Conferencing: Real-time communication requiring consistent quality

Critical Applications: Systems needing guaranteed performance

Packet Switching

Packet Switching divides data into small packets that are transmitted independently through the network and reassembled at the destination.

Key Features:

Connectionless Operation: No dedicated path establishment required

Dynamic Routing: Each packet may take different paths

Resource Sharing: Network bandwidth shared among multiple communications

Store-and-Forward: Intermediate nodes temporarily store packets

Advantages:

- Efficient Resource Utilization: Bandwidth shared dynamically
- Fault Tolerance: Alternative paths available if links fail
- Cost Effectiveness: No dedicated resources required
- Scalability: Supports varying traffic patterns

Packet Types:

Datagram: Each packet routed independently

Virtual Circuit: Logical connection established for packet sequence

Applications:

Internet Communication: TCP/IP networks

MCA 1ST SEM

Local Area Networks: Ethernet and Wi-Fi

Wide Area Networks: Modern data networks

Message Switching

Message Switching treats entire messages as single units, storing complete messages at intermediate nodes before forwarding.

Operation:

Store-and-Forward: Complete message stored at each intermediate node

No Real-Time Requirement: Messages processed when resources available

Full Message Integrity: Entire message forwarded as single unit

Flexible Routing: Messages can wait for optimal forwarding conditions

Characteristics:

High Latency: Messages may experience significant delays

Storage Requirements: Intermediate nodes need substantial memory

Error Recovery: Easy to retransmit entire messages if needed

Priority Handling: Messages can be prioritized and queued

Historical Context: Message switching was prevalent in early computer networks and telegraph systems but has largely been replaced by packet switching for most applications due to efficiency and real-time requirements of modern communications.



Summary and Key Takeaways

The Network Layer serves as the foundation for internetworking, providing essential services that enable global communication. Understanding its functions, addressing schemes, routing algorithms, and switching techniques is crucial for network professionals.

Critical Concepts:

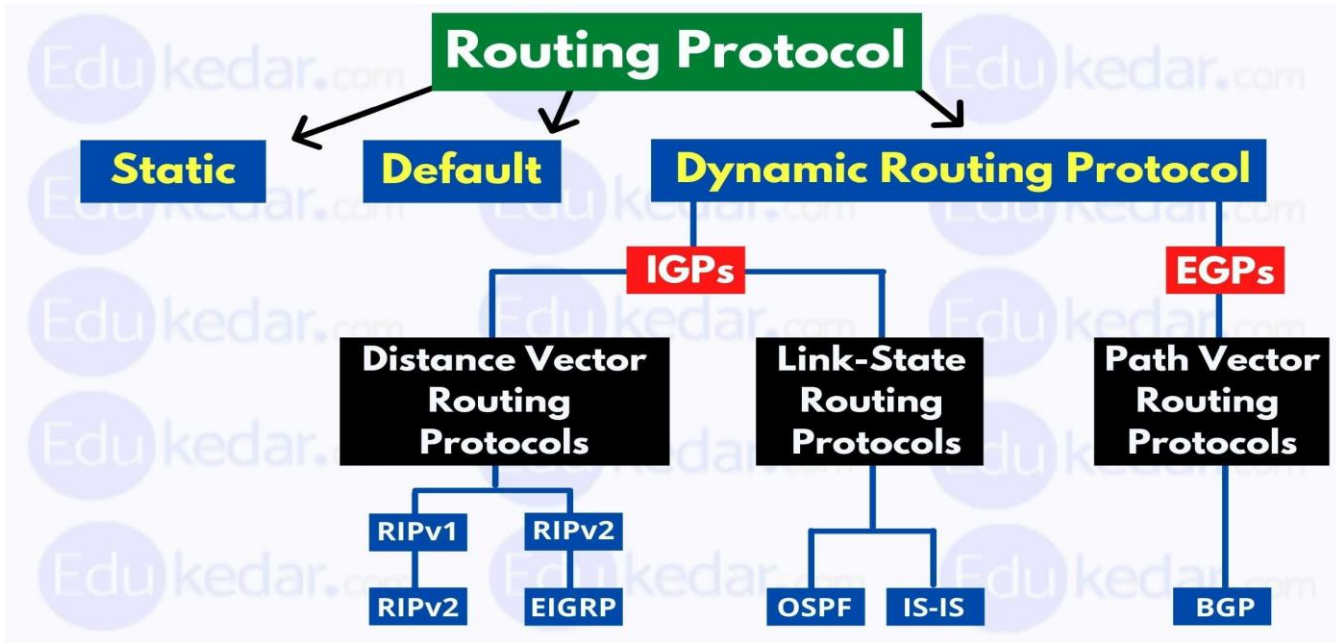
- Logical Addressing: Enables device identification across networks
- Routing and Forwarding: Ensures efficient packet delivery

MCA 1ST SEM

- IP Addressing: IPv4 and IPv6 provide global addressing schemes
- Subnetting/Supernetting: Optimize address space utilization
- Routing Algorithms: Distance vector and link state provide path determination
- Switching Techniques: Circuit, packet, and message switching serve different communication needs
- Practical Applications: These concepts form the backbone of modern internet infrastructure, enterprise networks, and telecommunications systems. Mastery of these fundamentals is essential for network design, implementation, and troubleshooting in professional environments.

MODULE - 4

Routing protocols: Shortest Path, Routing uni-cast Distance Vector Routing, RIP, link state protocols, path vector routing. Internetworking: logical addressing, internet protocols, IP address, CIDR, IPv4 addressing, IPv6 Protocol addressing, addresses mapping, ICMP, IGMP, ARP, RARP, DHCP.



Routing is the process of finding the **best path** for data packets to travel from source to destination across networks.

1. Shortest Path Routing

- **Idea:** Find the path with the minimum cost (distance, delay, hops, etc.).
- **Algorithm:** Dijkstra's Algorithm (used in OSPF).
- **Advantages:**
 - Efficient path selection.
 - Updates quickly when topology changes.
- **Metric examples:** Hop count, bandwidth, delay, cost.

Router A → Router B → Router C
Choose path with least total cost

2. Unicast Routing

- **Definition:** Sending packets from **one source to one destination** (one-to-one).
- Used by most IP networks.

3. Distance Vector Routing

- Each router knows only:
 - **Distance (metric)** to destination.

- **Next hop** to reach it.
- Periodically shares its routing table with neighbors.
- **Algorithm: Bellman–Ford.**
- **Problems:** Slow convergence, routing loops.
- **Example Protocol: RIP.**

Router A: B = 1 hop, C = 2 hops via B

4. RIP (Routing Information Protocol)

- **Type:** Distance Vector Protocol.
 - **Metric:** Hop count (max 15 hops).
 - **Updates:** Every 30 seconds.
 - **Limitations:**
 - Not suitable for large networks.
 - Slow convergence.
 - **Versions:** RIP v1 (classful), RIP v2 (classless, supports CIDR).
-

5. Link State Routing

- Each router has **complete topology information.**
- **Steps:**
 1. Discover neighbors.
 2. Measure link cost.
 3. Flood link-state packets to all routers.
 4. Use **Dijkstra's Algorithm** to compute shortest paths.
- **Example Protocol: OSPF (Open Shortest Path First).**
- **Advantages:**
 - Faster convergence.
 - Scalable and loop-free.

All routers share full network map
→ Independently compute best routes

6. Path Vector Routing

- Used in **inter-domain (between autonomous systems)** routing.
- Each router advertises the **entire path (sequence of ASes)** to reach a network.
- **Example Protocol: BGP (Border Gateway Protocol).**
- **Advantages:**
 - Prevents routing loops.
 - Scalable for the Internet.

INTERNETWORKING CONCEPTS

1. Logical Addressing

- **Purpose:** Identify devices **independently of physical hardware**.
 - Logical address = **IP address**.
 - Physical address = **MAC address**.
 - Used by **Network Layer**.
-

2. Internet Protocol (IP)

- **Main protocol of the Internet Layer.**
 - Provides **connectionless, best-effort** delivery.
 - **Responsibilities:**
 - Logical addressing (IP addresses).
 - Routing packets between networks.
 - Fragmentation and reassembly.
-

3. IP Address

- **Unique identifier** for each device on a network.
 - **Format (IPv4):** 32 bits = 4 octets (e.g., 192.168.1.1)
 - **Classes:**
 - A (1.0.0.0 – 126.255.255.255)
 - B (128.0.0.0 – 191.255.255.255)
 - C (192.0.0.0 – 223.255.255.255)
-

4. CIDR (Classless Inter-Domain Routing)

- Removes the rigid class-based addressing system.
 - Allows **variable-length subnet masks (VLSM)**.
 - Format: IP_address / prefix_length
 - Example: 192.168.1.0/24 → 24 bits for network, 8 bits for host.
-

5. IPv4 Addressing

- 32-bit address.
 - **Dotted-decimal notation.**
 - **Types:**
 - Unicast → One-to-one.
 - Broadcast → One-to-all.
 - Multicast → One-to-many.
 - **Limitations:** Exhaustion of address space.
-

6. IPv6 Protocol Addressing

- 128-bit address → Huge address space.
 - **Notation:** 8 groups of 16-bit hexadecimal numbers
(e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
 - **Features:**
 - Simplified header.
 - Auto-configuration.
 - Built-in security (IPsec).
 - No need for NAT.
-

7. Address Mapping

Used to translate between **logical (IP)** and **physical (MAC)** addresses.

(a) ARP (Address Resolution Protocol)

- Maps **IP** → **MAC** address.
- Used by sender before sending frame on LAN.

If MAC unknown → send ARP Request → Receive ARP Reply

(b) RARP (Reverse ARP)

- Maps **MAC** → **IP** address.
 - Used by diskless workstations to obtain IP address from server.
-

8. ICMP (Internet Control Message Protocol)

- Used for **error reporting and diagnostics.**

MCA 1ST SEM

- Examples:
 - **Echo Request/Reply** → used in ping.
 - Destination unreachable.
 - Time exceeded.
 - Works with IP (not a transport protocol).
-

9. IGMP (Internet Group Management Protocol)

- Used by hosts and routers for **managing multicast group membership**.
 - Example: A host joins/leaves a multicast group (like streaming video).
-

10. DHCP (Dynamic Host Configuration Protocol)

- **Automatically assigns IP addresses** and configuration parameters (gateway, DNS).
- **Process:**
 1. **Discover** → Client broadcasts request.
 2. **Offer** → Server sends IP offer.
 3. **Request** → Client requests chosen IP.
 4. **Acknowledge** → Server confirms assignment.

DHCP Server → automatically assigns → IP, Subnet Mask, Gateway, DNS

Summary Table

Concept	Full Form / Function	Layer	Example
RIP	Routing Information Protocol	Network	Distance Vector
OSPF	Open Shortest Path First	Network	Link State
BGP	Border Gateway Protocol	Network	Path Vector

MCA 1ST SEM

Concept	Full Form / Function	Layer	Example
IP	Internet Protocol	Network	IPv4/IPv6
ARP	Address Resolution Protocol	Network	IP→MAC
RARP	Reverse ARP	Network	MAC→IP
ICMP	Internet Control Message Protocol	Network	Ping, errors
IGMP	Internet Group Management Protocol	Network	Multicast
DHCP	Dynamic Host Configuration Protocol	Application	Auto IP assign

MODULE - 5

Transport Protocols: process to process delivery, UDP, TCP, TCP Sliding Window, TCP Congestion Control, congestion control and quality of service. Application Layer-World Wide Web, Standard client-server application-HTTP, FTP, electronic mail, TELNET, DNS.

TRANSPORT LAYER



Overview of Transport Layer

- **Layer 4** in the **OSI Model / TCP-IP Stack**.
 - Provides **process-to-process** communication (not just host-to-host).
 - **Main Functions:**
 - Segmentation and reassembly
 - Process addressing (port numbers)
 - Flow control
 - Error control
 - Connection establishment and release
-



Process-to-Process Delivery

- Each application (process) on a host is identified by a **port number**.
- The transport layer uses **IP addresses + port numbers** to deliver data to the correct application.

Example:

Source: 192.168.1.5:5000 → Destination: 192.168.1.8:80
(Process on PC1) (Web Server process)

Protocol	Port	Example Service
HTTP	80	Web
FTP	21	File Transfer
SMTP	25	Email
DNS	53	Name Resolution



UDP (User Datagram Protocol)

- **Connectionless, unreliable, but fast.**
- No error recovery or flow control.
- Used for real-time or simple transactions (e.g., video, DNS, VoIP).

Features:

- Simple header (8 bytes).

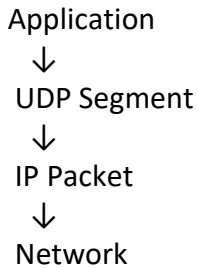
MCA 1ST SEM

- No acknowledgment or retransmission.
- Uses **best-effort delivery**.

UDP Header Fields:

| Src Port | Dest Port | Length | Checksum |

Diagram:



✅ Advantages:

- Low latency, small overhead.
- Suitable for streaming and gaming.

❌ Disadvantages:

- No guarantee of delivery or order.

TCP (Transmission Control Protocol)

- **Connection-oriented, reliable, byte-stream** protocol.
- Establishes a virtual connection before data transfer (3-way handshake).
- Provides error control, sequencing, and flow control.

TCP 3-Way Handshake (Connection Establishment)

Client Server
|----- SYN ----->|
|<----- SYN + ACK ---|
|----- ACK ----->|

1. **SYN** – Request to start connection.
2. **SYN-ACK** – Acknowledge + confirm connection.
3. **ACK** – Connection established.

TCP Header Fields

Field

Description

MCA 1ST SEM

Field	Description
Source & Destination Ports	Identify processes
Sequence Number	For ordering segments
Acknowledgment Number	For confirming received data
Flags	SYN, ACK, FIN, RST
Window Size	For flow control
Checksum	Error detection

TCP Sliding Window Protocol

- Ensures **flow control** between sender and receiver.
- Sender can send multiple segments before waiting for acknowledgment — controlled by **window size**.
- Receiver advertises window size (buffer capacity).

Diagram:

Sender Window:

|1|2|3|4|5|

↑ ↑

Sent Window End

ACK for 1 → Slide window → Send next segment

- **Dynamic window adjustment** allows efficient use of bandwidth.
- Used in **Go-Back-N** and **Selective Repeat** mechanisms.

TCP Congestion Control

- Prevents **network congestion** (too much data in transit).
- Adjusts transmission rate based on network feedback.

Phases of TCP Congestion Control:

1. **Slow Start:**
 - Begin with small window (e.g., 1 MSS).
 - Double window size each RTT until threshold.
2. **Congestion Avoidance:**
 - Increase window linearly (Additive Increase).
3. **Congestion Detection:**

MCA 1ST SEM

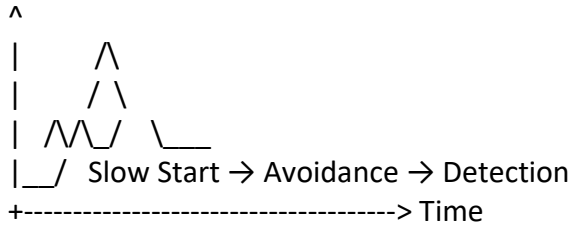
- If packet loss → reduce window (Multiplicative Decrease).

4. Fast Retransmit and Fast Recovery:

- On 3 duplicate ACKs → retransmit immediately (no timeout).

Diagram:

Congestion Window Size



Congestion Control (General Concept)

- **Definition:** Occurs when total network demand > available capacity.
- **Symptoms:** High delay, packet loss, retransmissions.
- **Solutions:**
 - TCP's built-in control (slow start, etc.)
 - Queue management (RED – Random Early Detection)
 - Traffic shaping (Leaky bucket, Token bucket)



Quality of Service (QoS)

QoS ensures **reliable performance** for critical applications (voice, video).

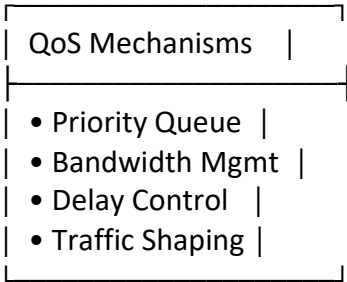
Parameters:

Parameter	Meaning
Bandwidth	Data rate supported
Delay	Time taken to deliver data
Jitter	Variation in delay
Packet Loss	% of dropped packets

QoS Techniques:

- **Traffic shaping:** Control data flow (Leaky/Token bucket).
- **Resource reservation:** RSVP (Reserve bandwidth).
- **Prioritization:** Assign higher priority to real-time traffic.

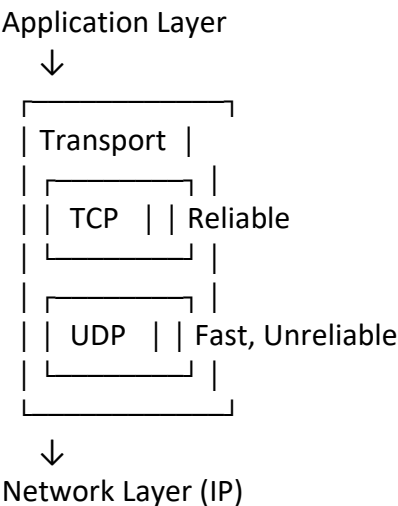
Diagram:



✔ Summary Table

Concept	Protocol/Feature	Description
Process-to-Process Ports		Identify apps on hosts
UDP	Connectionless	Fast but unreliable
TCP	Connection-oriented	Reliable with ACKs
Sliding Window	Flow Control	Sender window adjusts dynamically
Congestion Control	TCP feature	Prevents overload (Slow Start, etc.)
QoS	Service Quality	Guarantees performance for priority traffic

✚ Simplified Diagram — Transport Layer





Overview of Application Layer

- **Topmost layer (Layer 7) of the OSI model / part of the Application layer in TCP/IP.**
 - Provides **network services directly to users or applications.**
 - Functions include:
 - User interface to network.
 - Resource sharing.
 - File transfer, email, web browsing, remote login, etc.
-



World Wide Web (WWW)

- A **distributed information system** based on **hypertext** and **hyperlinks**.
- Uses **client-server model**:
 - **Client**: Web browser (Chrome, Firefox).
 - **Server**: Web server (Apache, Nginx) storing web pages.
- **Key Components**:
 - **Web page**: Written in HTML.
 - **Web browser**: Displays content.
 - **Web server**: Hosts pages and responds to requests.
 - **URL (Uniform Resource Locator)**: Identifies web resources.

Example:

<https://www.example.com/index.html>

- **Protocol**: HTTPS
 - **Domain**: www.example.com
 - **File**: index.html
-



Standard Client-Server Applications

These are core Internet applications built on **Application Layer protocols**.

1. HTTP (Hypertext Transfer Protocol)

- **Used for**: Transferring web pages between client and server.
- **Port**: 80 (HTTP), 443 (HTTPS).
- **Type**: Stateless, request-response protocol.

Process:

MCA 1ST SEM

1. Client sends HTTP request → GET / POST.
2. Server responds with HTTP response → status code + data.

Example:

Client → GET /index.html HTTP/1.1

Server → HTTP/1.1 200 OK

Versions: HTTP/1.1, HTTP/2, HTTP/3 (faster and secure).

HTTPS: Uses **SSL/TLS** encryption for secure communication.

2. FTP (File Transfer Protocol)

- **Used for:** Transferring files between client and server.
- **Port:** 20 (data), 21 (control).
- **Modes:**
 - **Active Mode:** Server initiates data connection.
 - **Passive Mode:** Client initiates data connection (firewall-friendly).

Operations:

- Upload / Download files.
 - Directory listing and navigation.
 - Authentication using username/password.
-

3. Electronic Mail (E-Mail)

- **Purpose:** Sending and receiving messages electronically.
- **Components:**
 1. **User Agent (UA):** E-mail client (Outlook, Thunderbird).
 2. **Mail Transfer Agent (MTA):** Transfers messages between servers.

MCA 1ST SEM

Protocols:

Protocol	Function	Port
SMTP (Simple Mail Transfer Protocol)	Sending mail	25
POP3 (Post Office Protocol v3)	Receiving mail (downloads & deletes)	110
IMAP4 (Internet Message Access Protocol)	Receiving mail (keeps copy on server)	143

Process:

Sender UA → SMTP → Mail Server → SMTP → Receiver's Server → POP3/IMAP → Receiver UA

4. TELNET (Telecommunication Network)

- **Used for:** Remote login to another computer.
- **Port:** 23.
- **Function:** Allows users to **access and control** remote systems as if locally logged in.
- **Disadvantage:** Sends data (including passwords) **in plain text — not secure**.
- **Alternative: SSH (Secure Shell)** uses encryption for secure remote access.

Local PC → TELNET → Remote Server

5. DNS (Domain Name System)

- **Used for:** Translating **domain names ↔ IP addresses**.
- **Port:** 53 (UDP/TCP).
- **Reason:** Humans use names; machines use IPs.

Example:

www.google.com → 142.250.182.36

Structure:

- **Hierarchical, distributed database** of names.
- **Levels:**
 - Root (.)
 - Top-Level Domain (TLD): .com, .org, .edu
 - Second-Level: example.com
 - Subdomain: mail.example.com

Types of DNS Records:

MCA 1ST SEM

Record	Purpose
A	Hostname → IPv4 address
AAAA	Hostname → IPv6 address
MX	Mail exchange server
CNAME	Canonical name (alias)
NS	Name server

Working Process:

1. Browser asks DNS resolver for IP of a domain.
2. Resolver queries root → TLD → authoritative name server.
3. IP address is returned and cached locally.

✓ Summary Table

Protocol	Purpose	Port	Type
HTTP/HTTPS	Web browsing	80 / 443	Request–Response
FTP	File transfer	20, 21	Control + Data channels
SMTP	Send email	25	Push
POP3	Receive email	110	Pull (delete after download)
IMAP4	Receive email	143	Pull (keeps copy on server)
TELNET	Remote login	23	Unsecure text-based
DNS	Name resolution	53	Hierarchical lookup

MCA 1ST SEM

Diagram Summary (Text Format)

