Flow control

Significance of transport layer:

This is responsible for end-to-end communication over a network that is process-to-process delivery. It provides logical communication between application processes running on a different host within a layered architecture.

Protocols used in this layer:

There are two important protocols used in this layer, those are:

- TCP: Transport communication protocol
- UDP: User datagram protocol

The communication between two ends can either be reliable or unreliable depending upon which protocol is in use that is either TCP or UDP.

Transport Protocol:

This is a connection-oriented protocol that provides a reliable, full-duplex byte stream to its end users.

TCP is an example of a stream socket that provides a bidirectional, reliable, and sequenced flow of data, unlike UDP which is a datagram socket.

What makes TCP protocol reliable:

TCP has four important feature which makes it reliable:

- Error control and
- Flow control
- Congestion control
- Connection management

Error control is achieved by:

- Acknowledgement number
- Re transmission
- Checksum
- Sequence number

Acknowledgment Number:

In TCP for every data/segment send to the other end, it requires an acknowledgment in return. The acknowledgment number is nothing but the sequence number of the next bytes the receiver expects to receive.

In the case of TCP, there is a cumulative acknowledgment number that is acknowledgment number is not send for each byte rather it is sent for a group of bytes that is called a segment.

For example:

If the acknowledgment number is 1635, means all the bytes before this number are reached and the receiver expects bytes with 1635 as the next sequence number.

If an acknowledgment number is not received, TCP automatically re-transmits the data(segment) and waits a longer amount of time.

Note:

- The maximum time it can keep trying re transmission is 4 to 10 mins, depending upon implementation.

- TCP does not guarantee that data will be received at other end, its just that it provides reliable delivery of data or reliable notification of failure.
- There is nothing called segment number in TCP, rather each segment is a collection of bytes and each bytes is associated with sequence number.

Thus acknowledgment number provides reliability to the TCP

Retransmission:

This is the heart of the TCP when it comes to reliability that is error control mechanism. If the packets is lost or damaged or corrupted or the ack itself is lost, TCP retransmits the data.

Retransmission takes place in two scenarios:

- Re transmission timer expires: that is it does not get the ack for the send bytes within stipulated time.
- Fast re transmission: This happens when the sender receives three duplicate ACK, in this segment is re transmitted even before RTO.

Checksum: This is one of the features of TCP along with acknowledgment and retransmission which is used for error control mechanisms in TCP.

The checksum is calculated on three fields:

- TCP header
- TCP Body
- Pseudo IP header

The most surprising field out of the above three is the pseudo IP header because the IP header is below the transport header and the values of its fields keep changing when the packet traverses the network. **So the IP fields are used for checksum are those which are constant in the network that is**:

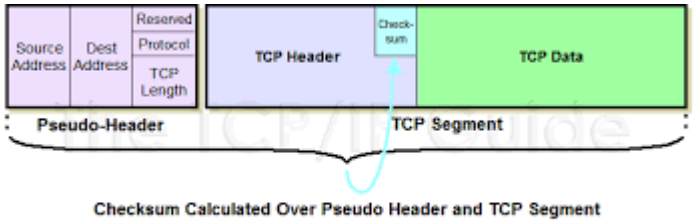
- Source IP address
- Destination IP address
- Protocol
- TCP segment size
- Fixed of 8 bits

The total size of the pseudo-header is 12 bytes.

Once the checksum is calculated with all the three fields, it is placed in the checksum field of TCP header and send to the receiver side and even calculates the checksum on the same fields and compares with what it received from the sender.

If the checksum happens not to be same, segment is considered as corrupted and ack is not being send and TCP autocratically retransmits the same.

Note: Pseudo header is not forwarded along with the network, it is discarded once checksum is calculated.



Sequence number:

TCP associates a sequence number with each bytes it send. For example if the application writes a data of size say 2048 bytes, TCP would send this in two segments where the first segment carries bytes ranging from 1-1024 and the second 1025-2048.

Significance of sequence number:
Reassembly of packet at receiver side:

If the segments arrive out of order, the receiving TCP will reorder the two segments on the basis of sequence number before passing it to the application. Hence in TCP segments never reach out of order.

Discard of duplicate data:

If TCP receives duplicate data may be because of lost acknowledgment or delay in receiving ack because of congestion, the receiving TCP can detect the duplicate data with the help of sequence number and discards the data.

Retransmission of lost or corrupted or for damaged data:

Segments which are lost or damaged are re-send on the basis of the sequence number.

Flow Control:

TCP provides a mechanism called flow control by which it always tells its peer how many bytes of data it is willing to accept. This is called advertised window which reflects the buffer size of the receiver side so that sender cannot overflow the receiver buffer.

This is also called **windowing mechanism.**