Layers of the OSI Model

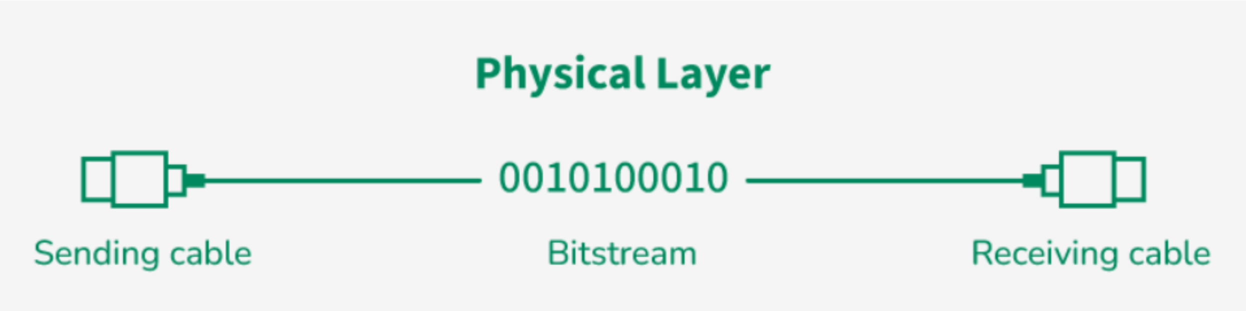
There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

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.



Functions of the Physical Layer

- **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.
- **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.

Protocols in Physical Layer

Typically, a combination of hardware and software programming makes up the physical layer. It consists of several protocols that control data transmissions on a network. The following are some examples of Layer 1 protocols:

- **Ethernet (IEEE 802.3)** : Widely used for wired networks.
- **Wi-Fi (IEEE 802.11)** : For wireless communication.
- **Bluetooth (IEEE 802.15.1)** : Short-range wireless communication.
- **USB (Universal Serial Bus)** : For connecting devices over short distances.

Need of Physical Layer in Security

In security, Physical Layer is essential because many attacks can occur before any software is involved. Threats at this level target the actual hardware or transmission medium.

- **Cable Tapping:** Hackers can intercept data by directly connecting to network cables.

- **Physical Access**: If someone gets into server rooms or hardware areas without permission, they can steal or damage equipment.
- **Wireless Signal Interception**: Attackers can capture Wi-Fi signals from outside using special tools.
- **Signal Jamming**: Devices can be used to block or disrupt Wi-Fi or other wireless communication.
- **Hardware Manipulation**: Someone might tamper with physical devices like routers or USB ports to secretly install harmful software.

Pros of the Physical Layer

- It ensures devices can transmit and receive raw data over physical mediums.
- It provides universal standards for cables, connectors, and signaling, ensuring compatibility.
- **Support for Various Media:** Works with wired (e.g., Ethernet) and wireless (e.g., Wi-Fi) technologies.

Limitations of the Physical Layer

- **No Error Handling**: Cannot detect or correct errors in data transmission.
- **Susceptible to Physical Damage**: Cables, connectors, and hardware failures can disrupt communication.
- **No Data Interpretation**: It only transmits bits and doesn't understand or process the actual data.

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 Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking, "Who has that IP address?" and the destination host will reply with its MAC address.

Sublayers of Data Link Layer

- Logical Link Control (LLC) : This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.
- Media Access Control (MAC) : MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access. The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.

- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** 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.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

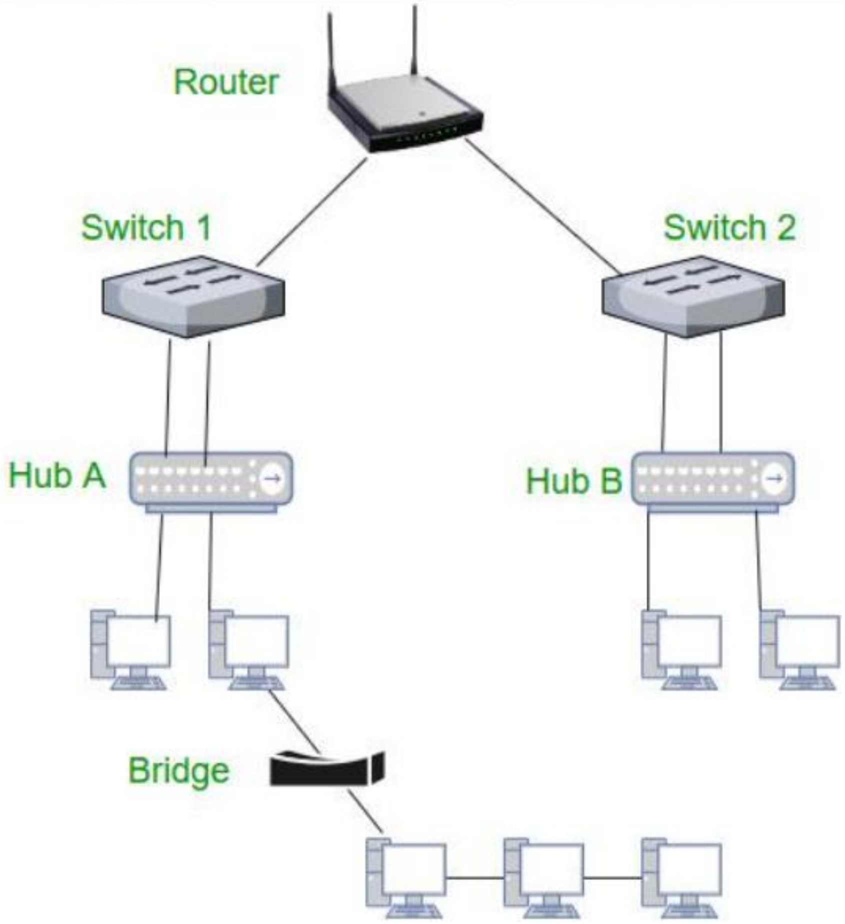
Protocols in Data link layer

There are various protocols in the data link layer, which are as follows:

- Synchronous Data Link Protocol (SDLC)
- High-Level Data Link Protocol (HDLC)
- Serial Line Interface Protocol (SLIP)
- Point to Point Protocol (PPP)
- Link Access Procedure (LAP)
- Link Control Protocol(LCP)
- Network Control Protocol (NCP)

Devices Operating at the Data Link Layer

All these devices rely on MAC addresses for efficient frame delivery and play a crucial role in local network communication and access control.



1. Switch

- A switch is a key device in the Data Link Layer.
- It uses MAC addresses to forward data frames to the correct device within a network.
- Works in local area networks (LANs) to connect multiple devices.

2. Bridge

- A bridge connects two or more LANs, creating a single, unified network.
- Operates at the Data Link Layer by forwarding frames based on MAC addresses.
- Used to reduce network traffic and segment a network.

3. Network Interface Card (NIC)

- A NIC is a hardware component in devices like computers and printers.
- Responsible for adding the MAC address to frames and ensuring proper communication with the network.
- Operates at the Data Link Layer by preparing and sending frames over the physical medium.

4. Wireless Access Point (WAP)

- A WAP allows wireless devices to connect to a wired network.
- Operates at the Data Link Layer by managing wireless MAC addresses.
- Uses protocols like Wi-Fi (IEEE 802.11) to communicate with devices.

5. Layer 2 Switches

- These are specialized switches that only operate at Layer 2, unlike multi-layer switches.
- Responsible for frame forwarding using MAC address tables.

***Note**: The Data Link Layer can be targeted by attacks like MAC spoofing or ARP poisoning. Understanding how devices and frames operate at this layer helps detect and mitigate such threats.*

Limitations of Data Link Layer

- **Limited Scope**: It operates only within a local network and cannot handle end-to-end communication across different networks.
- **Increased Overhead**: Adding headers, trailers, and redundant data (for error correction) increases the size of transmitted data.
- **Error Handling Dependency**: While it can detect and correct some errors, it relies on upper layers for handling more complex issues.
- **No Routing Capability**: The Data Link Layer cannot make routing decisions. It only ensures delivery within the same network segment.

- **Resource Usage**: Flow control and error correction mechanisms may consume extra processing power and memory

Applications of Data Link Layer

- **Local Area Networks (LANs)**: Enables reliable communication between devices within a local network using protocols like Ethernet (IEEE 802.3).
- **Wireless Networks (Wi-Fi)**: Manages communication between devices in wireless networks via protocols like IEEE 802.11 hence, handling media access and error control.
- **Switches and MAC Addressing**: Facilitates the operation of switches by using MAC addresses to forward data frames to the correct device within the network.
- **Point-to-Point Connections**: Used in protocols like PPP (Point-to-Point Protocol) to establish and manage direct communication between two nodes.

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.

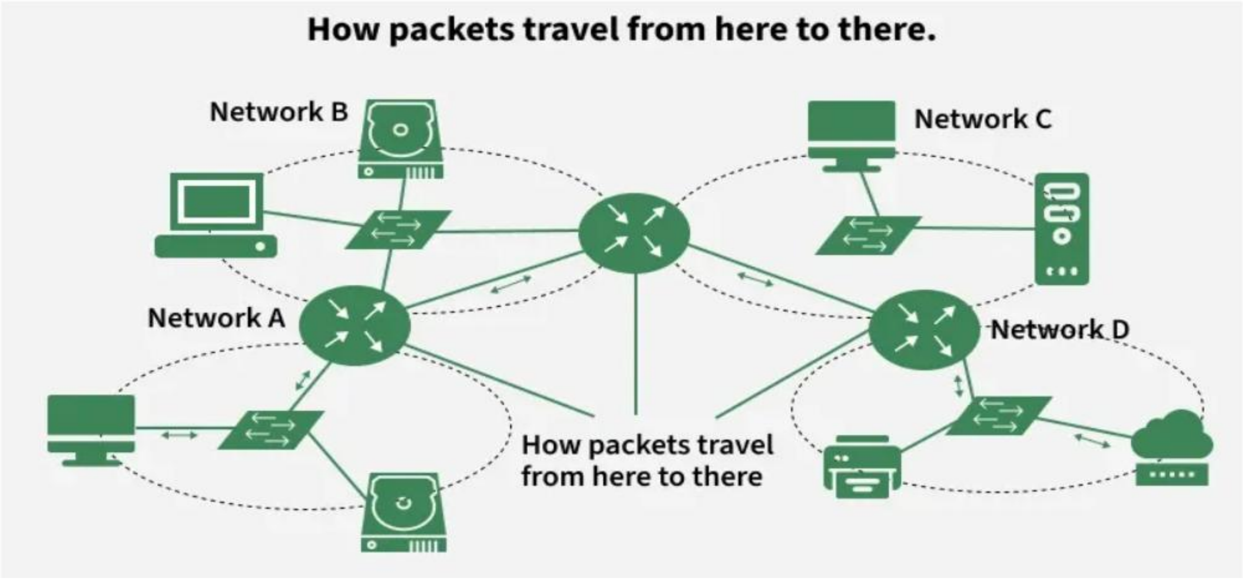
- The sender and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.**
- Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **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.
- **Packetization**: Encapsulates transport layer segments into packets for efficient transmission.
- **Host-to-Host Delivery**: Ensures reliable delivery of packets from the sender to the intended receiver across diverse networks.
- **Forwarding**: Moves packets from the input interface of a router to the appropriate output interface based on the destination IP.
- **Fragmentation and Reassembly**: Splits large packets into smaller fragments to match the maximum transmission unit (MTU) of a network, and reassembles them at the destination.
- **Subnetting**: Divides larger networks into smaller subnetworks for efficient addressing and traffic management.
- **Network Address Translation (NAT)**: Maps private IPs to public IPs for internet communication, conserving address space and adding security.

How the Network Layer Works


How packets travel from here to there.
Network B
Network C
Network A
Network D
How packets travel from here to there

- Each device is assigned a unique logical address (IP address).
- Data from the transport layer is encapsulated into packets, with source and destination IPs attached.
- Routers analyze the destination address and determine the best available path.
- Packets traverse the network hop-by-hop, moving across routers until reaching the destination.
- If the packet size exceeds the MTU, it is fragmented into smaller units.
- At the destination, the fragments are reassembled into the original data.
- If errors occur (e.g., unreachable destination), protocols like ICMP send error messages back to the source.

Protocols Operating at the Network Layer

- IP (Internet Protocol – IPv4/IPv6)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- NAT (Network Address Translation)
- IPSec (Internet Protocol Security)
- MPLS (Multiprotocol Label Switching)

Routing Protocols

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

Advantages of the Network Layer

- Enables end-to-end communication across multiple networks.
- Supports scalability by allowing subnetting and hierarchical addressing.
- Efficiently routes packets using shortest-path and dynamic routing algorithms.
- Provides inter-networking by connecting heterogeneous networks.

Limitations of the Network Layer

- No flow control mechanism; congestion may occur if too many datagrams are in transit.
- Limited error control; mainly relies on upper layers for reliability.
- Routers may drop packets under heavy load, leading to possible data loss.
- Fragmentation increases processing overhead and may affect performance.

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.
- At the sender's side, the transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow and error control to ensure proper data transmission.
- It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- Generally, this destination port number is configured, either by default or manually.
- **Example:** when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.
- At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

Functions of the Transport Layer

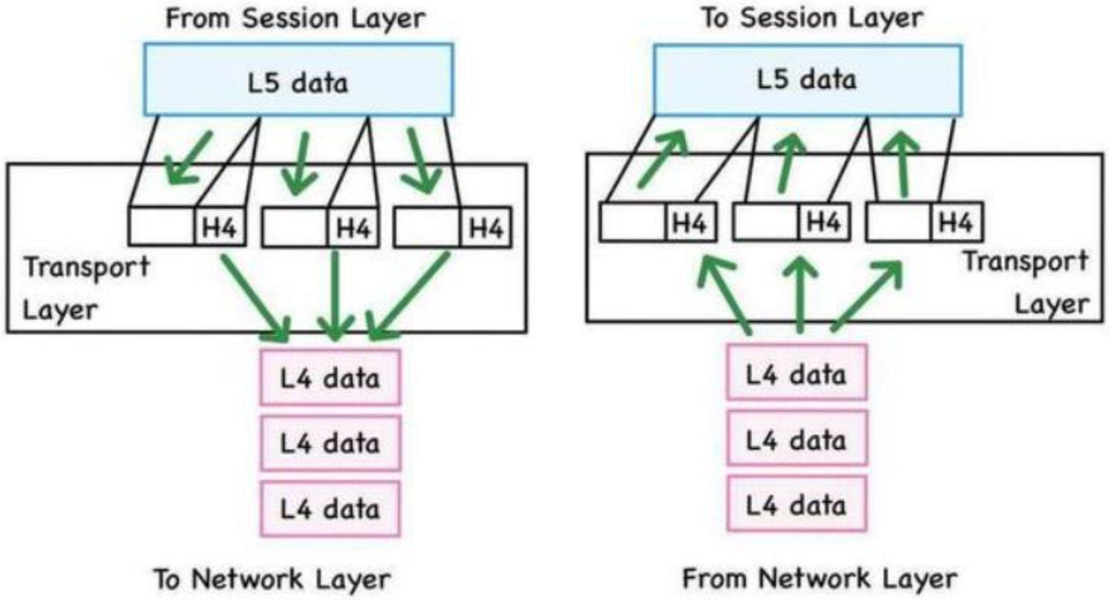
- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** 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.

Services Provided by Transport Layer

- Connection-Oriented Service
- Connectionless Service

Working of Transport Layer

The Transport Layer provides logical communication between processes on different hosts — meaning that even though data travels across various physical networks, the communicating applications perceive a direct, reliable link.



- Implemented **only in end systems**, not in intermediate routers.
- Uses **port numbers** to identify sending and receiving applications.
- Supports **process-to-process delivery**, enabling multiple applications to share a single network connection.
- Performs **multiplexing and demultiplexing** using port numbers to direct data to the correct process.
- Divides data from upper layers into **segments (TCP)** or **datagrams (UDP)** and adds necessary headers.
- Handles **error detection, retransmission, and sequencing** to maintain reliable communication.
- Coordinates **flow control** to ensure the receiver is not overloaded.
- Communicates with the **Network Layer**, which handles addressing and routing, to send data across networks.

- At the receiving end, it removes headers, reassembles data, and passes it to the appropriate application.

3-Way Handshake

The 3-Way Handshake ensures both client and server are ready before data transmission begins:

Step 1: SYN → (Client → Server)

- Client sends a TCP segment with **SYN=1**, including its ISN (Initial Sequence Number).
- Marks the request to initiate a connection

Step 2: SYN-ACK ← (Server → Client)

- Server replies with SYN=1 & ACK=1, containing its own ISN and ACK = **client_ISN + 1**.
- Confirms receipt of client's SYN and initiates its own sync

Step 3: ACK → (Client → Server)

- Client sends an ACK=1 segment with ACK = **server_ISN + 1**.
- Completes synchronization; connection enters **ESTABLISHED** state

Why not just two steps?

If there would have been just two steps i.e., SYN and SYN-ANK, the server would not know if the client is actually receiving the responses or not. Similarly the client would not know if server is receiving the responses or not. Therefore the third step is important for the mutual confirmation between both the client and server for the flow of data.

Transport Layer Protocols

Transport Layer Protocol uses different protocol for the better communication between two ends uses of protocol may differ from specifications. Below mention are some protocols used in Transport Layer

1. Transmission Control Protocol(TCP)

- TCP is connection-oriented Protocol.
- TCP is reliable protocol.
- As TCP is connection-oriented protocol, so first the connection is established between two ends and then data is transferred and then the connection is terminated after all data being sent.

2. User Datagram Protocol (UDP)

- UDP is not reliable protocol
- The protocol UDP is connectionless.
- When speed and size are more important than security and dependability, this kind of protocol is employed.
- The data from the higher layer is supplemented with transport-level addresses, checksum error control, and length information by UDP, an end-to-end transport level protocol.
- A user datagram is the packet that the UDP protocol generates.

3. Stream Control Transmission Protocol (SCTP)

- Many Internet applications use SCTP to perform transport layer duties, similar to User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).
- On top of a connectionless packet network like IP, SCTP is a dependable transport protocol that facilitates data transfer over the network in scenarios involving one or more IP addresses.

Layer 5: Session Layer

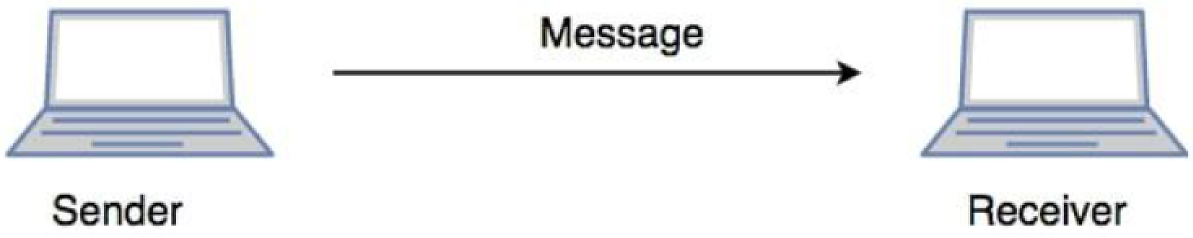
Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

- **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.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Example

Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.



Role of the Session Layer

The Session Layer ensures that two communicating devices can establish a meaningful dialogue, exchange data in an organized manner and properly close the session when communication is complete.

- It provides mechanisms for session setup, management and termination.

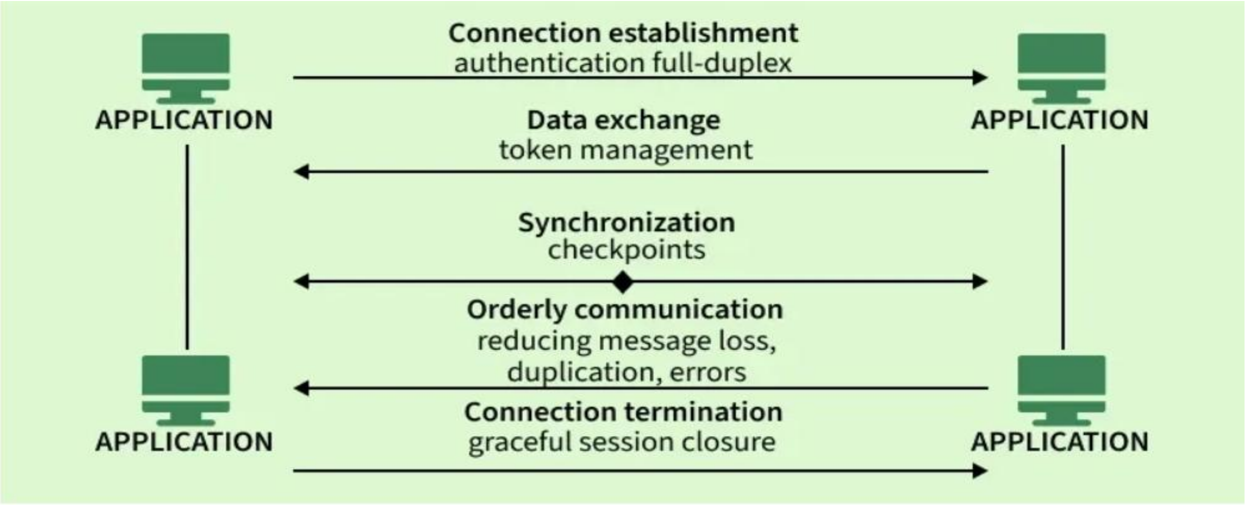
- It ensures that communication remains synchronized and reliable, even during long or complex data transfers.
- It handles dialogue control, deciding whose turn it is to send or receive data.

Note: *In modern TCP/IP networks, some of its functions (like session release and dialogue control) are handled at the Transport Layer (TCP) or Application Layer, reducing the Session Layer's independent role.*

Key Functions of the Session Layer

- **Session Establishment:** Initiates and negotiates communication parameters (e.g., authentication, duplex mode).
- **Communication Synchronization:** Keeps data streams in order using checkpoints.
- **Activity & Dialog Management:** Controls turns, prevents collisions, and avoids duplication.
- **Resynchronization & Recovery:** Recovers from failures using synchronization points.
- **Session Termination:** Gracefully ends communication after all data is exchanged.

Working of the Session Layer



- Establishes and negotiates session parameters (e.g., authentication, duplex mode).
- Manages token-based dialogue control to avoid collisions.
- Inserts synchronization checkpoints for recovery from failures.
- Ensures data integrity by reducing duplication or message loss.
- Gracefully terminates sessions after confirming all data has been exchanged.

Session Layer Protocols

Several protocols and technologies operate at the Session Layer:

- **AppleTalk Data Stream Protocol (ADSP):** Developed by Apple for LAN communication with self-configuration support.
- **Real-time Transport Control Protocol (RTCP):** Provides QoS feedback for RTP-based multimedia sessions.
- **Point-to-Point Tunneling Protocol (PPTP):** Enables Virtual Private Networks (VPNs) over TCP/IP.
- **Password Authentication Protocol (PAP):** Provides password-based user authentication in PPP connections.
- **Remote Procedure Call Protocol (RPCP):** Allows a program to execute procedures in another address space (client-server interaction).
- **Sockets Direct Protocol (SDP):** Supports socket communication over RDMA-enabled networks.

Devices Associated with the Session Layer

- **Firewalls:** Monitor and control sessions for security.
- **Proxy Servers:** Act as intermediaries, managing sessions between clients and servers.
- **Session Border Controllers (SBCs):** Secure and manage VoIP sessions.

- **Application Servers:** Create and maintain user sessions for applications.

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.

Functions of the Presentation Layer

- **Translation:** 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.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Role of the Presentation Layer

When the Application Layer generates data, the Presentation Layer converts it into a standard form that can be transmitted across the network. Similarly, when data is received, it translates it into a format the receiving system can process.

Key highlights:

- Maintains proper syntax and semantics of the data.
- Provides encryption and decryption for secure communication.
- Applies compression techniques to optimize bandwidth usage.
- Ensures compatibility between different systems and devices.

Services Provided by the Presentation Layer

The Presentation Layer ensures smooth and secure data exchange by providing the following services:

- **Compression**: Reduces data size for faster transmission.
- **Encryption/Decryption**: Protects data from unauthorized access.
- **Format Translation**: Converts application-specific data into a standard format.
- **Compatibility**: Makes communication possible between different operating systems and platforms.

Working of the Presentation Layer

- The Presentation Layer works as an intermediary between the Application Layer (Layer 7) and the Session Layer (Layer 5).
- At the sender's end, it formats, encrypts and compresses data received from the Application Layer before sending it to the Session Layer.
- At the receiver's end, it decrypts, decompresses and translates the data into a readable form before delivering it to the Application Layer.

Presentation Layer Protocols

- **Apple Filing Protocol (AFP):** File services protocol for macOS.
- **Lightweight Presentation Protocol (LPP):** Provides ISO presentation services over TCP/IP stacks.
- **NetWare Core Protocol (NCP):** Used in Novell NetWare for file and print services.
- **Network Data Representation (NDR):** Defines data types and representations for network communication.
- **External Data Representation (XDR):** Standard for describing and encoding data across different architectures.

- **Secure Socket Layer (SSL):** Provides encryption and secure communication between web browsers and servers.
- **Transport Layer Security (TLS):** The modern, more secure successor to SSL.

Presentation Layer Attacks

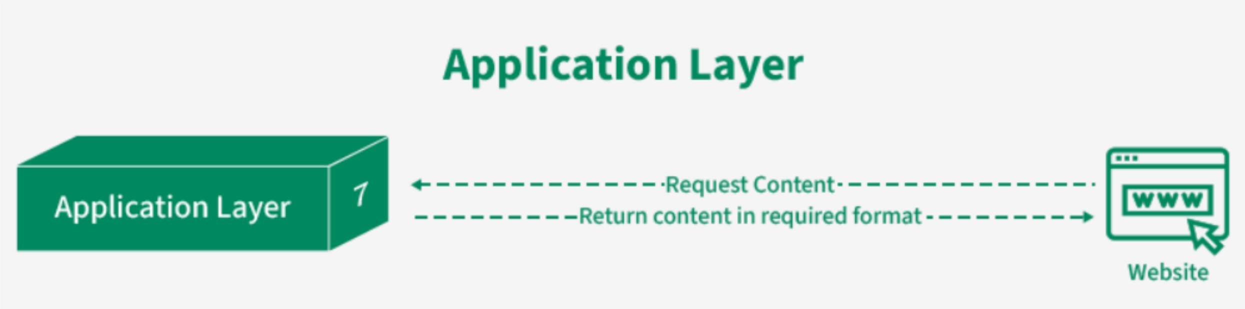
Since this layer deals with data formatting, compression and encryption, it is often targeted by attackers. Common attacks include:

- **Man-in-the-Middle (MITM) Attacks:** Interception of communication to steal sensitive data.
- **SSL/TLS Downgrade Attacks:** Forcing weaker encryption protocols.
- **Certificate Spoofing:** Using fake certificates to impersonate trusted entities.
- **Code Injection:** Exploiting vulnerabilities in data parsing or formatting.

Layer 7: Application Layer

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.



Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

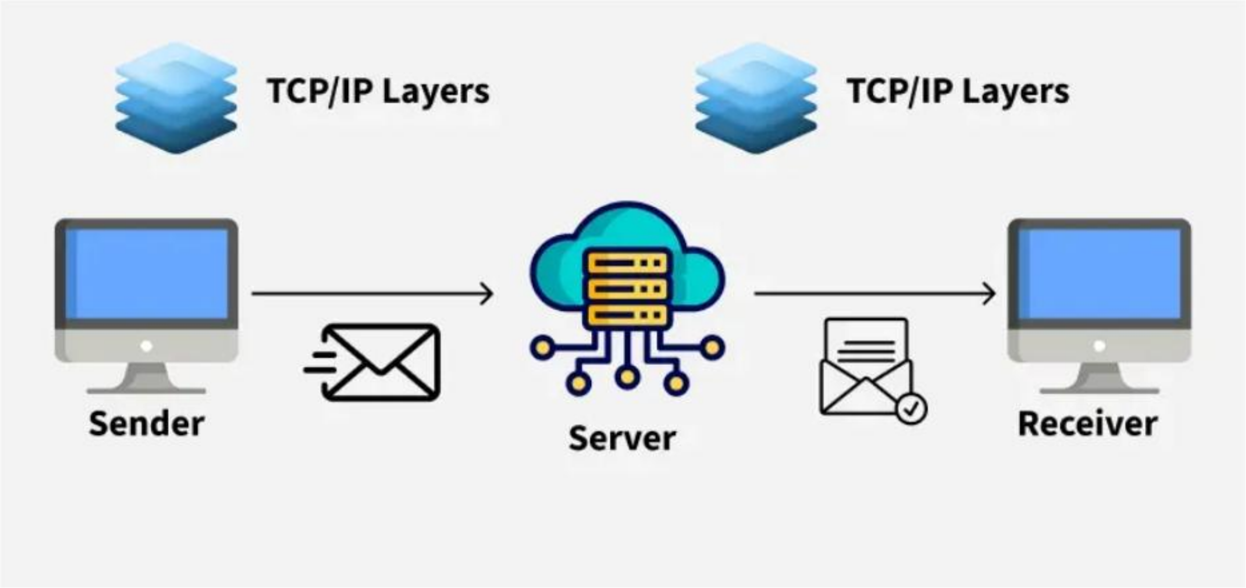
TCP/IP Model

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.

Role of TCP/IP

One of its main goals is to make sure that the data sent by the sender arrives safely and correctly at the receiver's end. To do this, the data is broken down into smaller parts called packets before being sent. These packets travel separately and are reassembled in the correct order when they reach the destination.



Note: *This helps prevent errors and makes sure the message is complete and accurate.*

Layers of TCP/IP Model

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

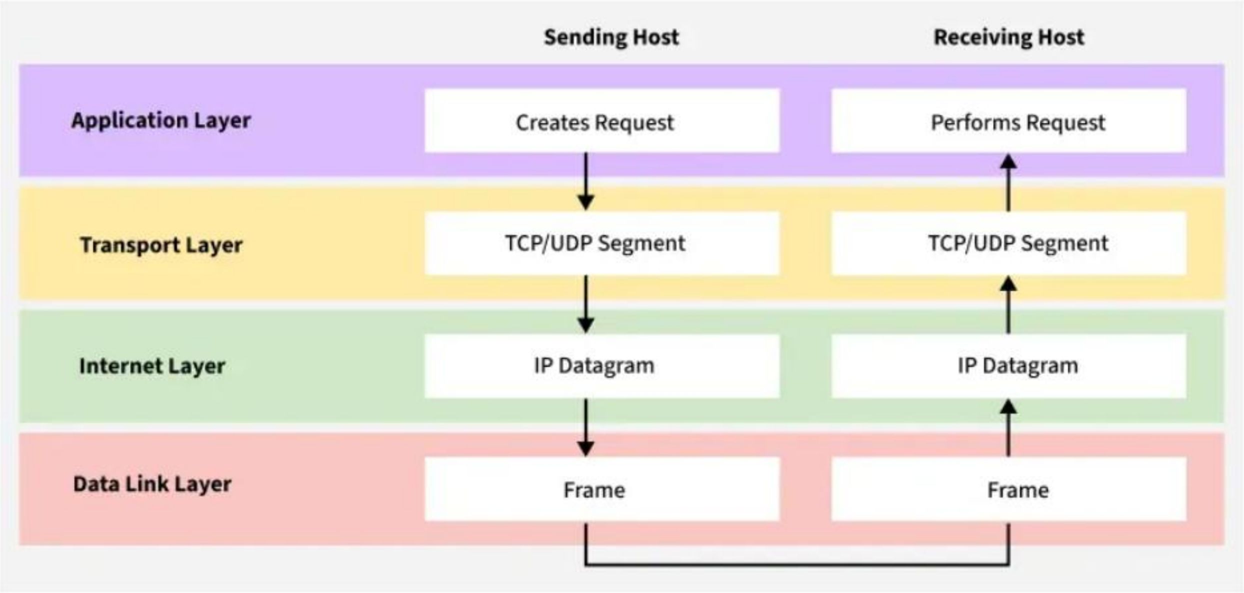
4. Network Access Layer

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.

Working of TCP/IP Model

The working of TCP/IP can be explained with the help of the diagram given below and explained :



When Sending Data (From Sender to Receiver)

- **Application Layer**: Prepares user data using protocols like HTTP, FTP, or SMTP.
- **Transport Layer (TCP/UDP)**: Breaks data into segments and ensures reliable (TCP) or fast (UDP) delivery.
- **Internet Layer (IP)**: Adds IP addresses and decides the best route for each packet.
- **Link Layer (Network Access Layer)**: Converts packets into frames and sends them over the physical network.

When Receiving Data (At the Destination)

- **Link Layer**: Receives bits from the network and rebuilds frames to pass to the next layer.
- **Internet Layer**: Checks the IP address, removes the IP header, and forwards data to the Transport Layer.
- **Transport Layer**: Reassembles segments, checks for errors, and ensures data is complete.
- **Application Layer**: Delivers the final data to the correct application (e.g., displays a web page in the browser).

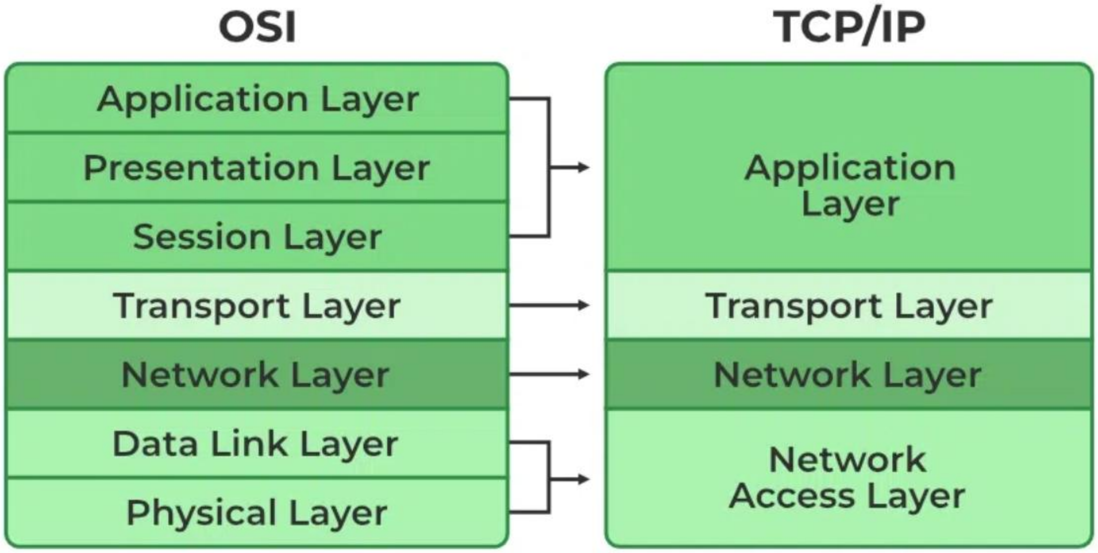
Advantages of TCP/IP Model

- **Interoperability** : The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.
- **Scalability** : TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
- **Standardization** : It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.
- **Flexibility** : The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
- **Reliability** : TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

Disadvantages of TCP/IP Model

- **Security Concerns** : TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
- **Inefficiency for Small Networks** : For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
- **Limited by Address Space** : Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
- **Data Overhead** : TCP the transport protocol, includes a significant amount of overhead to ensure reliable transmission.

How Data Flows When Accessing a Website


OSI
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
TCP/IP
Application Layer
Transport Layer
Network Layer
Network Access Layer