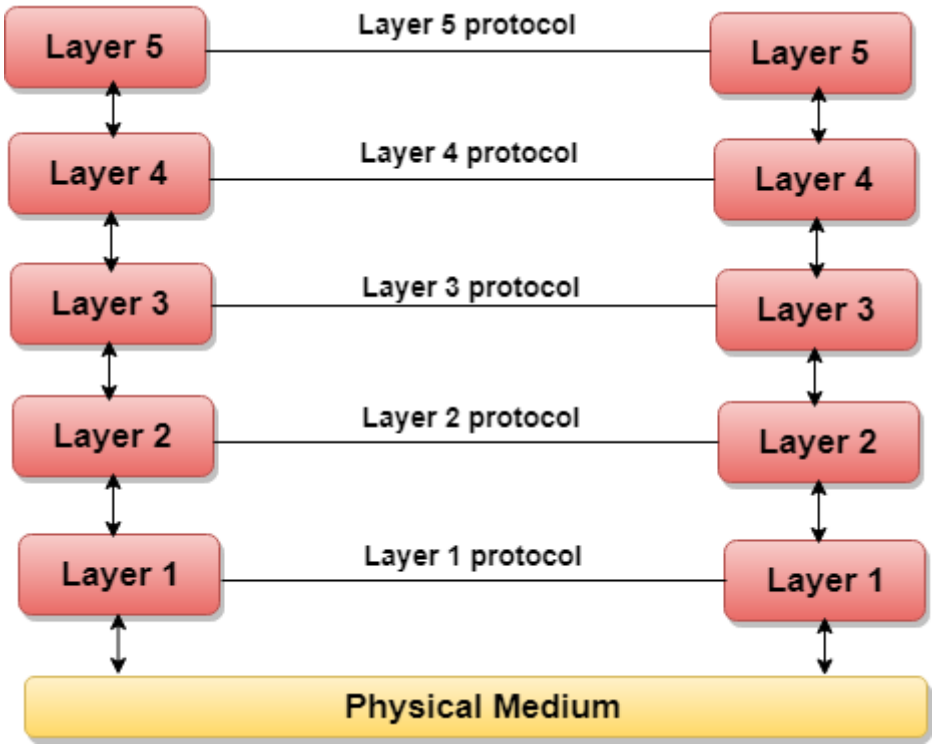
Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task.

Layered Architecture



- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a

higher layer and hiding the details from the layers of how the services are implemented.

- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.
- n case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Requirement of Layered architecture

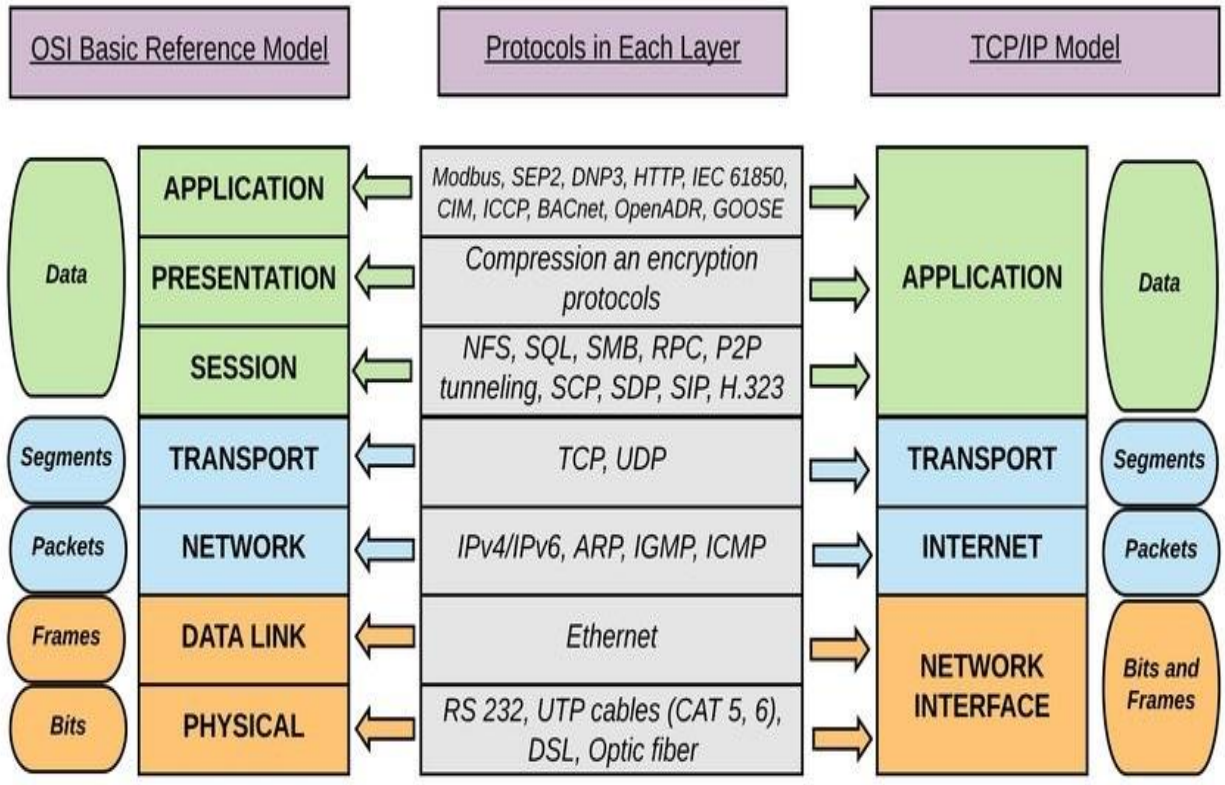
- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

OSI Model:

OSI stands for Open Systems Interconnection. It was developed by ISO – 'International Organization for Standardization', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. Each layer has a specific function and is responsible for specific aspects of communication.

The layers are:

- **Physical:** This layer deals with the physical components of the network, such as cables and network devices.
- **Data Link:** This layer manages the transfer of data between devices on the same network segment.
- **Network:** This layer routes data from one network to another.
- **Transport:** This layer ensures reliable delivery of data between endpoints.
- **Session:** This layer establishes and manages sessions between applications.
- **Presentation:** This layer formats and encrypts data for the application layer.
- **Application:** This layer provides the interface between the network and the end-user applications.



TCP/IP

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

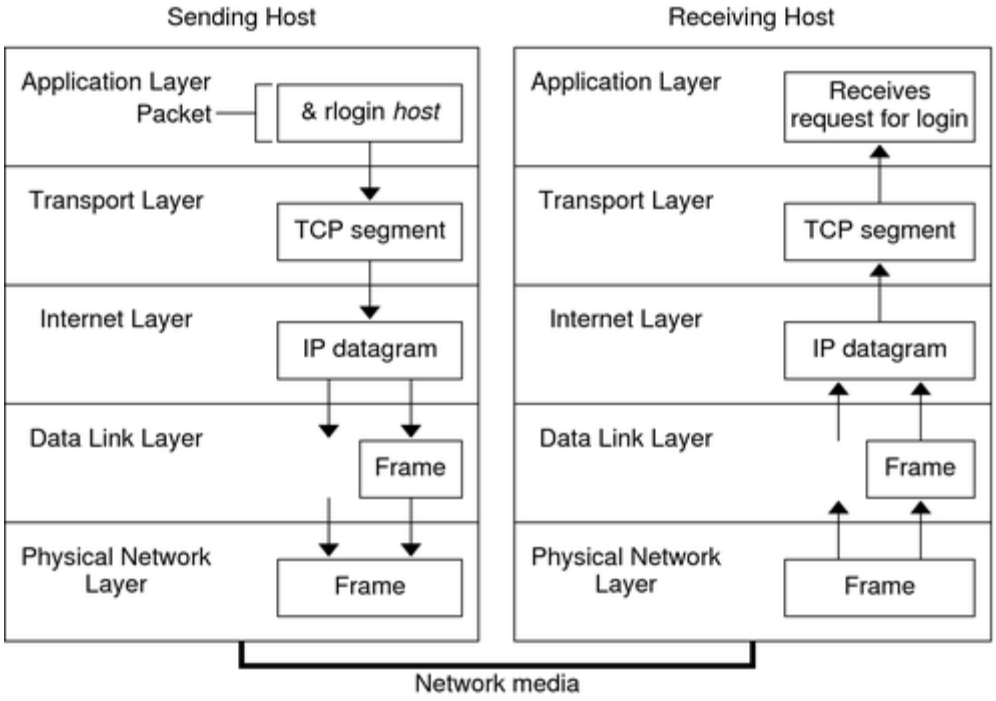
Work of TCP/IP

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

- **IP addressing** – The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.
- **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system's IP address.
- **Packet formatting** – IP assembles packets into units that are known as **datagrams**. Datagrams are fully described in Internet Layer: Where Packets Are Prepared for Delivery.
- **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.



TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets.

This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a "reliable, connection-oriented" protocol.

Difference between the TCP and IP

The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP.

1. **Link Layer**- The Link Layer deals with transmitting data over physical connections.
2. **Internet Layer -** The Internet Layer routes data packets between networks.
3. **Transport Layer -** The Transport Layer ensures reliable transmission of data.
4. **Application Layer** - The Application Layer provides interfaces for various applications to communicate using the underlying transport protocols.

Advantages of TCP/IP Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is widely used for communication on the internet and other computer networks.

Some of the advantages of the TCP/IP model include the following:

- **Wide Adoption:** TCP/IP is the foundation of the internet and is widely used in a variety of networks and communication systems.
- **Simplicity:** The TCP/IP model is relatively simple compared to other network models, making it easier to understand and implement.
- **Scalability:** TCP/IP is designed to be scalable and can accommodate growth and changes in network size and complexity.
- **Interoperability:** TCP/IP is designed to be flexible and interoperable, allowing different networks and systems to communicate with each other.
- **Robustness:** TCP/IP is designed to be robust and reliable, ensuring the delivery of data even in the presence of network errors and failures.

- **Flexibility:** The TCP/IP model is flexible and allows for the integration of new technologies and applications into existing networks.

Disadvantages of TCP/IP Model

The TCP/IP model has several disadvantages:

- **Complexity:** The TCP/IP model has a complex structure with multiple layers, protocols, and standards, making it difficult for novice users to understand and implement.
- **Security:** Although it provides some security measures, it is still vulnerable to attacks such as hacking, malware, and denial-of-service (DoS) attacks.
- **Scalability:** As the number of internet-connected devices increases, the TCP/IP model may become less scalable and unable to accommodate the growing demands placed on it.
- **Performance:** The TCP/IP model's performance can be affected by network congestion, outdated protocols, and slow transmission speeds.
- **Flexibility:** The TCP/IP model is not very flexible, and changing or updating protocols can cause compatibility issues with existing systems.

Difference between TCP/IP and OSI Model

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.
TCP/IP model network layer only provides	Connectionless and connection-oriented

TCP/IP	OSI
connectionless (IP) services. The transport layer (TCP) provides connections.	services are provided by the network layer in the OSI model.