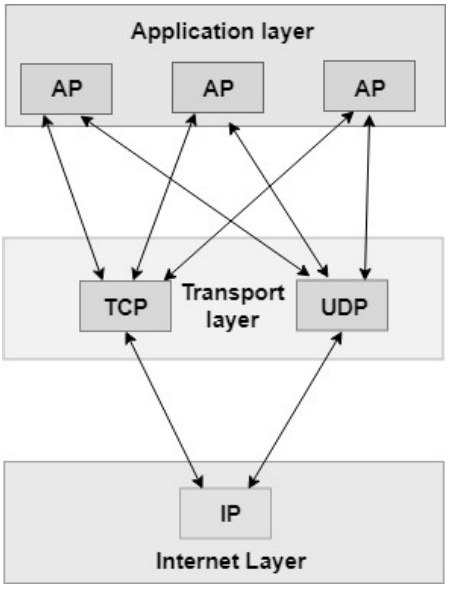
Unit-3

Transport Layer:

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees and delay guarantees.
- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.



Services provided by the Transport Layer:

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

1. End-to-end delivery
2. Addressing
3. Reliable delivery
4. Flow control
5. Multiplexing

End-to-end delivery:

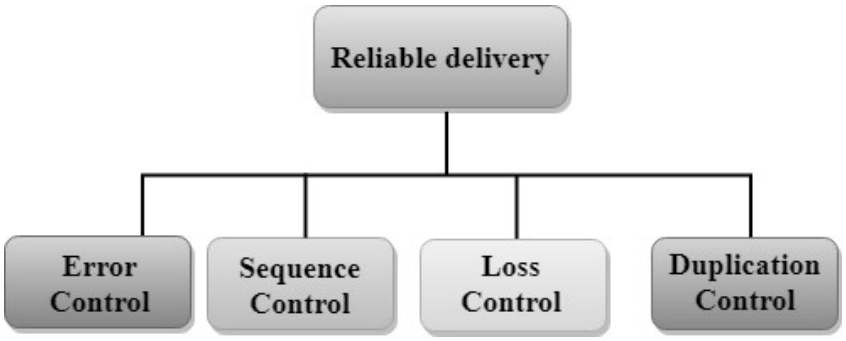
The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

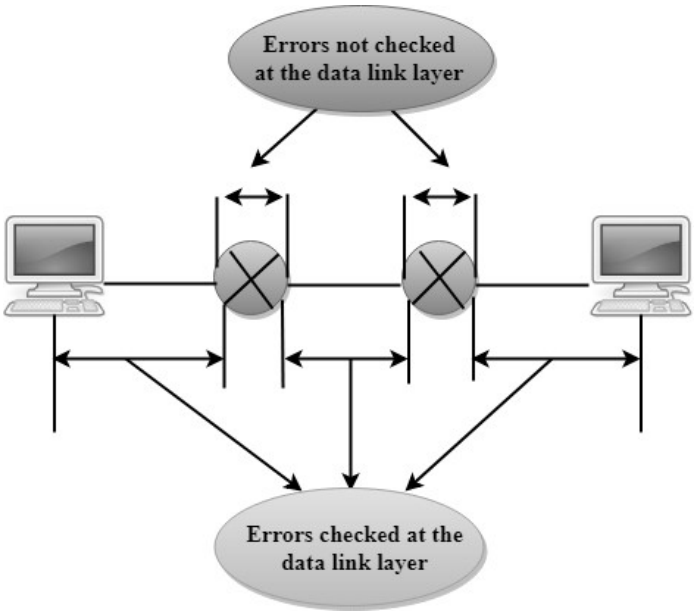
1. Error control
2. Sequence control
3. Loss control
4. Duplication control



Error Control:

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.

- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.



Sequence Control:

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control:

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver's transport layer to identify the missing segment.

Duplication Control:

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control:

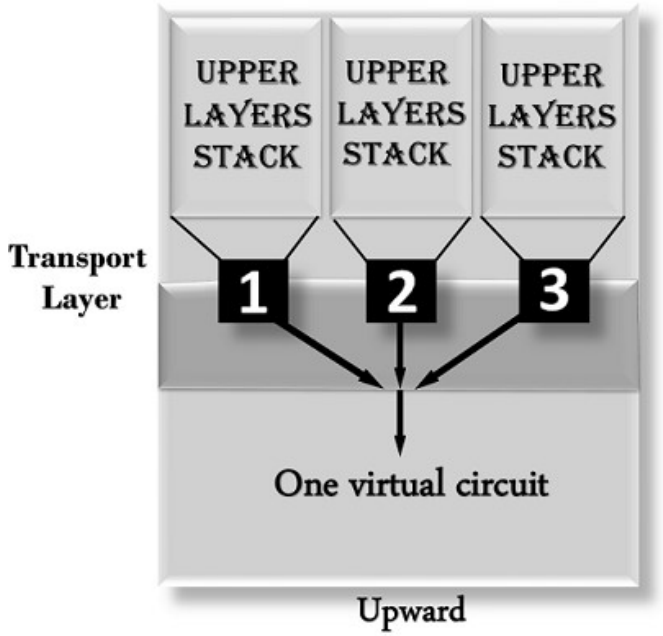
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing:

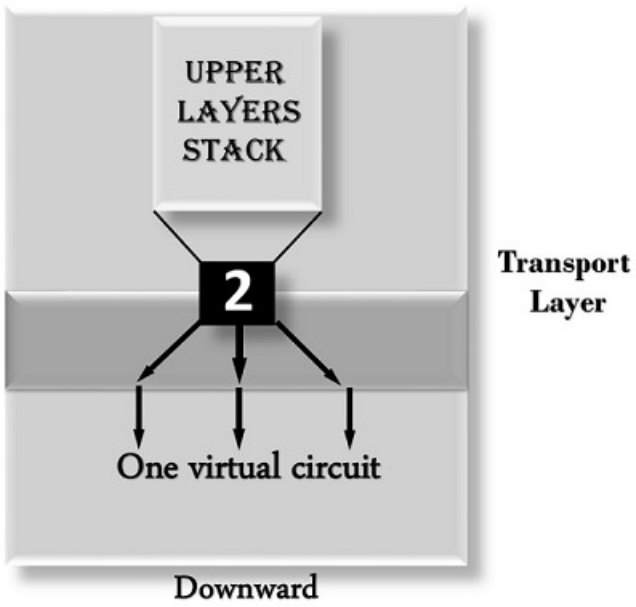
The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

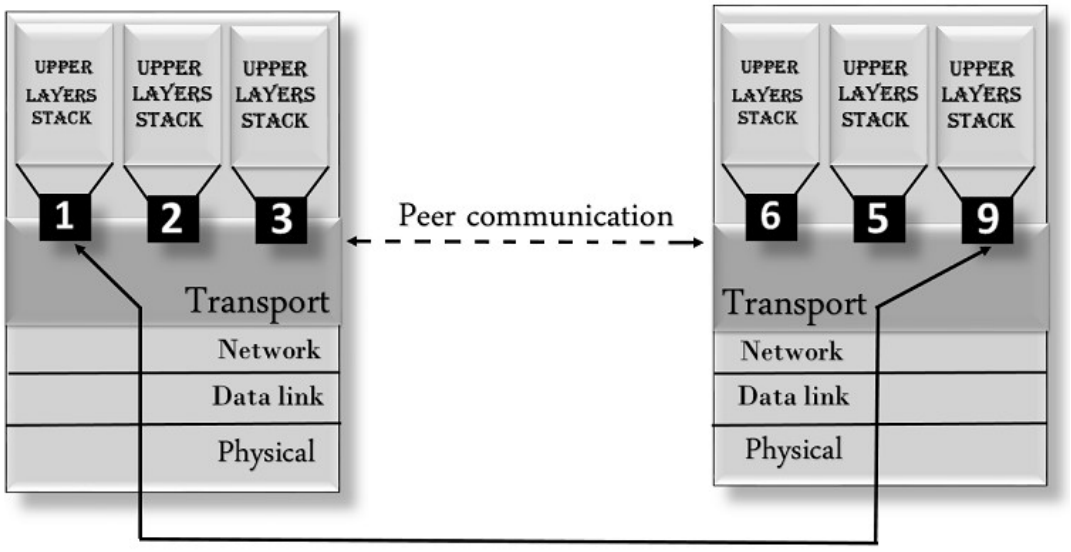


- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



Addressing:

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.



Elements of Transport Protocol:

To establish a reliable service between two machines on a network, transport protocols are implemented, which somehow resembles the data link protocols implemented at layer 2. The major difference lies in the fact that the data link layer uses a physical channel between two routers while the transport layer uses a subnet.

Following are the issues for implementing transport protocols:

Types of Service:

The **transport layer** also determines the type of service provided to the users from the **session layer**. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer.

Error Control:

Error detection and error recovery are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis. To control errors from lost or duplicate segments, the transport layer enables unique segment sequence numbers to the different packets of the message, creating virtual circuits, allowing only one virtual circuit per session.

Flow Control:

The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. The transport layer enables a fast process to keep pace with a slow one. Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms are used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.

Connection Establishment/Release:

The transport layer creates and releases the connection across the network. This includes a naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables us to establish and delete connections across the network to multiplex several message streams onto one communication channel.

Multiplexing/Demultiplexing:

The transport layer establishes a separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections. When the issue of throughput is not important, it multiplexes several transport connections onto the same network connection, thus reducing the cost of establishing and maintaining the network connections.

When several connections are multiplexed, they call for demultiplexing at the receiving end. In the case of the transport layer, the communication takes place only between two processes and not

between two machines. Hence, communication at the transport layer is also known as peer-to-peer or process-to-process communication.

Fragmentation and re-assembly:

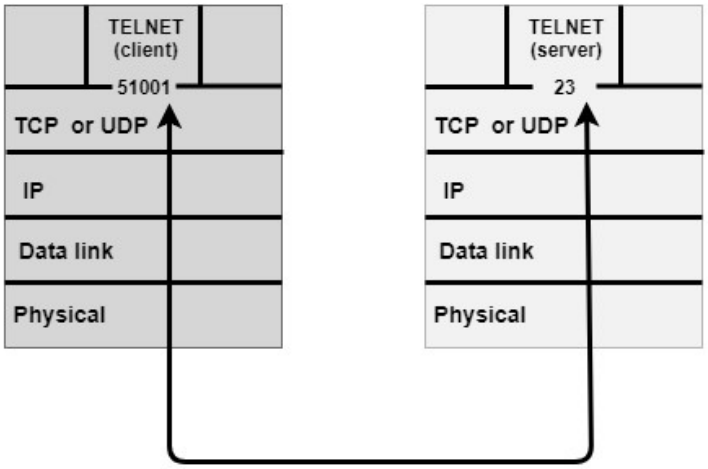
When the transport layer receives a large message from the session layer, it breaks the message into smaller units depending upon the requirement. This process is called fragmentation. Thereafter, it is passed to the network layer. Conversely, when the transport layer acts as the receiving process, it reorders the pieces of a message before reassembling them into a message.

Addressing:

Transport Layer deals with addressing or labeling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame, so the receiving device knows which process it has been sent from. This helps in keeping track of multiple-message conversations. Ports or sockets address multiple conservations in the same location.

Transport Layer Protocols:

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments; an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services and from IP services to the destination port.
- Each port is defined by a positive integer address and it is of 16 bits.

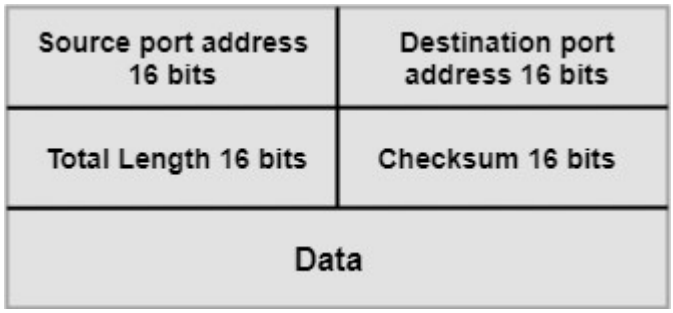


UDP:

- ✓ UDP stands for **User Datagram Protocol**.
- ✓ UDP is a simple protocol and it provides non-sequenced transport functionality.
- ✓ UDP is a connectionless protocol.
- ✓ This type of protocol is used when reliability and security are less important than speed and size.
- ✓ UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- ✓ The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format:

The user datagram has a 16-byte header which is shown below:



Where,

- ➢ **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- ➢ **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- ➢ **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- ➢ **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol:

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP:

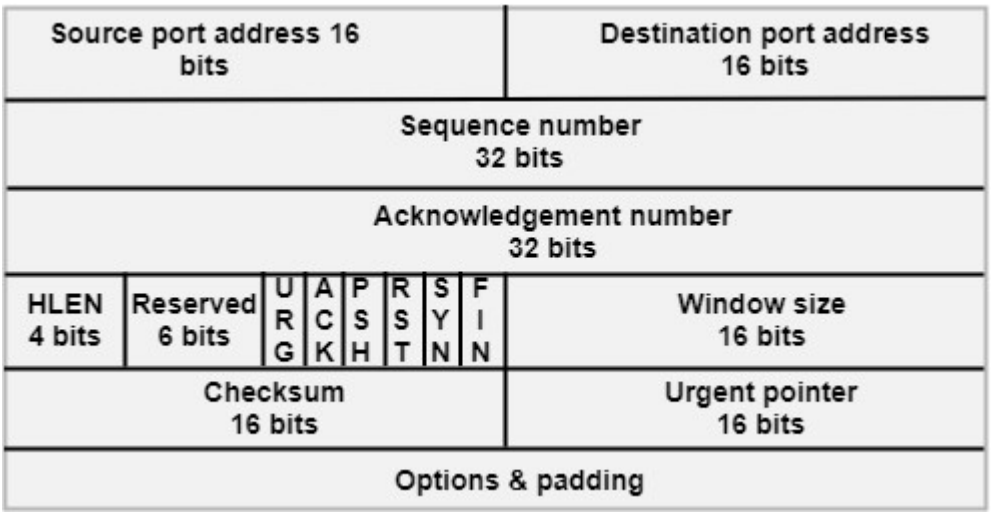
- o TCP stands for Transmission Control Protocol.
- o It provides full transport layer services to applications.

- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features of TCP protocol:

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  1. Establish a connection between two TCPs.
  2. Data is exchanged in both the directions.
  3. The Connection is terminated.

TCP Segment Format:



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.

- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set) and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
    - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

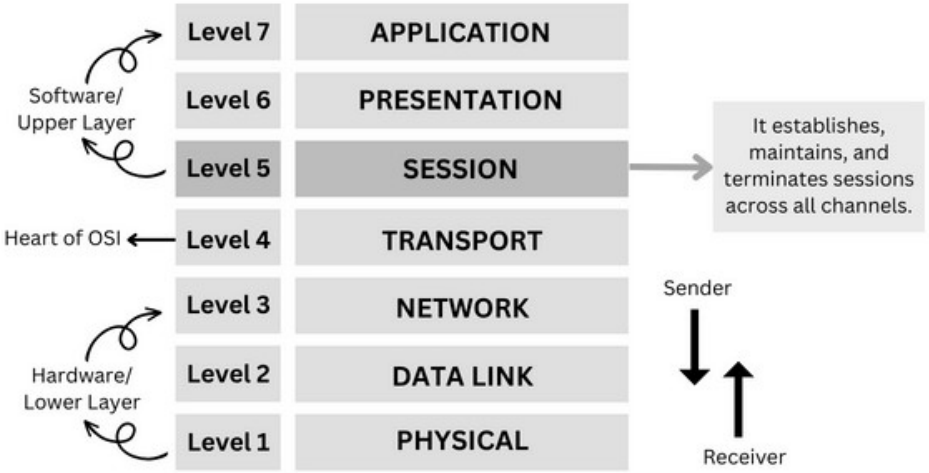
Differences b/w TCP & UDP:

Basis for Comparison	**TCP**	**UDP**
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	Slow	High
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor does it retransmit the damaged frame.

Session Layer:

The session layer is Layer 5 layer from the bottom in the OSI model. The job of the session layer is to control and maintain connections between systems to share data. It establishes, maintains and ends sessions across all channels. In case of a network error, it checks the authenticity and provides recovery options for active sessions. It manages sessions and synchronizes data flow.

Basically, this layer regulates when computers can send data and how much data they can send. Essentially it coordinates communication between devices.



The OSI Model: Session Layer

Functions of the Session Layer:

Session Establishment: The session layer establishes connections between devices which is known as sessions. The session which is created allows users to share data, remote access and file management. When the session is released, the transport connection is mapped. The ways in which transport connection maps are one-to-many, one-to-one and many-to-one.

Data Transfer: It is the very basic function of the session layer, which handles the exchange of data between systems in a full-duplex or half-duplex mode of transmission. The session layer allows only one user to transmit data in half-duplex as well as exchange data in full-duplex mode.

Dialog Management: The session layer keeps log data on which connections are established to transmit and receive data, which is called dialog management. It is accountable for establishing, synchronizing, preserving and ending the conversation between the sender and the receiver. It uses a token mechanism in which the user sharing the data is given a token in case of half duplex mode and, after the exchange, transfers it to another device. The token method maintains the efficiency of the connection.

Synchronization: The session maintains proper connectivity between systems, and if any error occurs, then it provides a recovery option which is called a known state. The session layer adds synchronization bits to the message to use the known state in the event of an error. These bits can be used as checkpoints. It adds synchronization points or checkpoints to the data stream for longer communication. It ensures that the data streams are successfully received and acknowledged up to the checkpoints. In case of any failure, only the stream needs to be retransmitted after the checkpoints.

Authentication: The process of identification is known as authentication. It takes a guarantee from the user to permit them access to the data. Authentication is very important because it provides security.

Authorization: It grants privileges after authentication of the user. Authorization means providing access to the data that is authorized to the specific user.

Protocols of the Session Layer:

The session layer offers many network protocols for the safety, security and efficiency of communication between devices.

Some of these protocols are discussed below:

RTCP: It is an abbreviation for Real-time Transport Control Protocol. It is used to provide audio and video over the Internet. Basically, it periodically transmits control packets to all participants in the session. It provides feedback on QoS (Quality of Service) to all participants in the session. It is used in video conferencing, television services, etc.

PPTP: It is the full form of Point-to-Point Tunneling Protocol. This is the technology used to implement VPN. With the help of PPTP, data can be transmitted securely from one node to another through a tunnel.

PAP: It is an abbreviation for Password Authentication Protocol. The point-to-point protocol uses it to authenticate the user. It takes care of whether the user is authentic or not and then grants access. It works in such a way that the user will enter the id and password, then after the authentication, the server will reply with a confirmation. It is a weak type of authentication system as it is highly vulnerable to attackers.

ADSP: It is an abbreviation for AppleTalk Data Stream Protocol. It is a networking protocol that was introduced 38 years ago, in 1985, and was created for Apple Macintosh networks. It allows users to share printers and folders for access by other network users.

RPC: It is an abbreviation for Remote Procedure Call Protocol. It helps in communication between processes that are residing in different systems connected over a network. It helps one program to

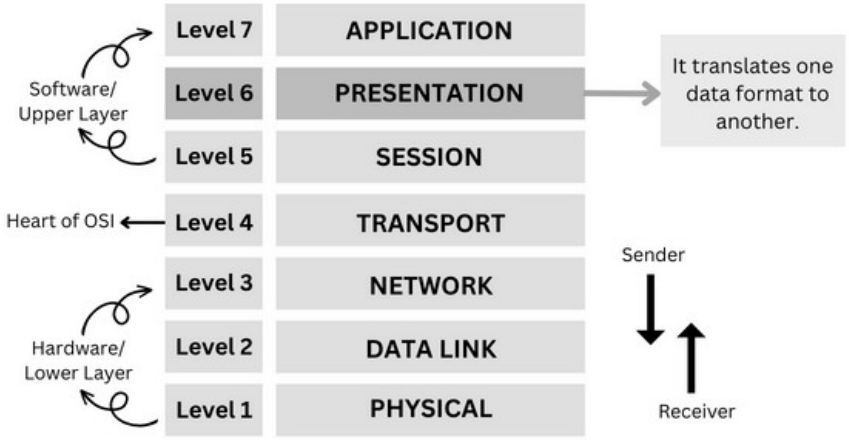
request a service from another program located on another computer on a network. The processes that are communicating do not need to comprehend the details of the network.

iSNS: It is an abbreviation for Internet Storage Name Service. It manages and configures Fibre Channel and iSCSI devices. This protocol is used by many platforms.

SDP: It is an abbreviation for Sockets Direct Protocol. It is a standard wire protocol that supports stream sockets on RDMA (Remote Direct Memory Access) fabrics.

Presentation Layer:

The presentation layer is the 6th layer from the bottom in the OSI model. This layer presents the incoming data from the application layer of the sender machine to the receiver machine. It converts one format of data to another format of data if both sender and receiver understand different formats; hence this layer is also called the translation layer. It deals with the semantics and syntax of the data, so this layer is also called the syntax layer. It uses operations such as data compression, data encryption & decryption, data conversion, etc.



The OSI Model: Presentation Layer

Functions of the presentation layer:

Translation: Data is sent from sender to receiver, but what if the sender device and receiver device understand different formats of code? For example, suppose one device understands ASCII code and another device understands EBCDIC code. In that case, the data must be translated into a code that the recipient understands to determine what data has been sent. The presentation layer is responsible for translating ASCII codes to EBCDIC or vice versa. With the help of the presentation layer, the receiver understands the data effectively and uses it efficiently.

Encryption and Decryption: Whatever data is being transmitted between the sender and the receiver that data must be secure because an intruder can hack the data passing between the sender and the receiver. Hackers can modify the data and send the modified data to the receiver to create false communication. The presentation layer is responsible for encrypting and decrypting data to avoid data leakage and data modification.

The plaintext data at the source is encrypted into ciphertext (unreadable format), then it is sent to the receiver, where the ciphertext is decrypted into plaintext. Now, if the hacker tries to hack the data, the hacker receives an encrypted, unreadable form, and if the hacker tries to send modified data, the receiver can detect the modification during decryption; thereby, the data remains safe.

Compression and Decompression: If the file size is large, it becomes difficult to transmit the large file over the network. File size can be decreased by compressing the file for easy transmission of data. Compression is the method of diminishing the size of a file to transmit data easily in less time. When the compressed data reaches the receiver, the data is reconstructed back to the original size and this process is called decompression.

Sublayers of presentation layer in the OSI model:

The presentation layer in the OSI model is classified into two Sublayers:

Common Application Service Element (CASE): This sublayer offers services to layer-7, i.e., the application layer, and requests services from layer-5, i.e., the session layer. It supports various application services, such as Reliable Transfer Service Element (RTSE), Remote Operation Service Element (ROSE), Association Control Service Element (ACSE), and Commitment Concurrency and Recovery (CCR).

Specific Application Service Element (SASE): This sublayer offers application-specific protocols, such as Message Oriented Text Interchange Standard (MOTIS), Remote Database Access (RDA), File Transfer Access and Manager (FTAM), Common Management Information Protocol (CMIP), Virtual Terminal (VT), Distributed Transaction Processing (DTP), Job Transfer and Manipulation (JTM) and others.

Protocols of the Presentation layer:

Independent Computing Architecture (ICA): It is a presentation layer protocol in the OSI model, which was formed by Citrix Systems. It is used for transferring data from server to client. It is a very thin protocol as it does not require much overhead in order to transmit data from the server over to the client. It is well-optimized for the WAN.

Network Data Representation (NDR): It is the protocol that is used to implement the presentation layer of the OSI model. It provides different kinds of data representation, such as images, video, audio, numbers, etc. It is used for Microsoft Remote Procedure Call (Microsoft RPC) and Distributed Computing Environment (DCE) / Remote Procedure Calls (RPC).

Apple Filing Protocol (AFP): It is a communication protocol that was specifically designed for macOS by Apple, Inc. It provides file services for Classic Mac OS and macOS. This protocol is used to share files over the network.

NetWare Core Protocol (NCP): It is a protocol that is associated with the client-server operating system. The user can access the directory, print, message, file, clock synchronization, etc., with the help of this protocol. It supports many platforms, such as Linux, Classic Mac OS, Windows NT, Mac OS X and Microsoft Windows.

Packet Assembler/Disassembler Protocol (PAD): It is telecommunications equipment that splits a stream of data into separate packets and formats packet headers for asynchronous communication on X.25 networks. It receives packets from the network and converts them into a stream of data. The PAD provides many asynchronous terminal connectivity's to a host computer.

eXternal Data Representation (XDR): It is a computer network protocol that is used to transfer data between two systems. It was first published in 1987. XDR is used by various systems such as NDMP, Network File System, NetCDF, ZFS, Open Network Computer Remote Procedure Call and others.

Lightweight Presentation Protocol (LPP): It is a protocol that offers ISO presentation services over TCP/IP based networks. This protocol explains an approach to provide stream-line support for OSI over TCP/IP based networks.

Application Layer Protocols:

The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user. Application layer performs several kinds of functions which are requirement in any kind of application or communication process.

Application Layer Protocol in Computer Network:

1. TELNET:

Telnet stands for the TELetype NETwork. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

2. FTP:

FTP stands for File Transfer Protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

3. TFTP:

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. The Port number for TFTP is 69.

4. NFS:

It stands for a Network File System. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

5. SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.

6. LPD:

It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A "daemon" is a server or agent. The Port number for LPD is 515.

7. X window:

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window starts from 6000 and increases by 1 for each server.

8. SNMP:

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state and also a channel

through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

9. DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.
The Port number for DNS is 53.

10. DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

11. HTTP/HTTPS:

HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure. This protocol is used to access data from the World Wide Web. The Hypertext is the well-organized documentation system that is used to link pages in the text document.

1. HTTP is based on the client-server model.
2. It uses TCP for establishing connections.
3. HTTP is a stateless protocol, which means the server doesn't maintain any information about the previous request from the client.
4. HTTP uses port number 80 for establishing the connection.

12. POP:

POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.
POP protocol work with Port number 110.

1. It uses TCP for establishing connections.
2. POP works in dual mode- Delete mode, Keep Mode.
3. In Delete mode, it deletes the message from the mail server once they are downloaded to the local system.
4. In Keep mode, it doesn't delete the message from the mail server and also facilitates the users to access the mails later from the mail server.

Electronic Mail:

Introduction:

Electronic mail, commonly known as email, is a method of exchanging messages over the internet. Here are the basics of email:

An email address: This is a unique identifier for each user, typically in the format of name@domain.com.

An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook or Apple Mail.

An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.

To send an email:

1. Compose a new message in your email client.
2. Enter the recipient's email address in the "To" field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click "Send" to deliver the message to the recipient's email server.
7. Emails can also include features such as cc (carbon copy) and bcc (blind carbon copy) to send copies of the message to multiple recipients and reply, reply all and forward options to manage the conversation.

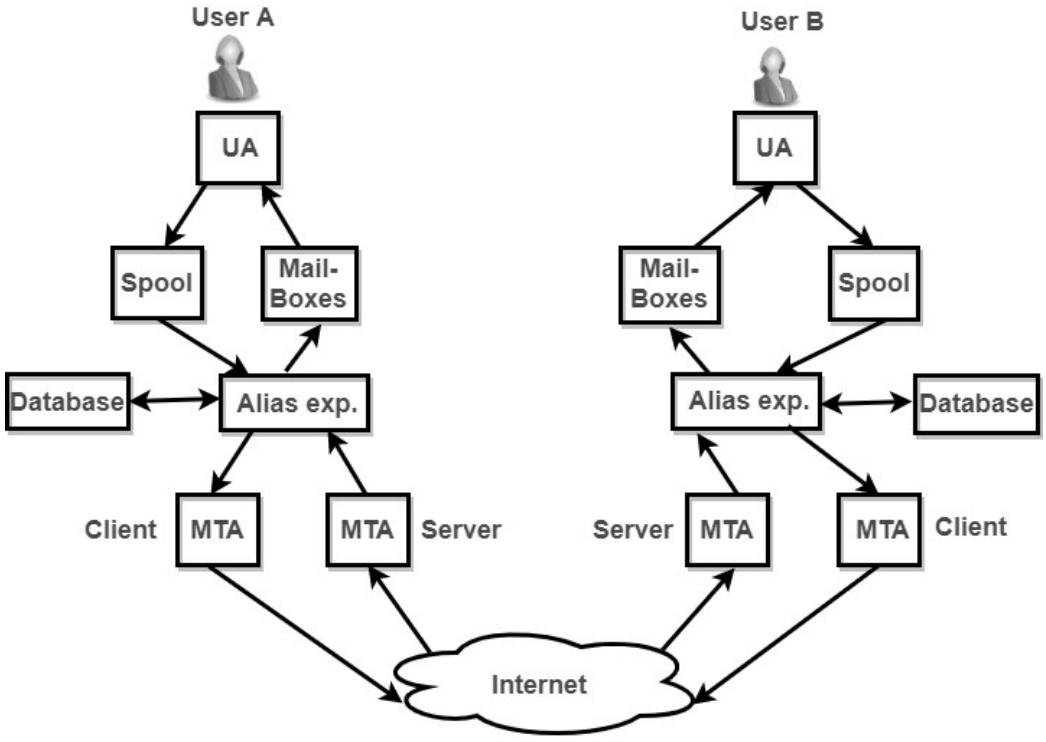
Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data.

The person who is sending mail is called sender and person who receives mail is called recipient. It is just like postal mail service. Components of E-Mail System: The basic components of an email system are: User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

User Agent (UA): The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.

Message Transfer Agent (MTA): MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfers mail to

mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by.



Mailbox: It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox. Access to mailbox is only to owner of mailbox.

Spool file: This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an alias, to represent several different e-mail addresses. It is known as mailing list, Whenever user have to sent a message, system checks recipient's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system:

Composition – The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.

Transfer – Transfer means sending procedure of mail i.e. from the sender to recipient.

Reporting – Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.

Displaying – It refers to present mail in form that is understand by the user.

Disposition – This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

Advantages or Disadvantages:

Advantages of email:

1. Convenient and fast communication with individuals or groups globally.
2. Easy to store and search for past messages.
3. Ability to send and receive attachments such as documents, images and videos.
4. Cost-effective compared to traditional mail and fax.
5. Available 24/7.

Disadvantages of email:

1. Risk of spam and phishing attacks.
2. Overwhelming amount of emails can lead to information overload.
3. Can lead to decreased face-to-face communication and loss of personal touch.
4. Potential for miscommunication due to lack of tone and body language in written messages.
5. Technical issues, such as server outages, can disrupt email service.
6. It is important to use email responsibly and effectively, for example, by keeping the subject line clear and concise, using proper etiquette and protecting against security threats.

World Wide Web (WWW):

The World Wide Web is abbreviated as WWW and is commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

WWW can be defined as the collection of different websites around the world, containing different information shared via local servers (or computers).

History:

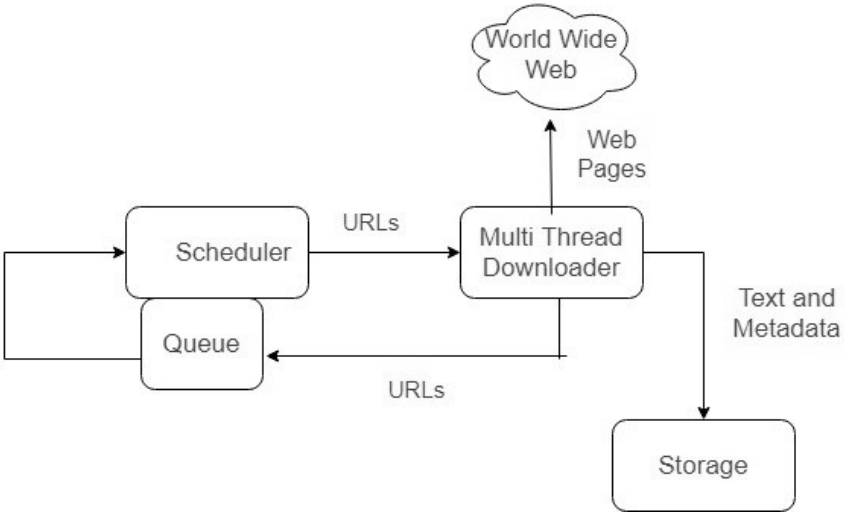
It is a project created, by Timothy Berner Lee in 1989, for researchers to work together effectively at CERN. is an organization, named the World Wide Web Consortium (W3C), which was developed for further development of the web. This organization is directed by Tim Berner's Lee, aka the father of the web.

System Architecture:

From the user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google Chrome, etc are

the popular ones. The browser fetches the page requested interprets the text and formatting commands on it and displays the page, properly formatted, on the screen.

The basic model of how the web works are shown in the figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.



Here the browser displays a web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com; the browser follows the hyperlink by sending a message to the abd.com server asking for the page.

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal.

Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

Features of WWW:

1. HyperText Information System
2. Cross-Platform
3. Distributed
4. Open Standards and Open Source
5. Uses Web Browsers to provide a single interface for many services
6. Dynamic, Interactive and Evolving.
7. “Web 2.0”

Components of the Web:

There are 3 components of the web:

Uniform Resource Locator (URL): serves as a system for resources on the web.

HyperText Transfer Protocol (HTTP): specifies communication of browser and server.

Hyper Text Markup Language (HTML): defines the structure, organization and content of a webpage.