UNIT-IV

Transport Layer: Transport Services, Elements of Transport protocols, Connection management, TCP and UDP protocols.

Transport Services

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:

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- 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:

- Error control
- Sequence control
- Loss control
- 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 receivers 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.

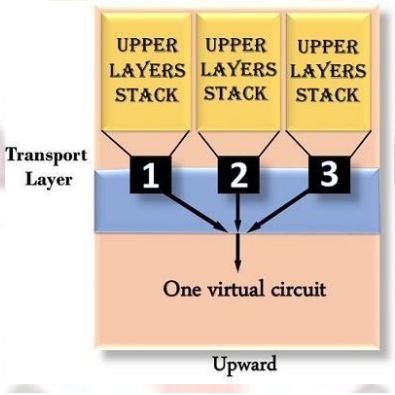
Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

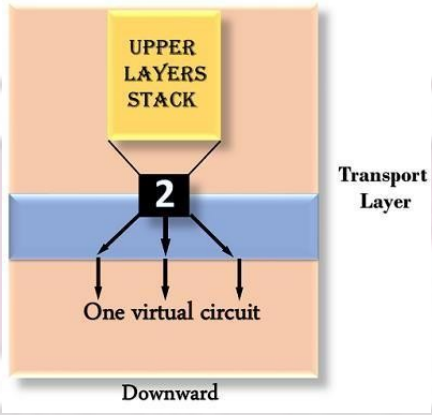
Multiplexing can occur in two ways:

- **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.

- 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.

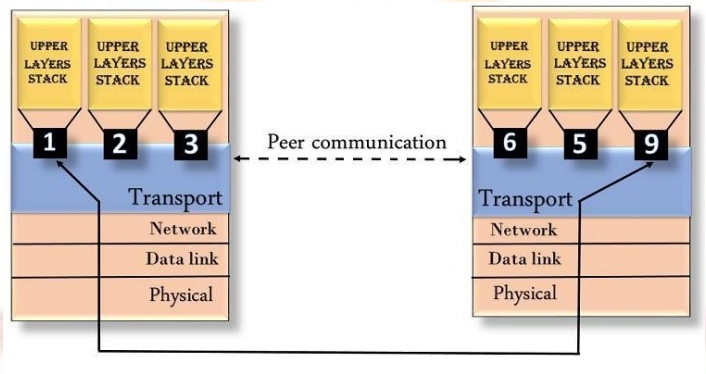


Addressing

- 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.



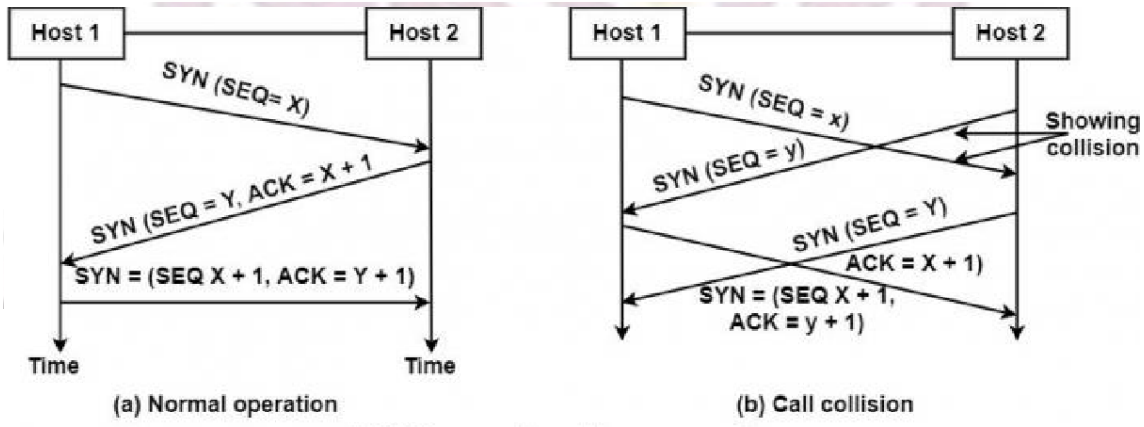
Connection Management

The connection is established in TCP using the three-way handshake to create a connection. One side, say the server, passively stays for an incoming link by implementing the LISTEN and ACCEPT primitives, either determining a particular other side or nobody in particular.

The other side performs a connect primitive specifying the I/O port to which it wants to join. The maximum TCP segment size available, other options are optionally like some private data (example password).

The CONNECT primitive transmits a TCP segment with the SYN bit on and the ACK bit off and waits for a response.

The sequence of TCP segments sent in the typical case, as shown in the figure below −



TCP Connection Management

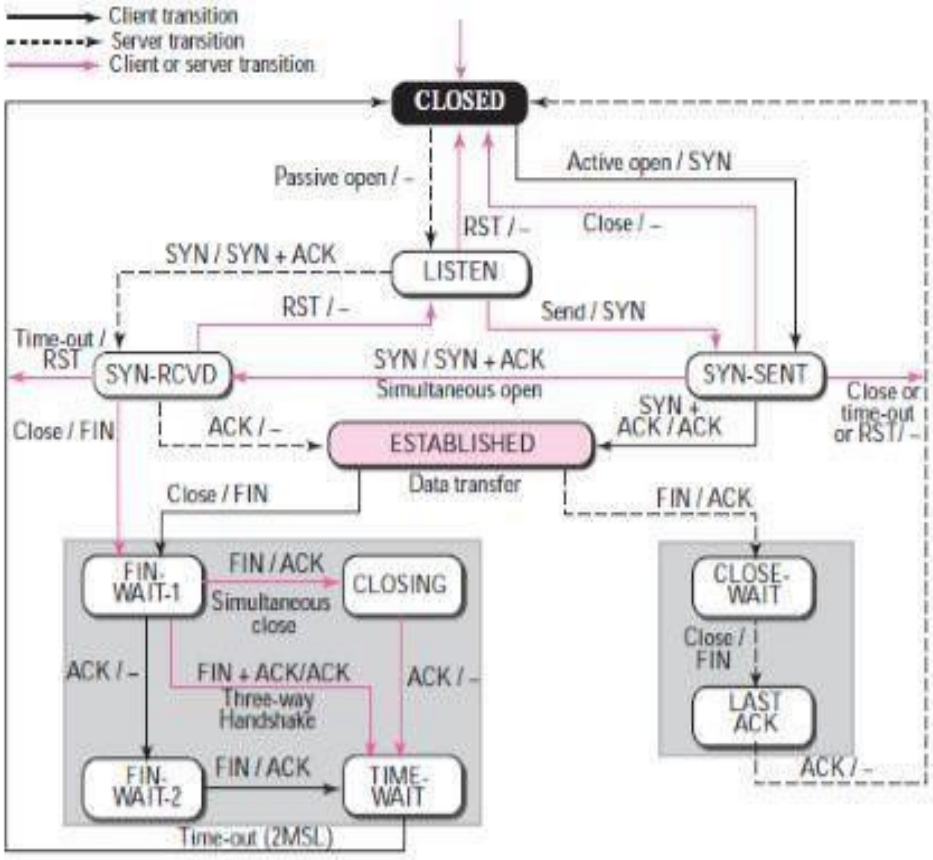
When the segment sent by Host-1 reaches the destination, i.e., host -2, the receiving server checks to see if there is a process that has done a LISTEN on the port given in the destination port field. If not, it sends a response with the RST bit on to refuse the connection. Otherwise,it governs the TCP segment to the listing process, which can accept or decline (for example, if it does not look similar to the client) the connection.

TCP Connection Termination

TCP (Transmission Control Protocol) is a transmission protocol that ensures data transmission in an ordered and secure manner. It sends and receives the data packets in thesame order. TCP is a **four-layer** protocol compared to OSI (Open System InterconnectionModel), which is a **seven-layer** transmission process. It is recommended to transmit data from high-level protocols due to its integrity and security between the server and client.

TCP needs a 4-way handshake for its termination. To establish a connection, TCP needs a 3-way handshake

Connection Management in transport layer using state machine



The client application opens a connection to the server by sending a TCP segment which only the header is present (no data). This header contains a flag SYN stands for "Synchronize" and the TCP port number the server (application). The client is in SYN_SENT state (SYN sent).

The server (application) is listening (listen) and on receipt of the SYN from the client, it changes of state and responds with a SYN and ACK flag. The server is then able SYN_RCVD(SYN received).

The client receives the server's TCP segment with SYN ACK indicators and move in status ESTABLISHED. He also sent a response ACK to the server that also passes in status ESTABLISHED.

This exchange in three phases (three-way handshake) complete the establishment of the TCPconnection can now be used to exchange data between the client and server.

The client side of the connection is responsible for the connection performs an active connection (active open) while the server performs a passive connection (passive open).

In the event that a connection request arrives on the server and that no application is listening on the requested port, a segment with flag RST (reset) is sent to the client by the server, the connection attempt is immediately terminated.

Principle termination of a TCP connection state diagram

The termination of a TCP connection requires four exchanges of TCP segments.

As a TCP connection is bidirectional (full duplex) , connection termination process should be made in both directions of the communication. The client as the server can send a segment with FIN flag, this mean an end to sending data. Receiving a segment with FIN indicates that the other end will not send more data. The term used then is half closed, the connection is half closed.

Typically, the client generates the transmission segment with a FIN flag, he made a closing force (active close), the server receives the segment realizes a passive close. The server acknowledge the FIN with ACK, informs the application for the release of this connection and when done then sends a FIN segment to the customer which in turn, acknowledge it with an ACK flag.

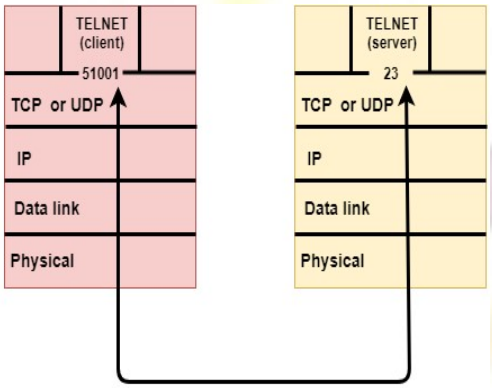
Transport Layer protocols

- 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
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to

thedestination 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 fromIP 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 nonsequenced 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:

633.7K

Source port address 16 bits	Destination port address 16 bits
Total Length 16 bits	Checksum 16 bits
Data	

7eginners

Where

- **Source port address:** It defines the address of the application process that has delivered amessage. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive themessage. 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

- TCP stands for Transmission Control Protocol.
- 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 bytesis 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.