

## CHAPTER 4

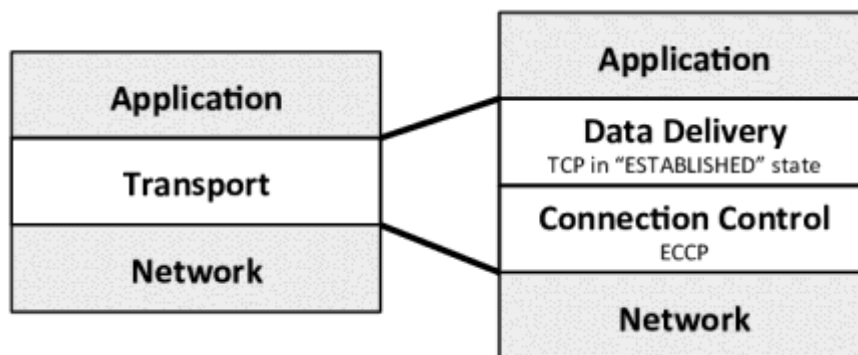
### 4. Transport Layer

#### Objectives

- To recognize the transport layer.
- Illustrating the definition of TCP, UDP and SCTP.
- Learning about congestion management and its forms in order to prevent congestion.
- To consider the standard of service (QoS) and its characteristics.

## 4.1. Overview of Transport Layer

In OSI model, the transport layer is the center layer. Transport layer is mainly used for end to end process delivery, concatenation and segmentation. This layer offers services to the application layer and eliminates services from the network layer.



### 4.1.1. Duties of Transport Layer

The **main duties of transport layer** are the process to process delivery and by performing a variety of functions like packetizing, connection control, error control, addressing, flow control, providing reliability, congestion control and QoS.

#### 1. Packetizing

The transport layer generates packets from application layer where messages obtained. The method of splitting a long message into smaller messages is said to be as Packetizing. These packets are encapsulated in the transport layer packet data field and the headers are attached. The length of the message is split into smaller parts. Each segment is encapsulated in a separate packet. Header is applied to each packet so that the layer can perform its other functions.

#### 2. Connection Control

In connection control, there are two types:

1. Connection oriented
2. Connectionless

Connection oriented creates a connection (i.e. a virtual route between sender and receiver, where packets are numbered consecutively and communicated bi-directionally. The Connectionless Protocol will handle each packet independently. There won't be a link between them. Each packet may take a different route of its own.

### ***3. Addressing***

The client needs the address of the remote machine that the client wants to connect with. Here, the remote computer has a unique address so that it can be distinguished from the ability to connect with the remote computer.

### ***4. Providing Reliability***

Flow management and error detection should be implemented for high reliability.

### ***5. Flow Control***

Flow control always happened from end to end delivery rather than via a single connection.

### ***6. Error Control***

Error correction can be accomplished by retransmission.

### ***7. Congestion Control and QOS***

The transport layer may allow the user to define the desired, appropriate and minimum value of the different service parameters when setting up a connection.

- Connection establishment delay
- Connection establishment failure
- Throughput
- Transit delay
- Protection
- Resident error ratio
- Priority
- Residence

#### ***4.1.2. Quality of Service (QOS)***

The QOS parameters are:

##### ***1. Connection Establishment Delay***

The delay time between the instant at which a transport connection is sought and the instant at which it is accepted is called the connection establishment delay. The shorter the gap, the better the service is. It's the likelihood of a connection.

## ***2. Connection Establishment Failure Probability***

It is probable that the link will not be formed even after the maximum link has been delayed. This could be due to network congestion, lack of table space, or any other issues.

## ***3. Throughput***

It measures the number of bytes of user data transmitted per second, calculated over a period of time. It is calculated for each direction separately.

## ***4. Transit Delay***

It is time for a message to be sent to the source computer by the transport user and received by the transport layer.

## ***5. Residual Error Ratio***

It calculates the amount of lost or clogged messages as a function of the total number of messages sent. The value of this ratio should be zero and as small as possible.

## ***6. Protection***

This parameter provides a way to protect the transmitted data from being read or changed by unauthorized parties.

## ***7. Priority***

It provides a way for the user to demonstrate that some of its connections are more important than others, while managing congestion. Since service should be provided higher priority than low priority connections.

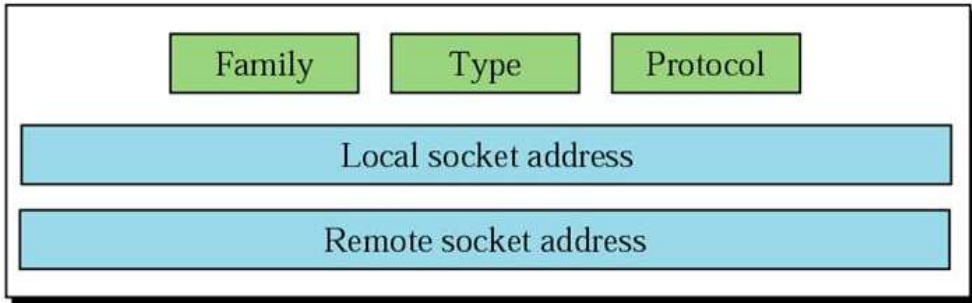
## ***8. Resilience***

The transport layer spontaneously terminates the connection due to internal problems or congestion. The resilience parameter lowers the chances of such termination.

### ***4.1.3. Sockets***

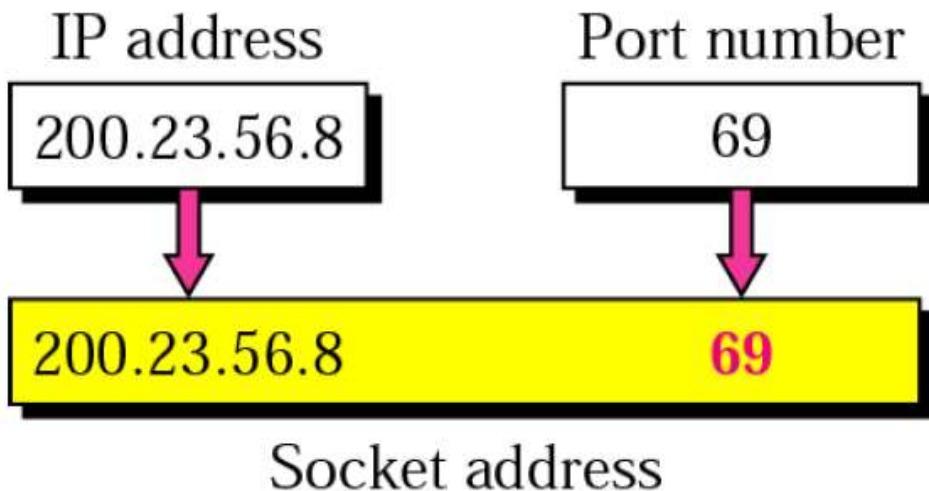
The socket specifies a series of system calls or procedures that function as an interface. The socket also serves as an end point where two processes will interact if and only if and only if they have a socket at either end.

## Socket



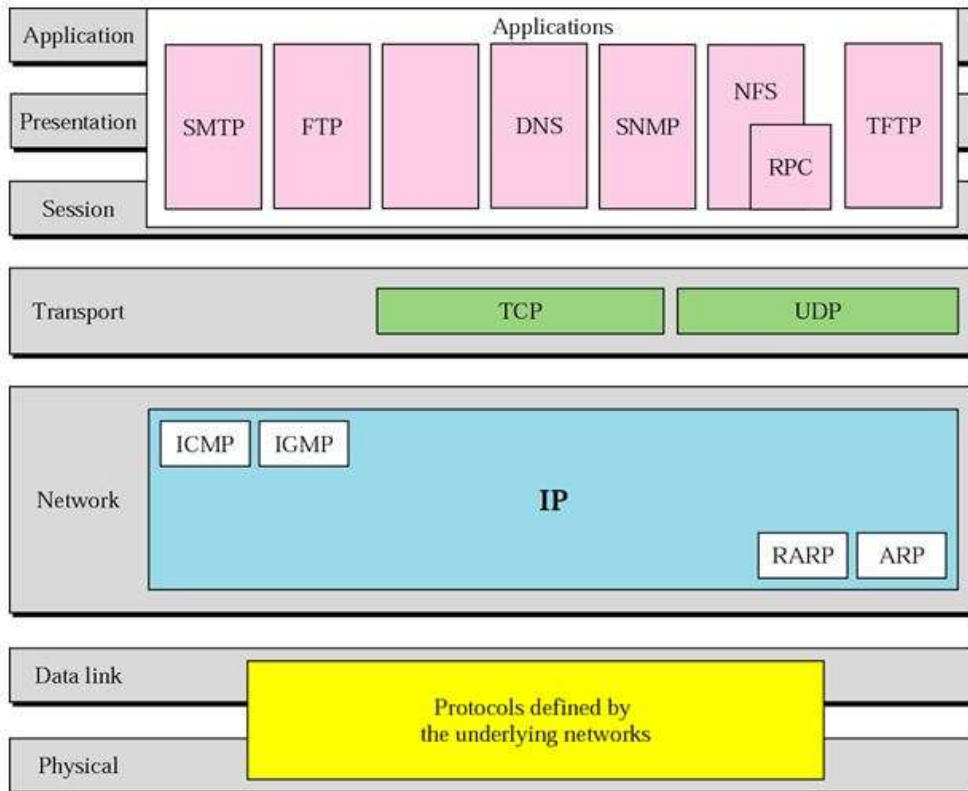
### *Socket Types*

- There are 3 types of sockets. They are stream socket, packet socket and raw socket. In this process to process delivery mechanism, it needs two identifiers, one is IP address and another one is Port number.
- Socket address is defined as the combination of port number and IP address.
- It defines the client and server process uniquely just as the sever socket address defines.
- There is pair of socket addresses used. They are client socket address and server socket address.



**Connectionless service - UDP**

**Connection - oriented service - TCP, SCTP**



## 4.2. User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless, unstable transport protocol. It is a process to process communication where a data unit sent by UDP is called a datagram. UDP has four 16-bit header fields (8 bytes) to every data sent.

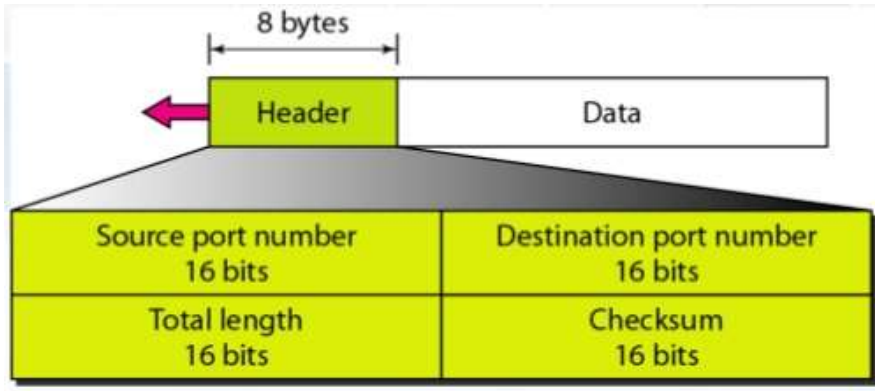
- A length field
- A checksum field
- Source port number
- Destination port number

The port number is used to identify the protocol module which has sent or to receive the data. The use of the standard port number makes it possible for clients to connect with a server without having to specify which port to use.

### 4.2.1. Purpose of UDP

UDP offers a connectionless packet service that represents the most unreliable attempt to deliver. The delivery of the packets, the right sequence of the packets sent, is not guaranteed. UDP is often used for applications that usually transmit small quantities of data at one time.

It also distinguishes between multiple programs running on a single computer. Each UDP message includes both a destination port number and a source port number. This helps to make UDP applications accessible at the destination to send a message to the current program and to send a reply to the application program. The UDP header is divided into four 16 bits.



### 1. Source Port

This port is an optional field that indicates the sending process port and the reply to the address of absence portion. It is said to be not interested when 0 is not used.

### 2. Destination Port

The destination port has significance of a specific destination IP address.

### 3. Length

This field denotes the size of the UDP packet bytes; it includes the header and the data. The minimum length of the header is 8 bytes.

### 4. UDP Checksum

It is used to check the consistency of the UDP header. The pseudo code header is used to carry the checksum. It consists of data from source and destination with IP header and the UDP header.

Source IP Address		
Destination IP Address		
Zero	Protocol	UDP Length

### 4.2.2. UDP Operation

UDP operations are similar as the transport layer.

#### **Connectionless Services**

User Datagram Protocol (UDP) is a connectionless service to every user datagram that UDP delivers. So it is also said to be an independent datagram. In this service, the data comes from same source and delivers to the same destination without any relationship. It does not count the user datagrams and also no link formed for the termination process. Each datagram of the user will follow a different route. UDP cannot send a data in to the stream and hacked into various related datagrams.

#### **Flow Control and Error Control**

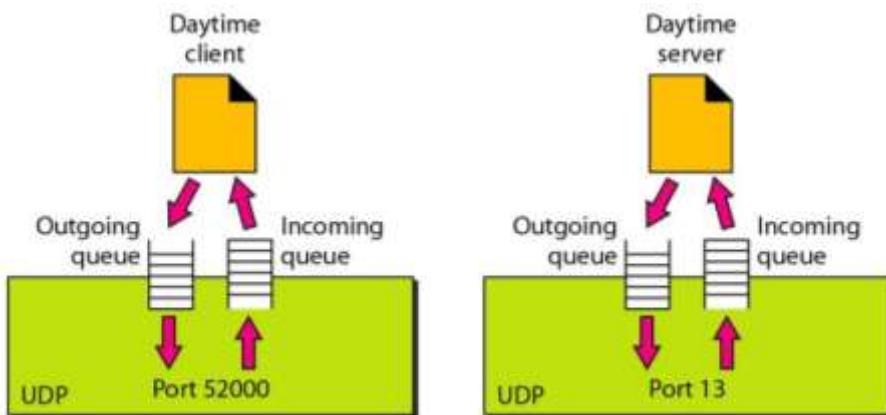
User Datagram Protocol (UDP) is a connectionless transport protocol. There is no window mechanism because of less error and flow control. The received messages are filled in the receivers. In UDP, only in the checksum there is error management. When a message is duplicated or lost, the sender is not able to find. The user datagram will be terminated when receiver detects an error in the checksum. The UDP process provided the mechanism of controlling flow and errors.

#### **Encapsulation and Decapsulation**

Both encapsulation and decapsulation helps to send a message from one process to another in an IP datagram.

#### **Queuing**

When a process begins, the client demands a port number from the operating system.





The incoming and outgoing queue is generated for each operation. When several number of systems are connected with a process: port number, one incoming and one outgoing queues will be generated. The queues will be killed, once process ended. The outgoing queue is used to send message to the client using source port numbers. One by one the messages will be removed by UDP after delivering them to IP after inserting the UDP header. The outgoing queue can overflow. When a message receives at a client side, UDP immediately checks the incoming queue whether the port number has been generated in the field of destination port number of the user datagram. Once UDP receives the user datagram, the unreachable port message will be send to the server from ISMP protocol. All the incoming messages from same or different server are sent to the queue. After receiving the message at UDP server, it verifies the port number of user datagram destination port number at incoming queue. At the end of the queue, UDP sends an acknowledgement of receiving datagram. UDP terminates the user datagram if there is no queue. Finally ICMP sends an unreachable request to the client. All the incoming messages from same or different client are sent to the same queue. UDP removes the message one by one and delivers those messages to the IP after inserting the UDP header.

#### ***4.2.3. Advantages of UDP***

- The process like simple request, flow control and error management are supported by UDP.
- Multicasting is also supported by UDP transport layer.
- It also supports controlling process like SNMP.
- It uses updating protocols for certain routes like RIP.
- It is also suitable for internal flow and error management processes.

### **4.3. Transmission Control Protocol (TCP)**

Transmission Control Protocol (TCP) is a process to process or program to program protocol. It is a link oriented protocol where port numbers are used in TCP. Virtual connection is established for data transmission between two TCPs. It uses an error management system and flow control in the transport layer. This TCP protocol is always a secure transport protocol because of connectivity-oriented and it provides reliable features to IP services.

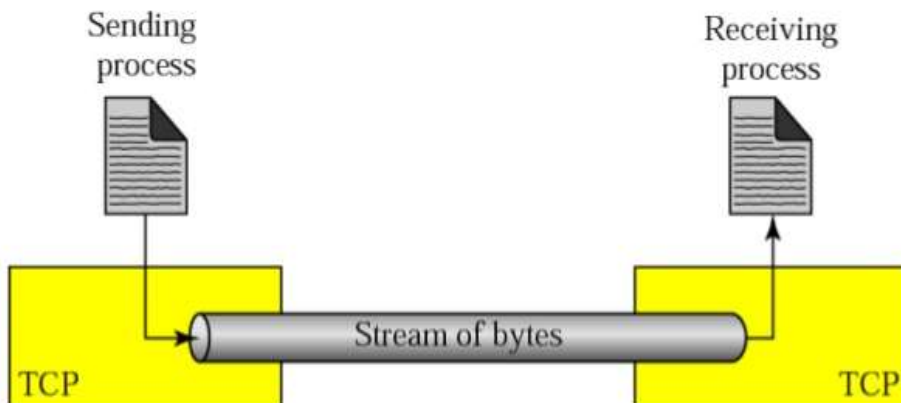
#### ***4.3.1. TCP Services***

**Process to process communication** is provided by port numbers in TCP. These are list of well-known port numbers used by TCP.

Port	Protocol	Description
7	echo	echoes a received/send back
9	discard	discards received datagram
11	users	active users
13	daytime	returns day/ time
17	quote	returns quote
19	chargen	returns string of character
20	FTP, data	File Transfer Protocol/ data
21	FTP, control	File Transfer Protocol/control
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	HyperText Transfer Protocol
111	RPC	Remote Procedure Call

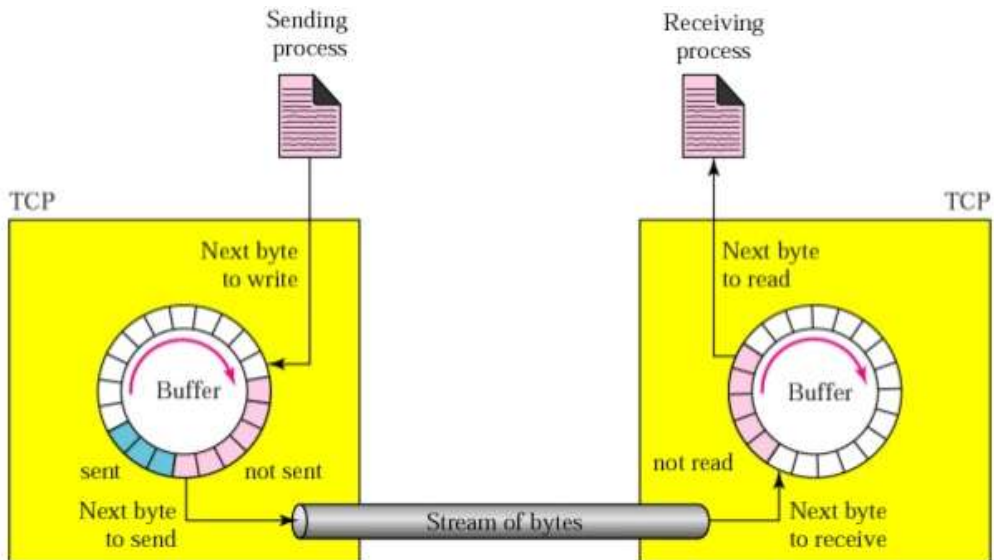
### ***Stream Delivery Service***

Transmission Control Protocol (TCP) is a streaming protocol which helps to send the data to convey using stream of bytes and enables to receive data as a stream of bytes. An imaginary tube is used to carry the data between two processes over the internet. This imaginary environment is used to send a mechanism that generates to write or read the stream of bytes over the sending/receiving device.



## ***Sending and Receiving Buffers***

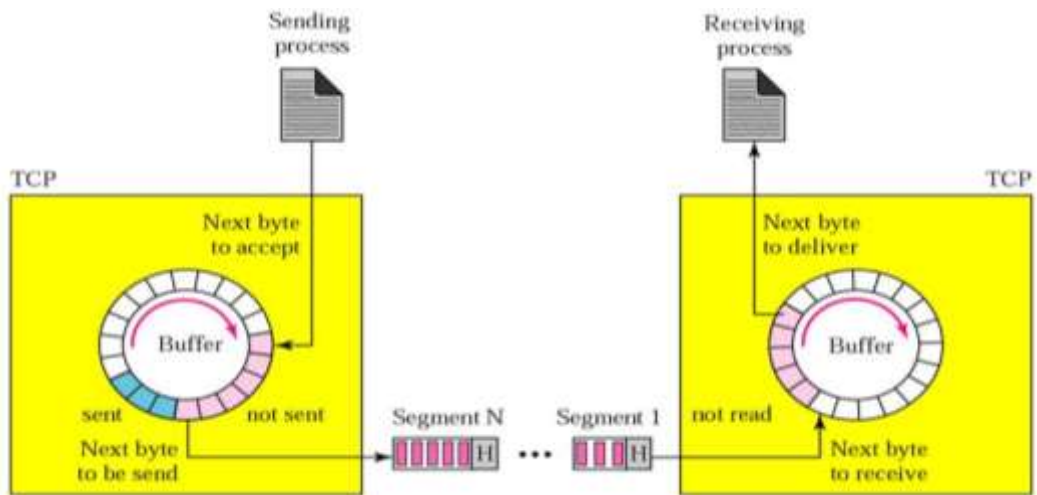
The write or read operation over data cannot be done at the same speed in sending and receiving process. Buffers are using in TCP for storage. There are mainly 2 buffers used in TCP, one is used for sending buffer and the receiving buffer and another is used to implement a buffer is to use a 1 byte location circular array.



There are 3 chambers of buffer used at the sending side; they are white section, gray section, and colored section. Empty chambers are filled by sending process in white section. The sent data which is not recognized are presented in grey area by bytes. TCP holds these bytes in the buffer till the acknowledgment receives. The sent data by the sender are presented in the colored area. At the receiver side the operation will be completed easily. There are 2 areas in the circular buffer; they are white and colored. The empty chambers are filled by bytes in the white buffer which is obtained by the network. The received bytes are read by the receiver side and filled in the empty chamber in colored buffer area. The chamber is returned and recycled to the empty chamber area, once the byte is read at the receiving process.

## ***Segments***

An empty chamber which is obtained from network is filled by bytes in the white buffer. All the received bytes in receiving methods are read in colored segment. The chamber is returned and recycled to the empty chamber area, once the byte is read at the receiving process.



### ***Full Duplex Communication***

In this communication, TCP offers data flow in both direction and at also at the same time. In both the direction TCP buffer sends and receives the segments.

### ***Connection Oriented Service***

In a TCP, if one process needs to send and receive the data from the next process, there establishes a two connection between them. They are,

1. In both directions, data to be exchanged.
2. Connection termination.

It is a stream oriented environment and it acknowledges the distributing bytes to its destination. In an IP datagram, if the TCP segment is encapsulated the data can be misplaced, corrupted or sent out of order and then it should be resent. Different paths can be used to reach the destination.

### ***Reliable Service***

TCP is always said to be a secured protocol for transporting services. It detects and verifies the arrival of data and its safety.

### ***4.3.2. TCP Features***

#### ***Number System***

TCP is used to track the segment number in the header for both the sent and received segments. Acknowledgment number and Sequence number are the two fields in the segment header.

### ***Byte Number***

TCP numbers the transmitted bytes of data to each link. The numbering begins with a number generated at random. They're stored in the send buffer and counted.

### ***Sequence Number***

Once the bytes numbered, sequence number will be assigned to each segment by the TCP. In that segment, sequence number is the first byte number for each segment. Combination of both control and data information uses the sequence number in each section. When there is no data in the segment, sequence number will not be defined. The receiver should have a sequence number when it has control information to acknowledge it.

### ***Acknowledgement Number***

The acknowledgement number will be used by the sender and also receiver site to confirm the received bytes. The acknowledgment number should be given to the next byte information to be received. Cumulative acknowledgement gives the received number of last byte.

### ***Flow Control***

Flow control uses byte-oriented. The sum of data which is transmitted by the sender is monitored by data receiver.

### ***Error Control***

Error control is byte-oriented. Errors are detected by data unit segments.

### ***Congestion Method***

The sender's data will be governed by the receiver and in network it is also measured by the degree of congestion.

### ***Source Port Address***

This address is the 16-bit field. It is used to specify the port number where the host sends the application in the section.

### ***Destination Port Address***

This address is the 16-bit field. It is used to determine the port number where the host receives the application in the section.

### ***Sequence Number***

It is the 32-bit field. It is used to determine the first data byte and also the destination. Initial Sequence Number (ISN) is generated by random number generator for each parity in different direction.

## ***Acknowledgement Number***

It is the 32-bit field. The byte number is determined for the receiver which receives from another entity.

## ***Header Length***

This is 4 bit field. It shows the number in TCP header of 4 byte words.

## ***Reserved***

This is a 6 bit field. It is mainly reserved for future.

## ***Control***

This is 6 bit field. It is used to identify 6 separate flags or control bits and also more than one can be set at a time.

**URG** – Urgent Pointer field value

**ACK** – Acknowledgement value

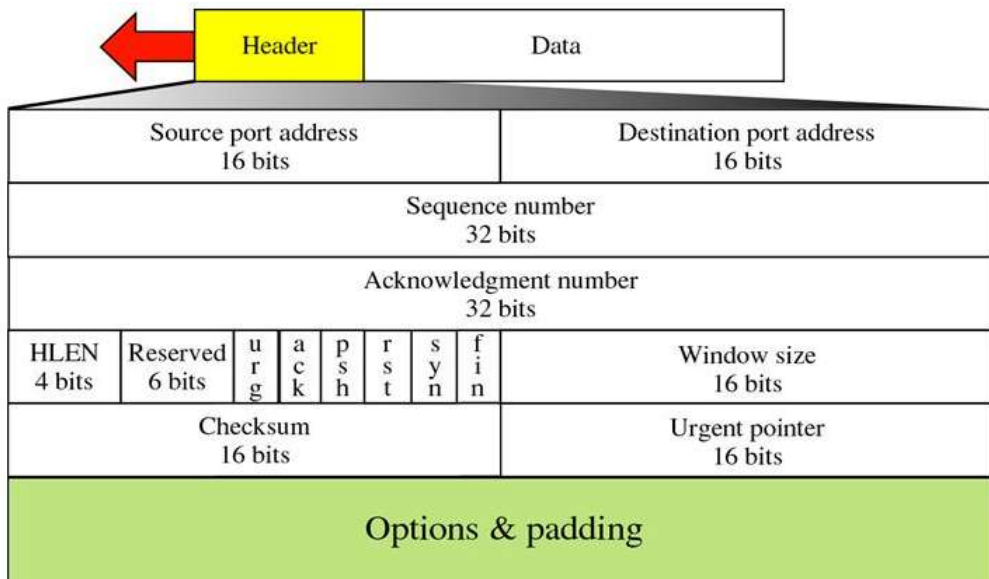
**PSH** – Data Push

**RST** – Connection resetting

**SYN** – Synchronization

**FIN** – Connection termination

## ***Segment Format***



Header Segment Consists of 20-60 Bytes

### 4.3.3. TCP Connection

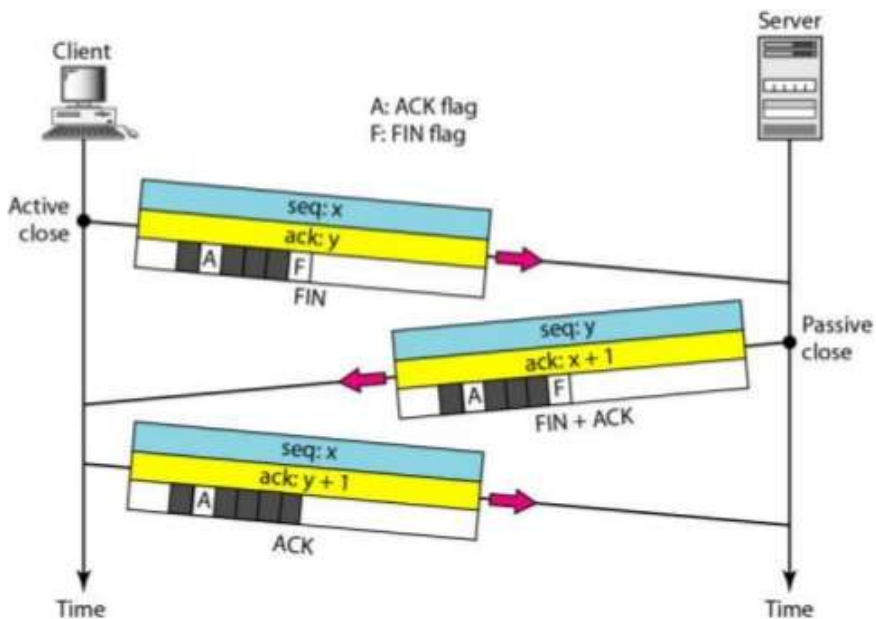
Transmission Control Protocol (TCP) makes a virtual path between the source and the destination so it is said to be a connection-oriented network. Through this virtual path all the segment messages are sent. It is made by these 3 phases. One is connection establishment; two is data transfer and last is connection transfer.

#### 1. Connection Establishment

In this connection establishment, full duplex method is used to transmit the data. The segments are sent concurrently by linking two TCPs along with two devices. Before the data transfer each device must initialize and also should be able to receive the data from another device.

#### Three - Way Handshaking

- Three-way Handshaking method is linked with TCP system.
- Using TCP transport layer the client sends the link to the server.
- Server will start the program.
- An passive open request is an request accepts the connection which is ready and it is informed to TCP by server program.
- An active open request is issued by client program.
- If any client wants to be connected to open server it will be informed by the any server to its TCP.



There are 3 steps in this phase,

- SYN segment – It consumes one sequence number and it does not carry any data.
- SYN +ACK – It does consume one sequence number and it does not carry any data.
- ACK segment - It does not consume one sequence number and data.

## 2. Data Transfer

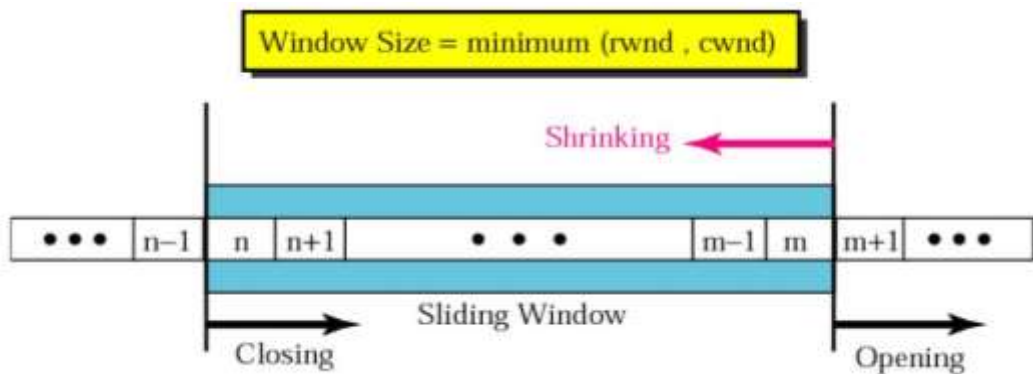
Bi-directional data transfer can take place after the link has been formed. Both the client and the server will submit data and acknowledgements. The receipts are piggybacked with the results.

## 3. Connection Termination

Link termination uses their way or four-way handshaking. The FIN segment consumes one sequencing number if it does not carry data. The FIN+ACK segment consumes one sequencing number if it does not carry data.

### 4.3.4. Flow Control

TCP uses a sliding window to control the movement. The sliding window protocol used by TCP is between Go-back N and selective sliding repeat window. It is byte-oriented and variable size fixed.



The window covers a portion of the buffer containing the bytes obtained from the method. Bytes in the window can transit and also sent without acknowledgement. The two wall on the left and right side acts like an imaginary window. It carries out three activities: opened, closed, and reduced. In these operations, the receiver instructions should be followed by the sender. The windows opened by shifting the right wall to the right side. The windows closed by shifting the left wall to the right. The window shrinks by shifting the right wall to the left. The



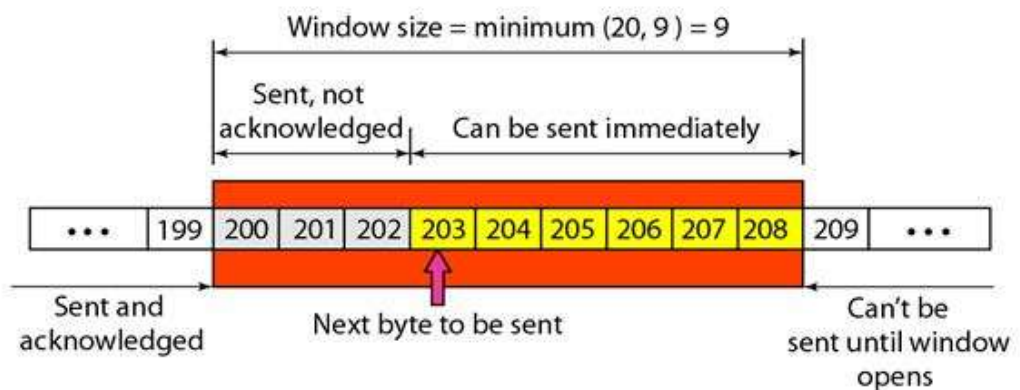
left wall moves only if it receives an acknowledgement from the previous one. The size of the window is determined at the one end and it should be lesser than two values.

1. Receiver window (rwnd)
2. Congestion window (cwnd)

Acknowledgement section at the opposite ends value is marked at the receiver window. The value which is calculated by the network is to prevent congestion at congestion window. By this method the flow of data is controlled and transmission is also more effective, so the data is not overloaded in the destination. This method is said to be as byte-oriented.

**Note**

- Window size is small (rwnd & cwnd).
- In this window the source will not submit the complete data.
- The receiver can open and close the window, but not in narrow.
- At the any time, destination can submit the acknowledgment at any time.
- Shrinking window does not result in destination.
- The sender window is shut downed by the receiver temporarily.
- After the window shut downs, it can send segment of 1 byte.



**4.3.5. Error Control (Retransmission)**

Transmission Control Protocol (TCP) is a stable protocol for the transport layer. A data stream is delivered to TCP to transmit the overall stream to the application. An application program will not lose or duplicated. It provides reliability through error management. A system identifies the corrupted, lost, duplicated or out of ordered segments by error management. Checksum is used to identify the error and its correction and also the time recognition.

## ***Checksum***

- The damages segment will be checked by the checksum in each segment.
- The corrupted segment is discarded by TCP and it is said as missing.
- 16 bit checksum is mandatory for each segment in TCP.

## ***Acknowledgement***

- Acknowledgement is used to validate the stream of data fragments in TCP.
- It is not acknowledged by ACK segments.
- The sequence number is acknowledged and does not hold any data in control segments.

## ***Retransmission***

- The retransmission is the center of error control.
- It is retransmitted once the section delays, corrupted or skipped.
- The retransmission is twice the section.
  1. When the timer of retransmission expires.
  2. The 3 duplicate ACKs received at the sender side.

### ***1. When the Timer of Retransmission Expires***

- For all sent segments one timer Retransmission Time-Out (RTO) is retained by TCP.
- The segment which sent earlier is also retransmitted because delay and lack of ACK received or missed acknowledgement.
- In TCP, the RTO value is dynamic in nature and modification for the segments is done by Round Trip Time (RTT).
- The acknowledgement and time taken by the segment to reach the destination is said to be as Round Trip Time (RTT).

### ***2. The 3 Duplicate ACKs Received at the Sender Side***

- The receiver receives more than one segment at the time of segment loss, because it is not able to save.
- When one segment is lost and the receiver receives so many segments out of order that they cannot be saved (limited buffer size). It follows three duplicate ACK rules and immediately retransmits the missing segments.
- This happens because of limited buffer size and it is said to be as quick retransmission.

## ***Out of Order Segments***

- The segment may be out of order because of delay, skip or discard of the segments.

- The missing of segments may flag it as out of order.
- Most of the implementation is not able to terminate as out of order because they stored as temporary.
- Data which is received by TCP is stored as temporary when it is out of order.
- Out of order segments should not be delivered and it should be verified by TCP.

#### 4.4. Stream Control Transmission Protocol (SCTP)

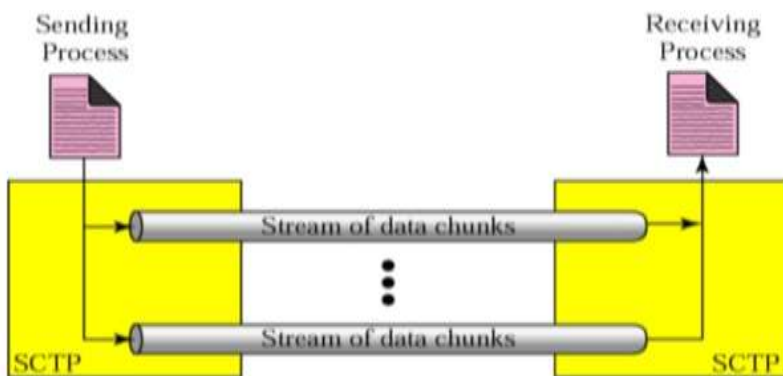
Stream Control Transmission Protocol (SCTP) is a message-oriented, modern, efficient transport layer protocol. It provides better efficiency and reliability. SCTP incorporates the best User Datagram Protocol and Transmission Control Protocol functionality. This protocol maintains the boundary for message and also able to detect the duplicates/missing data on out-of-order segment. This protocol has a system for managing congestion and flow.

##### 4.4.1. SCTP Services

In STCP process-to-process communication uses all the well-known parts in TCP.

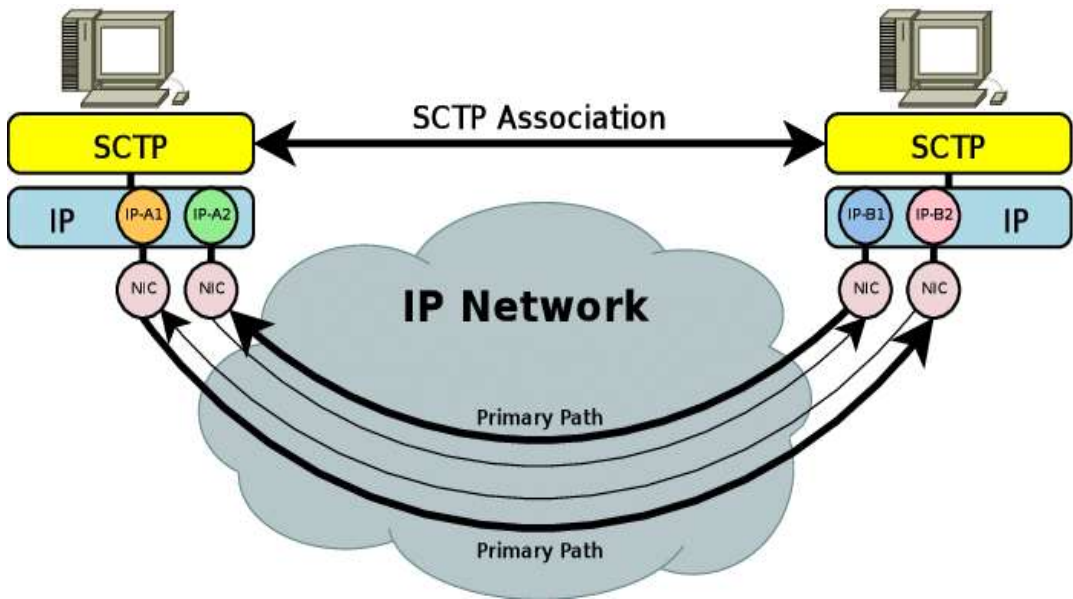
##### *Multiple Streams*

Both the TCP client and server have a connection as a single stream. This protocol enables multiple stream connection to be established that is referred to as Stream Control Transmission Protocol association. If one stream has been blocked, the other streams will deliver the data. Multiple streams is always allowed in Stream Control Transmission Protocol association.



##### *Multihoming*

Multihoming service sends and receives a host that can specify several IP addresses for each and every association. Alternate interface will be used without any interruption when one route fails. SCTP allows multiple IP address at both the end.



### ***Full Duplex Communication***

Full duplex is used when data flows in both directions at the same time. In both connections, it has buffer sender and receiver to send/receive the packets at both directions.

### ***Connection Oriented Service***

When process A needs to send the data and receives another data from process B. The following shall occur:

1. An association should be created between two SCTPs.
2. In both the directions, data can be send/receive.
3. Then association can be terminated.

### ***4.4.2. Sctp Features***

#### ***Transmission Sequence Number***

In Stream Control Transmission Protocol (Sctp), the one to one communication may be used to transfer the message due to fragmentation. By numbering data chunks in Sctp, data transmission is managed. Transmission Sequence Number (TSN) is used to number the data chunks. TSN is 32 bit long in Stream Control Transmission Protocol (0 & 2-1).

#### ***Stream Identifier***

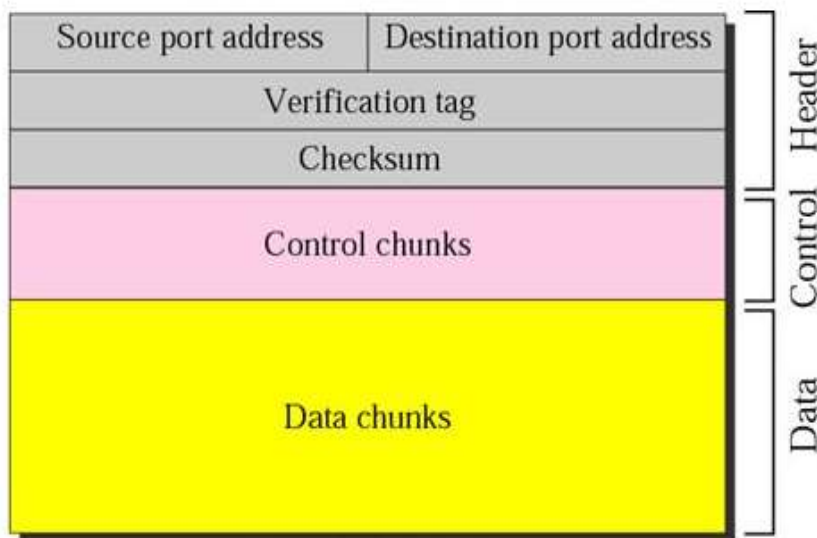
Stream Identifier (SI) is used to identify the stream in Sctp. Before arriving to the destination each data should have its SI in header.

### ***Stream Sequence Number***

In SCTP destination, the data packets will be forwarded to their stream once it arrives. Stream Sequence Number (SSN) is used to define the data packets in their stream.

### ***Packets***

Information is transmitted as data packets and control information is transmitted as control packets. A lot of control and data packets can be bundled in a single packet. The Stream Control Transmission Protocol packet also has a same mechanism as the Transmission Control Protocol portion. TCP has parts, SCTP has packets.



### ***Acknowledgement Number***

The ICP acknowledgement numbers are applied to sequence it. It is byte-oriented. However the Stream Control Transmission Protocol acknowledgements are always packet oriented by reference TSN.

### ***Flow Control***

Flow control is used to prevent exhausting the receiver.

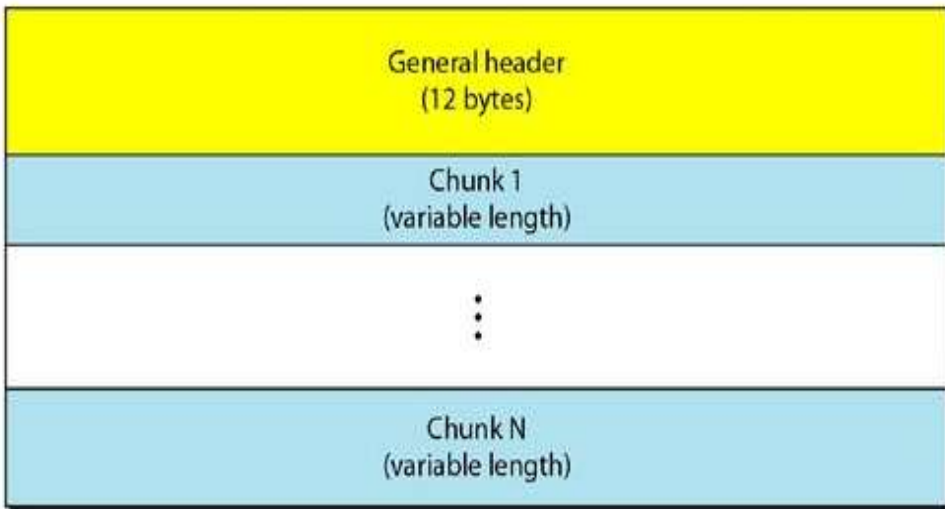
### ***Error Control***

It implements error management to provide reliability.

### ***Congestion Control***

It is used to determine how many data chunks can be rejected on the network.

## ***Packet Format***



## ***General Header***



## ***Source Port Address***

It is 16-bit field address. Port number is determined for sending the packet.

## ***Destination Port Address***

It is 12-bit field address. Port number is determined for receiving the packet.

## ***Verification Tag***

Packets are connected by using this verification number. It is used to describe the process that is replicated in every packet during the process.

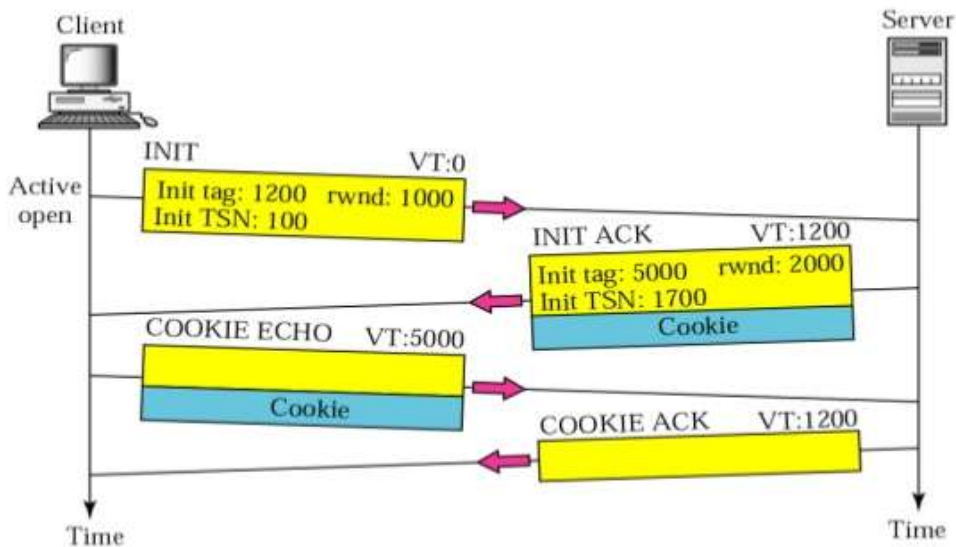
## ***Checksum***

It is 32-bit field. It includes the CRC-32 checksum.

### 4.4.3. SCTP Connection

#### 1. Association Establishment

- Four Way Handshaking process is used in the SCTP.
- The server uses SCTP as a transport layer and client creates a link with the process.
- The client initiates the link (active open) and server must be ready to accept the link (passive open).
- The 4 way handshaking steps are:
  1. The INIT chunk is the first packet send by the client.
  2. The INIT ACK chunk is the second packet.
  3. The COOKIE ECHO chunk is the third packet send by the client. It includes a simple chunk that echoes without any change.
  4. The COOKIE ACK chunk is the fourth packet send by the server. It includes acknowledgement receipt of the cookie echo chunk.
- The solution is to pack the information and send it back to the client. This is called generating a cookie.



#### 2. Data Transfer

- Bi-directional data transfer can take place after the association has been formed.
- The boundaries are established and recognized.
- After processing, the message will be considered as a single unit and it may be fragmented into data chunks.

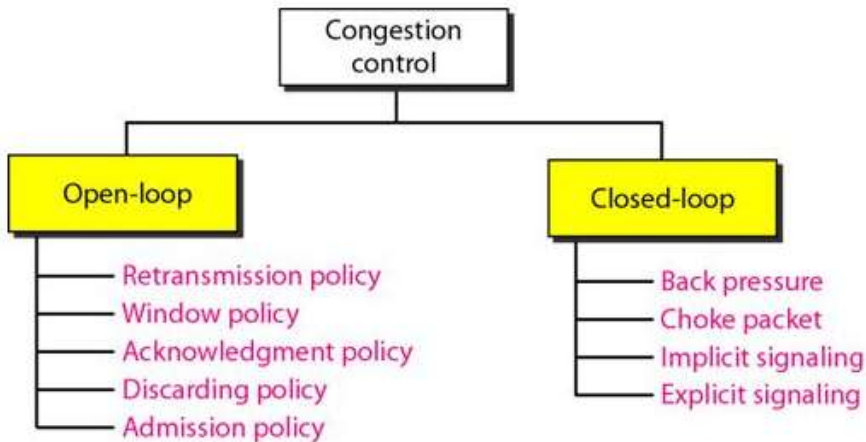
- Then data chunks will be broken down by adding header to the message.
- A single TSN is given for the message or fragments which has set of information.

### 3. Connection Termination

- The process should avoid sending the new data once the process has been terminated.
- The queued data should be submitted or closed before the request sends for termination.
- The three packets are used for process termination; they are shutdown, ACK shutdown, and full shutdown.

### 4.5. Congestion Control

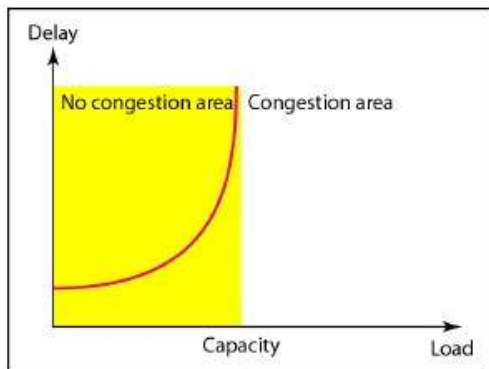
The process of avoiding congestion before it occurs or eradicate congestion after it has been occurs is said to be as congestion control. It is divided into two wide categories.



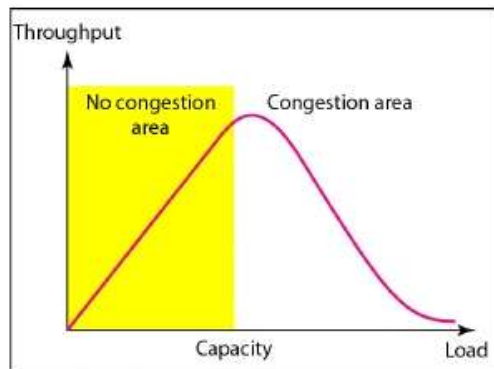
#### 4.5.1. Congestion - Network Performance

- When network is loading the number of packets sent to the network is greater than the ability of the network. Here the number of packets the network can handle is said to be a network congestion.
- The mechanism of managing congestion and holding the load below capacity is congestion control.
- The routers and switches have buffer queues to carry both the before and after processing packets.
- It has 2 factors to calculate the network efficiency. They are throughput and delay.





a. Delay as a function of load



b. Throughput as a function of load

### 4.5.2. Open Loop Congestion Control

In the form of open loop congestion management, policies are implemented to avoid congestion before it occurs. This can be happened by source or destination.

#### 1. Retransmission Policy

- This policy is also unnecessary.
- The packets are retransmitted when the sender send the packet as misplaced or identical.
- Network congestion occurs by retransmission.
- A strong transport policy will avoid congestion.
- The policy on retransmission and timers must be structured to maximize performance and also avoid congestion.

#### 2. Window Policy

- Congestion can cause on the sender windows.
- Instead of using back N window, the selective repeat window manages congestion.
- The packets will be mistrustful when timer times out. Few packets may receive safe at the receiver in back N window.
- The lost and corrupted unique packets are tried to send in the selective repeat window.

#### 3. Acknowledgement Policy

- The acknowledgement policy can also have an effect on congestion.
- If the receiver does not accept any packets it receives, it can slow down the sender and help avoid congestion.

- A receiver can send an acknowledgment only if a packet has to be sent or a special timer has expired.
- Only N packets can be acknowledged at a time by the receiver.
- Sending fewer acknowledgements in the network.

#### **4. Discarding Policy**

- Congestion and transmission integrity is avoided by discarding policy.

#### **5. Admission Policy**

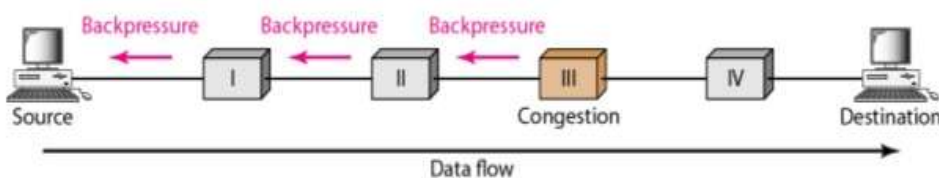
- It is also said to be a quality of service mechanism.
- In this policy, congestion is avoided in virtual circuit networks.
- In flow requirement switches are first verified before moving to the network.
- A virtual circuit link is refused by the router when there is congestion.

#### **4.5.3. Closed Loop Congestion Control**

In this control, congestion is minimized only after it occurs.

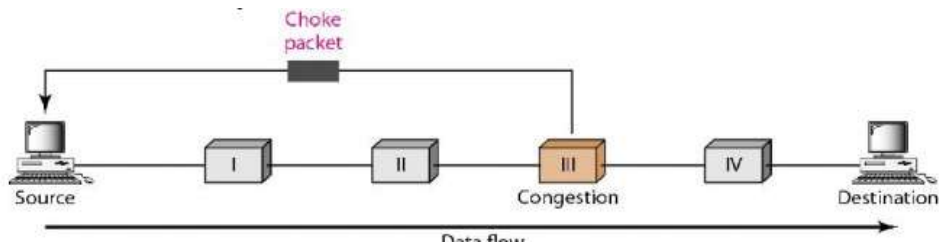
##### **1. Back Pressure**

- The technique of back pressure refers to the congestion management system under which the congestion node avoids receiving data from the immediate upstream node or node.
- Congestion occurs in the upstream node and data's also refused from its node.
- Back pressure is a also said to be a node-to-node congestion control.
- This control starts by beginning and flows till the opposite side to the source.
- It happens only in virtual circuit networks and data flows of each node are identified only by upstream node.



##### **2. Choke Packet**

- A choke packet sends packet to the source to identify congestion.
- It sends congestion warning directly to the source station from router.
- The intermediate nodes are not able to alert.



### 3. Implicit Signaling

- In this signaling, there will be no contact between source and congested node.
- If there is any congestion in the system the source will inform to the network.

**Eg:-** If a source needs to send multiple data streams and if there are no acknowledgements, there may be a congestion. A network congestion may cause by delay in receiving the acknowledgement or it may slows down the source.

### 4. Explicit Signaling

- In this signaling, the signal will be sent to the source or destination to find the congestion.
- The method of choke packets is not as same as signaling.
- For this reason, a separate packet is used, and this signal is included in the packets that carry the data.
- In either forward or backward directions, the congestion control of the frame relay occurs.

#### a) Background Signaling

- A bit can send through the packet of data by travelling in opposite direction of the congestion window. In case of discarding, the bit will send an alert to the source to slow down the process.

#### b) Forward Signaling

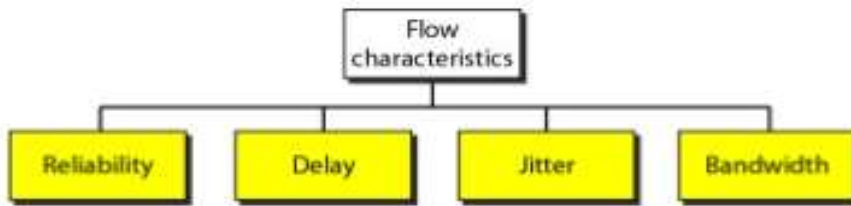
- In this signaling a set of packets can travel in a congestion window as bits. When congestion occurs in particular bit the alert will be sent.
- Congestion is reduced by slowing down the acknowledgement.

## 4.6. Quality of Service (QOS)

A problem which occurs in internetworking to flow seeks to be attained is defined as Quality of Services.

### 4.6.1. Flow Characteristics

There are 4 types of characteristics are attributed to a flow.



#### 1. Reliability

Reliability is the characteristics that a flow requires Lack of reliability implies the failure of a packet or an acknowledgment that includes retransmission.

**Eg:-** Email, transferring a file and internet connectivity.

#### 2. Delay

This is used get delay from source to destination.

**Eg:-** Audio/video conference, telephony, remote access.

#### 3. Jitter

Jitter is a difference in the delay of packets belonging to the same flow.

**Eg:-** If 4 packets depart in time 0,1,2,3 and arrive at 20,21,22,23 all have the same delays, 20 units of time.

If 4 packets arrive at 21,23,21,28, they will have different delays: 21,22,19,24.

Jitter is known as the variation in the delay of the packet. High jitter means that the difference between delays is large, low jitter means that the variance is small.

#### 4. Bandwidth

There is a variable bandwidth depending on the different applications. In video conferencing, millions of bits per second are required to refresh the color screen while the total number of bits in email may not even exceed a million.