Protocol Layers: Introduction, Layered Architecture, The Internet protocol stack, Network entities and Layers.

Layered Architecture :

Q-1. Why it is necessary to have layering in a network?

- A computer network is a very complex system. It becomes very difficult to implement as a single entity.
- The layered approach divides a very complex task into small pieces each of which is independent of others and it allow a structured approach in implementing a network.
- The basic idea of a layered architecture is to divide the design into small pieces.
- Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications.

Q-2. What are the key benefits of layered network?

- Complex systems can be broken down into understandable subsystems.
- Any facility implemented in one layer can be made visible to all other layers.
- Services offered at a particular level may share the services of lower level.
- Each layer may be analyzed and tested independently.
- Layers can be simplified, extended or deleted at any time.
- Increase the interoperability and compatibility of various components build by different vendors.

Architecture models are *OSI Reference Model and TCP/IP Reference Model*

layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

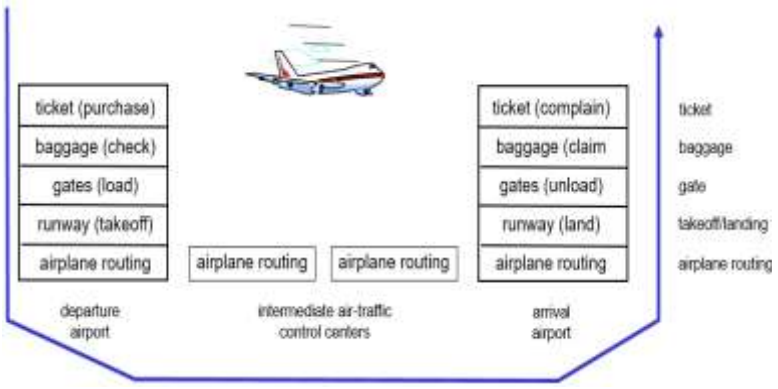


Fig. Layering of airline functionality

ISO-OSI Model:

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication **ISO (International Organization of Standardization.)** developed this model. This is called a model for **Open System Interconnection (OSI)** and is normally called as OSI model. OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system.

Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Protocol Data Unit (PDU) :

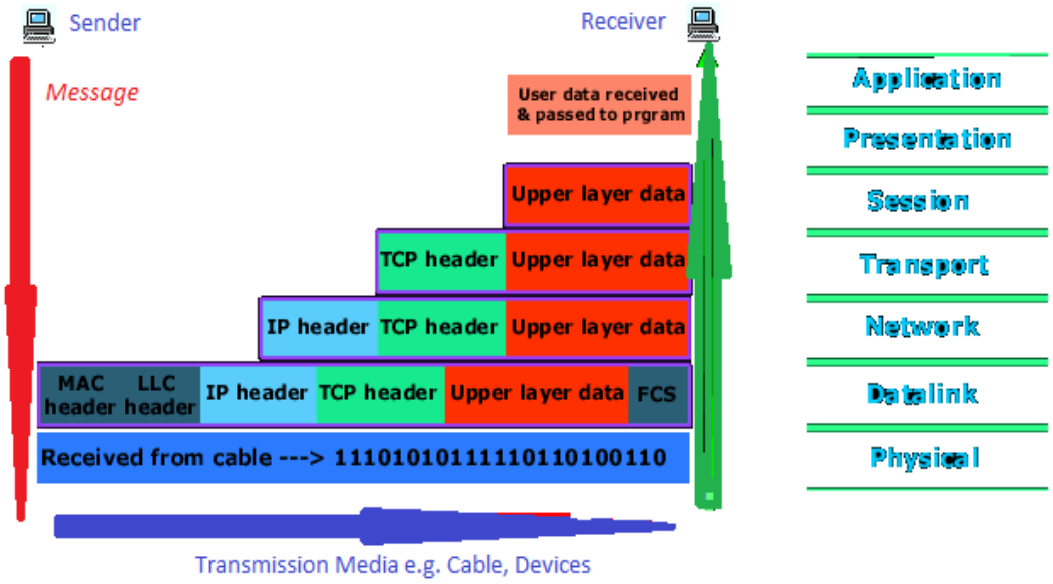
- **In telecommunications Information** that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data, also known as a service data unit (SDU).
- **In a layered system**, a unit of data which is specified in a protocol of a given layer and which consists of protocol-control information and possibly user data of that layer. For example: Bridge PDU or iSCSI PDU

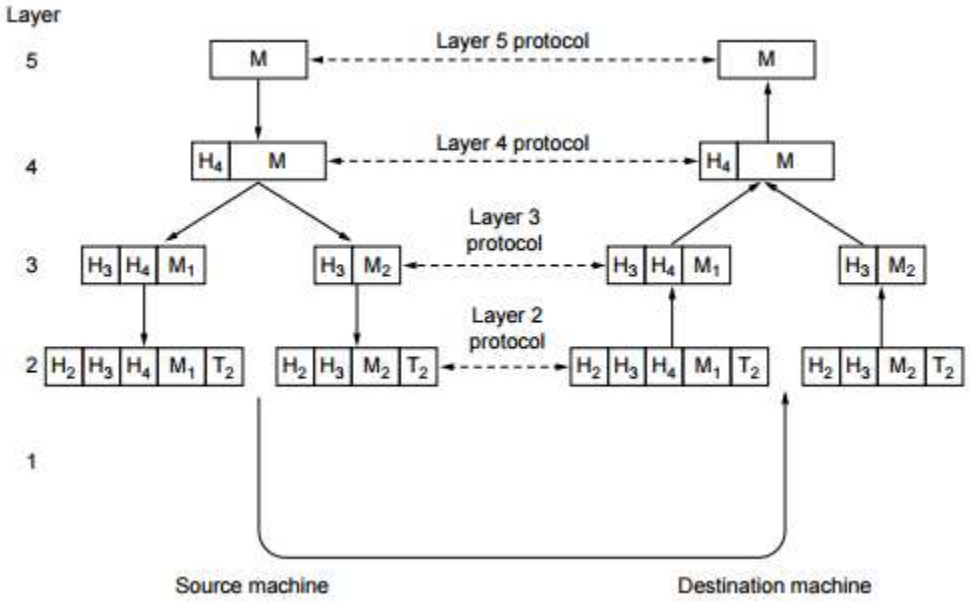
Protocol Control Information(PCI) :

- **In telecommunication**, The queries and replies among communications equipment to determine the respective capabilities of each end of the communications link.
- **For layered systems**, information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation.

DATA ENCAPSULATION & DECAPSULATION IN THE OSI MODEL

Decapsulation is the process of opening up **encapsulated** data that are usually sent in the form of packets over a communication network. It can be literally defined as the process of opening a capsule, which, in this case, refers to **encapsulated** or wrapped-up data.





Header and Trailer

- Like a web page, header is the upper portion of page and trailer is lower portion of page after main body.
- In data communication, header is the upper part of packet and trailer is lower part of packet which carries the source and destination addresses, synchronization points, information for error detection, etc.
- Is control data added at the beginning and the end of each data unit at each layer of the sender and removed at the corresponding layers of the receiver

Perspective on the OSI Architecture

The annotation along the right-side suggests viewing the seven layers in three parts. The lower three layers contain the logic for a computer to interact with a network. The host is attached physically to the network, uses a data link protocol to reliably communicate with the network, and uses a network protocol to request data exchange with another device on the network and to request network services. Continuing from this perspective, the transport layer provides a reliable end-to-end service regardless of the intervening network facility; in effect, it is the user's liaison to the communications facility. Finally, the upper three layers, taken together, are involved in the exchange of data between end users, making use of a transport service for reliable data transfer.

Another perspective is suggested by the annotation to the left. The lower two layers deal with the link between the host and the network. The next three layers are all involved in transferring data from one host to another: The network layer makes use of the communication network facilities to transfer data from one host to another; the transport layer assures that the transfer is reliable; and the session layer manages the flow of data over the logical connection. Finally, the upper two layers are oriented to the user's concerns, including considerations of the application to be performed and any formatting issues.

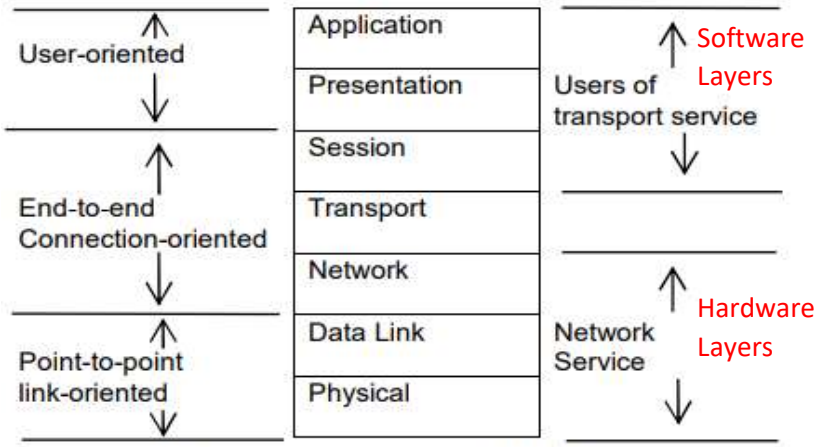


Fig. Perspective on the OSI Architecture.

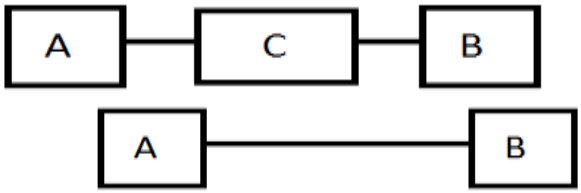


Fig. End-to-End Connection

Fig. Point-to-Point Connection

- **END TO END NETWORK**

The end-to-end principle is a design framework in computer networking. In computer networking according to this principle, application-specific features reside in the communicating end nodes of the network, rather than in intermediary nodes, such as gateways and routers that exist to establish the network.

- **POINT TO POINT NETWORK**

Point-to-point network topology is a simple topology that displays the network of exactly two hosts (computers, servers, switches or routers) connected with a cable. Point-to-point topology is widely used in the computer networking and computer architecture. It is also used in the telecommunications systems when we speak about the communication connection of two nodes or endpoints.

ISO-OSI 7 Layers :-

1.PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium e.g Cable-Ethernet, Fibre. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station defines a frame
- Physical medium attachment, accommodating various possibilities in the medium:
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
  - What physical medium options can be used
  - How many volts/db should be used to represent a given signal state, using a given physical medium

Example :- The data is finally transferred onto the network medium at the Physical layer, in the form of raw bits. Signaling and encoding mechanisms are defined at this layer, as is the hardware that forms the physical connection between the client and the web server

2.DATA LINK LAYER

The data link layer provides framing and error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. operations package and unpack the data in frames. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

Example :- Data cannot be sent directly to a logical address. As packets travel from network to network, IP addresses are translated to hardware addresses, which are a function of the Data-Link layer. The packets are encapsulated into frames to be placed onto the physical medium.

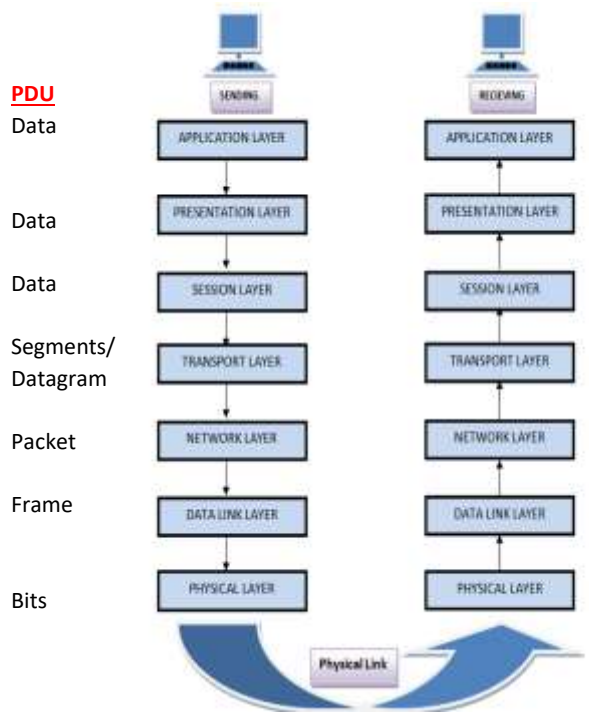


Fig. OSI 7 Layers

OSI model Protocol Suits
7. Application layer NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet, DHCP, Netconf
6. Presentation layer MIME, XDR
5. Session layer Named pipe, NetBIOS, SAP, PPTP, RTP, SOCKS, SPDY
4. Transport layer TCP, UDP, SCTP, DCCP, SPX
3. Network layer IP , IPv4, IPv6, ICMP, IPsec, IGMP, IPX, AppleTalk, X.25 PLP
2. Data link layer ATM, ARP, IS-IS, SDLC, HDLC, CSLIP, SLIP, GFP, PLIP, IEEE 802.2, LLC, MAC, L2TP, IEEE 802.3, Frame Relay, ITU-T G.hn DLL, PPP, X.25 LAPB, Q.921 LAPD, Q.922 LAPF
1. Physical layer EIA/TIA-232, EIA/TIA-449, ITU-T V-Series, I.430, I.431, PDH, SONET/SDH, PON, OTN, DSL, IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, ITU-T G.hn PHY, USB, Bluetooth, RS-232, RS-449,

3.NETWORK LAYER

The network layer controls the operation of the subnet, routing : deciding which physical path the data should take based on network conditions, priority of service. Handles packet routing via logical addressing and switching functions. It provides:

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's Maximum Transmission Unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses

Example **:-** The best path to route the data between the client and the web server is determined by IP, a Network layer protocol. IP is also responsible for the assigned logical addresses on the client and server, and for encapsulating segments into packets.

4.TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. provides quality of service (QoS) functions and ensures the complete delivery of the data. The integrity of the data is guaranteed at this layer via error correction and similar functions. The transport layer provides:

- Message segmentation*:* accepts a message from the (session) layer above it, **splits** the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station **reassembles** the message.
- Message acknowledgment*:* provides **reliable end-to-end** message delivery with acknowledgments.
- Message traffic control*:* tells the transmitting station to **"back-off"** when no message buffers are available.
- Session multiplexing*:* multiplexes several message streams, or sessions **onto one logical link** and keeps track of which messages belong to which sessions (see session layer).

Example :- HTTP utilizes the TCP Transport layer protocol to ensure the reliable delivery of data. TCP establishes and maintains a connection from the client to the web server, and packages the higher-layer data into segments. A sequence number is assigned to each segment so that data can be reassembled upon arrival.

5.SESSION LAYER or PORT LAYER

Handles authentication and authorization functions. It also manages the connection between the two communicating end points, establishing a connection, maintaining the connection, and ultimately terminating it. The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

For Internet applications, each session is related to a particular port, a number that is associated with a particular upper layer application. For example, the HTTP program or daemon always has port number 80. The port numbers associated with the main Internet applications are referred to as well-known port numbers. Most port numbers, however, are available for dynamic assignment to other applications.

Example :- The Session layer is responsible for establishing, maintaining, and terminating the session between devices, and determining whether the communication is half-duplex or full-duplex. However, the TCP/IP stack generally does not include session-layer protocols, and is reliant on lower-layer protocols to perform these functions.

6.PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station. The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

7.APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access, printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

Example : The Internet can provide data in a wide variety of formats, a function of the Presentation layer. Common formats on the Internet include HTML, XML, PHP, GIF, and JPEG. Any encryption or compression mechanisms used on a website are also considered a Presentation layer function.

TCP/IP REFERENCE Model

TCP/IP protocols map to a four-layer conceptual model known as the ***DARPA model*** , named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.

IP is the clerk - *deals with addressing of packets like mapping the logical/network address to MAC address.*

TCP is the postman *which deals with delivering the data packets to various hosts over the internet. It is dependent on the IP. Provides services like Flow control , error detection and correction.*

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

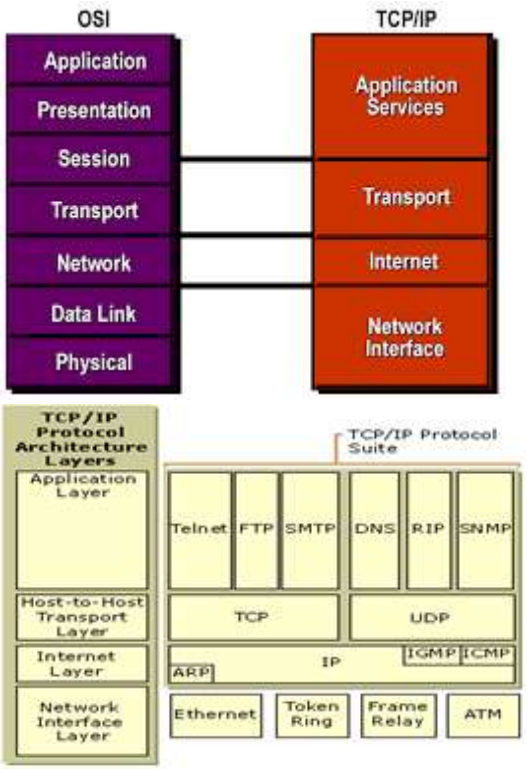


Fig. TCP/IP Protocol Architecture

TCP/IP protocol suite

Application layer

BGP, DHCP, DNS, FTP, HTTP, IMAP, LDAP, MGCP, NNTP, NTP, POP, ONC/RPC, RTP, RTSP, RIP, SIP, SMTP, SNMP, SSH, Telnet, TLS/SSL, XMPP

Transport layer

TCP, UDP, DCCP, SCTP, RSVP

Internet layer

IP , IPv4, IPv6, ICMP, ICMPv6, ECN, IGMP, IPsec

Link layer

ARP, NDP, OSPF, Tunnels , L2TP, PPP, MAC , Ethernet, DSL, ISDN, FDDI,

1.Network Interface Layer : Deals with all physical components of network connectivity between the network and the IP protocol.

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model.

2.Internet Layer : Contains all functionality that manages the movement of data between two network devices over a routed network. The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (**IP**) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (**ARP**) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (**ICMP**) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The *Internet Group Management Protocol* (**IGMP**) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

3.Transport Layer (Host-to-Host): Manages the flow of traffic between two hosts or devices, ensuring that data arrives at the application on the host for which it is targeted. The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- **TCP** provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- **UDP** provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

4.Application Layer : Acts as final endpoints at either end of a communication session between two network hosts(Sender, Receiver). The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (**HTTP**) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (**FTP**) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (**SMTP**) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (**DNS**) is used to resolve a host name to an IP address.
- The Routing Information Protocol (**RIP**) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (**SNMP**) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Comparison of OSI and TCP/ IP model

OSI (Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol

8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers
11. Layer was first developed than protocol	11. Protocol were first developed than layer

Internet Protocol Stack

A protocol stack refers to a group of protocols that are runnning concurrently that are employed for the implementation of network protocol suite.

The protocols in a stack determine the interconnectivity rules for a layered network model such as in the OSI or TCP/IP models. To become a stack the protocols must be interoperable being able to connect both vertically between the layers of the network and horizontally between the end-points of each transmission segment.

A set of network protocol layers that work together. The OSI Reference Model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the internet.

The term *stack* also refers to the actual software that processes the protocols. So, for example, programmers sometimes talk about *loading a stack*, which means to load the software required to use a specific set of protocols. Another common phrase is *binding a stack*, which refers to linking a set of network protocols to a network interface card (NIC). Every NIC must have at least one stack bound to it.