OSI Reference 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.

Layers of the OSI Model

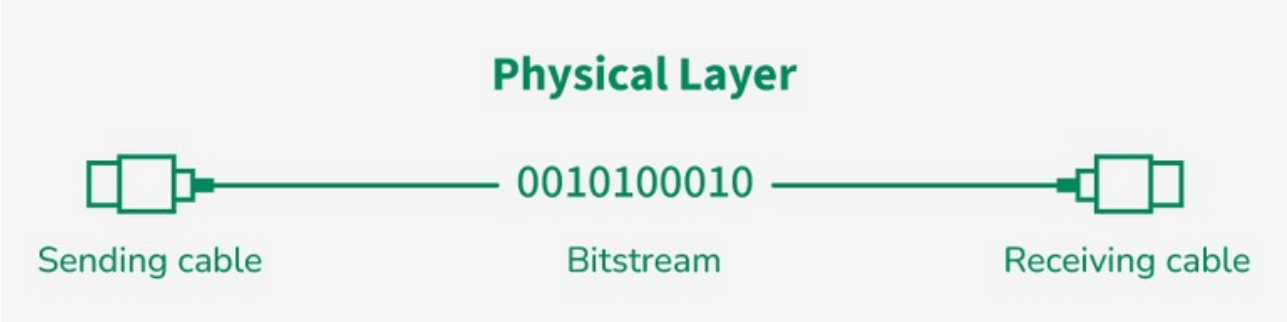
There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

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

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.

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 Data Link Layer is divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

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.

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.

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.

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.

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. For 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

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.

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.

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

Network Virtual Terminal (NVT): It allows a user to log on to a remote host.

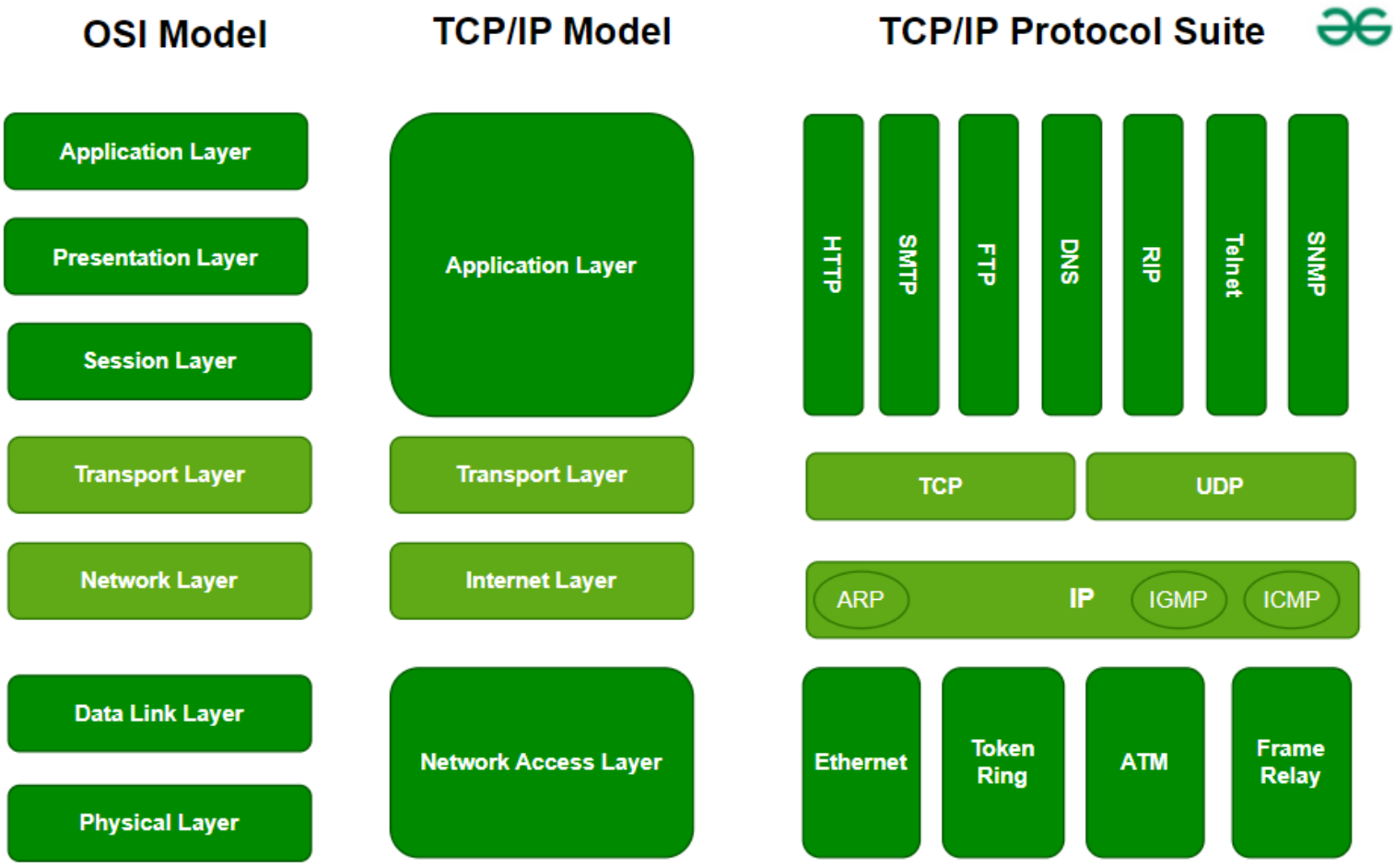
File Transfer Access and Management (FTAM): This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.

Mail Services: Provide email service.

Directory Services: This application provides distributed database sources and access for global information about various objects and services.

Difference Between OSI and TCP/IP Model

OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
OSI model has 7 layers.	TCP/IP model consists of 4 layers.
Package delivery is guaranteed in OSI Model.	Package delivery is not guaranteed in the TCP/IP Model.
In the OSI model, only layers 1,2 and 3 are necessary for data transmission.	All layers of the TCP/IP model are needed for data transmission.
Protocols at each layer is independent of the other layer.	Layers are integrated; some layers are required by other layers of TCP/IP model.
OSI Model is a conceptual framework, less used in practical applications.	Widely used in actual networks like Internet and Communication Systems.



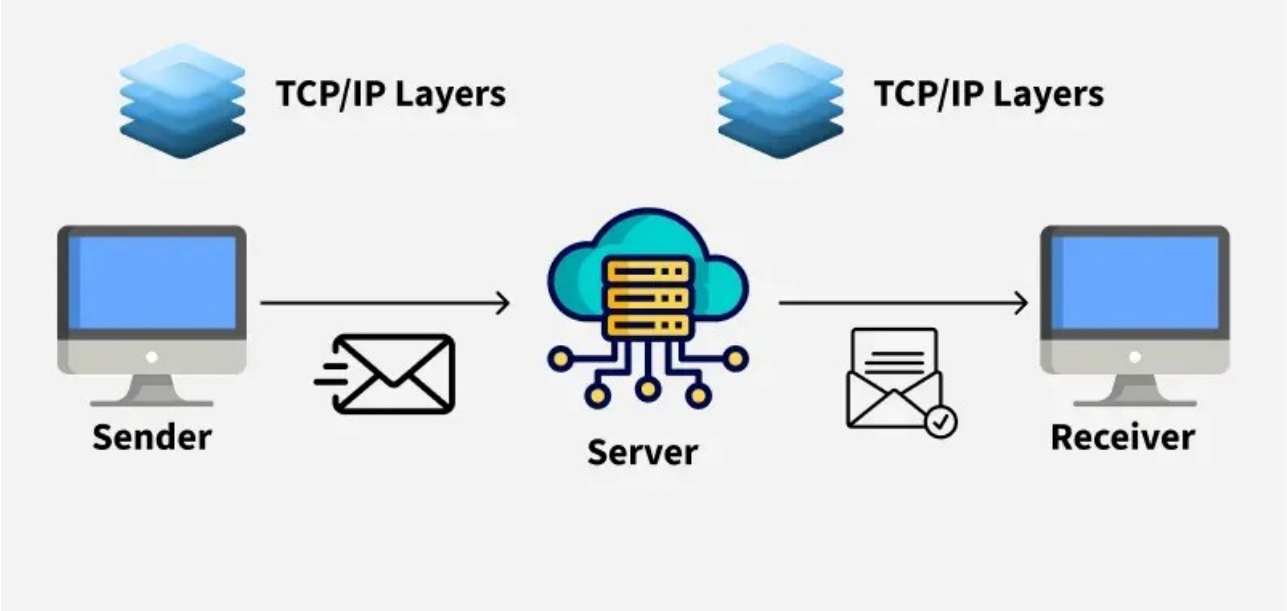
The TCP/IP model is a framework that is used to model the communication in a network. It is mainly a collection of network protocols and organization of these protocols in different layers for modeling the network.

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. 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.