**Principles Computer Networking (CST102) Services of TCP layer**

###### 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:

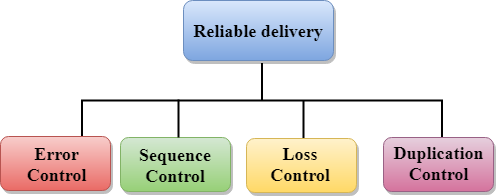
The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

## Reliable delivery:

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

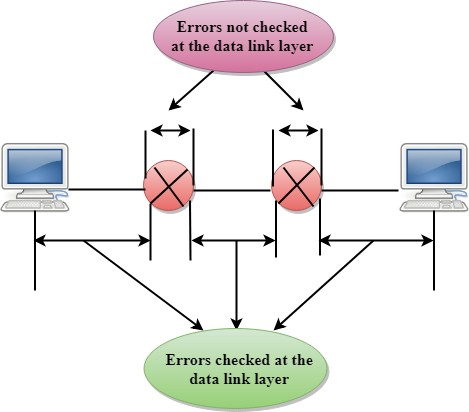
###### The reliable delivery has four aspects:

* 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 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

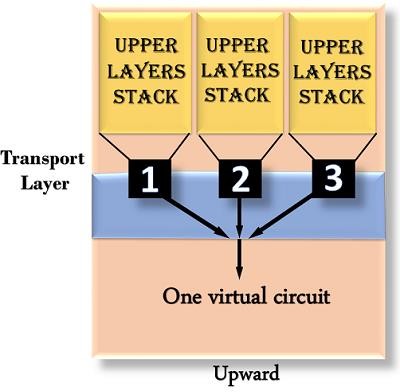
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport 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

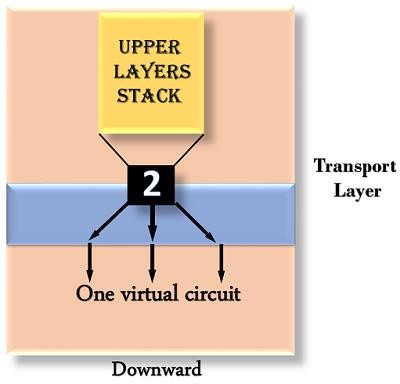
The transport layer uses the multiplexing to improve transmission efficiency.

###### 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.

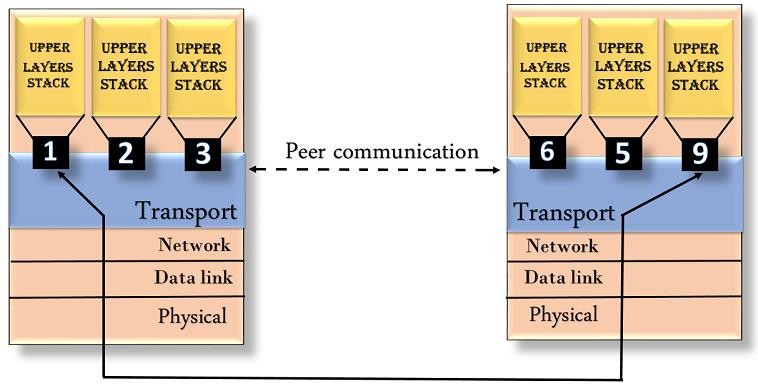


* **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low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



## TCPTCP Header format

* **Source port:** It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.
* **Destination port:** It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.
* **Sequence number:** This field contains the sequence number of data bytes in a particular session.
* **Acknowledgment number:** When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.
* **HLEN:** It specifies the length of the header indicated by the 4-byte words in the header. The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15.
* **Reserved:** It is a 4-bit field reserved for future use, and by default, all are set to zero.

###### Flags

**There are six control bits or flags:**

* 1. **URG:** It represents an urgent pointer. If it is set, then the data is processed urgently.
  2. **ACK:** If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.
  3. **PSH:** If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
  4. **RST:** If it is set, then it requests to restart a connection.
  5. **SYN:** It is used to establish a connection between the hosts.
  6. **FIN:** It is used to release a connection, and no further data exchange will happen.

###### Windowsize

It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.

###### Checksum

It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.

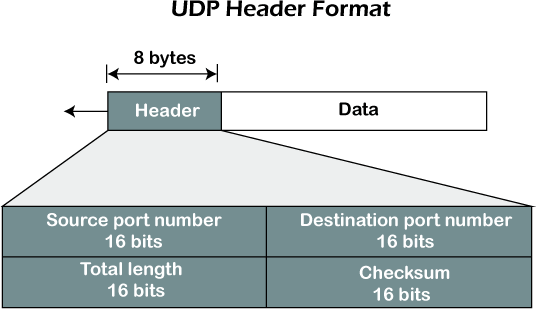
###### Urgentpointer

It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.

###### Options

It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

## UDP Header Format

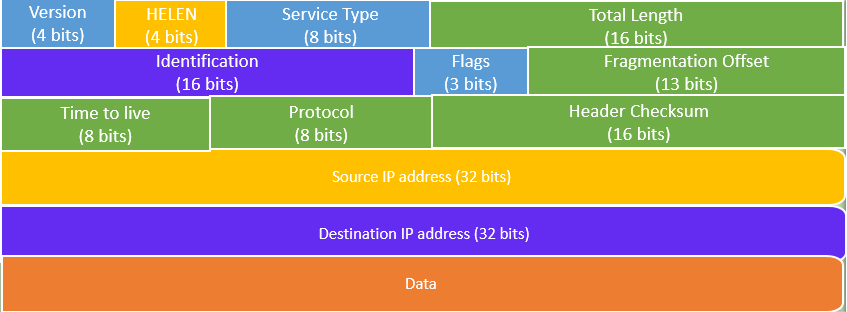


In UDP, the header size is 8 bytes, and the packet size is upto 65,535 bytes. But this packet size is not possible as the data needs to be encapsulated in the IP datagram, and an IP packet, the header size can be 20 bytes; therefore, the maximum of UDP would be 65,535 minus 20. The size of the data that the UDP packet can carry would be 65,535 minus 28 as 8 bytes for the header of the UDP packet and 20 bytes for IP header.

###### The UDP header contains four fields:

* **Source port number:** It is 16-bit information that identifies which port is going t send the packet.
* **Destination port number:** It identifies which port is going to accept the information. It is 16-bit information which is used to identify application-level service on the destination machine.
* **Length:** It is 16-bit field that specifies the entire length of the UDP packet that includes the header also. The minimum value would be 8-byte as the size of the header is 8 bytes.
* **Checksum:** It is a 16-bits field, and it is an optional field. This checksum field checks whether the information is accurate or not as there is the possibility that the information can be corrupted while transmission. It is an optional field, which means that it depends upon the application, whether it wants to write the checksum or not. If it does not want to write the checksum, then all the 16 bits are zero; otherwise, it writes the checksum. In UDP, the checksum field is applied to the entire packet, i.e., header as well as data part whereas, in IP, the checksum field is applied to only the header field.

**IPv4 Header Components/Fields**

IP

header format

#### Following are various components/fields of IP packet header

* **Version:** The first IP header field is a 4-bit version indicator. In IPv4, the value of its four bits is set to 0100, which indicates 4 in binary. However, if the router does not support the specified version, this packet will be dropped.
* **Internet Header Length:** Internet header length, shortly known as IHL, is 4 bits in size. It is also called HELEN (Header Length). This IP component is used to show how many 32-bit words are present in the header.
* **Type of Service:** Type of Service is also called Differentiated Services Code Point or DSCP. This field is provided features related to the quality of service for data streaming or VoIP calls. The first 3 bits are the priority bits. It is also used for specifying how you can handle Datagram.
* **Total length:** The total length is measured in bytes. The minimum size of an IP datagram is 20 bytes and the maximum, it can be 65535 bytes . HELEN and Total length can be used to calculate the dimension of the payload. All hosts are required to be able to read 576-byte datagrams. However, if a datagram is too large for the hosts in the network, the fragmentation method is widely used.
* **Identification:** Identification is a packet that is used to identify fragments of an IP datagram uniquely. Some have recommended using this field for other things like adding information for packet tracing, etc.
* **IP Flags:** Flag is a three-bit field that helps you to control and identify fragments. The following can be their possible configuration:

Bit 0: is reserved and has to be set to zero Bit 1: means do not fragment

Bit 2: means more fragments.

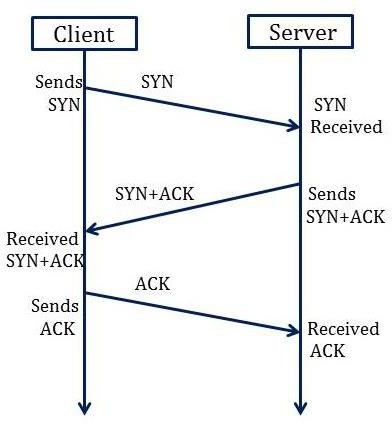
* **Fragment Offset:** Fragment Offset represents the number of Data Bytes ahead of the particular fragment in the specific Datagram. It is specified in terms of the number of 8 bytes, which has a maximum value of 65,528 bytes.
* **Time to live:** It is an 8-bit field that indicates the maximum time the Datagram will be live in the internet system. The time duration is measured in seconds, and when the value of TTL is zero, the Datagram will be erased. Every time a datagram is processed its TTL value is decreased by one second. TTL are used so that datagrams are not delivered and discarded automatically. The value of TTL can be 0 to 255.
* **Protocol:** This IPv4 header is reserved to denote that internet protocol is used in the latter portion of the Datagram. For Example, 6 number digit is mostly used to indicate TCP, and 17 is used to denote the UDP protocol.
* **Header Checksum:** The next component is a 16 bits header checksum field, which is used to check the header for any errors. The IP header is compared to the value of its checksum. When the header checksum is not matching, then the packet will be discarded.
* **Source Address:** The source address is a 32-bit address of the source used for the IPv4 packet.
* **Destination address:** The destination address is also 32 bit in size stores the address of the receiver.
* **IP Options:** It is an optional field of IPv4 header used when the value of IHL (Internet Header Length) is set to greater than 5. It contains values and settings related with security, record route and time stamp, etc. You can see that list of options component ends with an End of Options or EOL in most cases.
* **Data:** This field stores the data from the protocol layer, which has handed over the data to the IP layer.

**3-Way Handshake**

Transmission Control Protocol (TCP) provides a secure and reliable connection between two devices using the 3-way handshake process. TCP uses the full-duplex connection to synchronize (SYN) and acknowledge (ACK) each other on both sides. There are three steps for both establishing and closing a connection. They are − SYN, SYN-ACK, and ACK.

# Way Handshake Connection Establishment Process

The following diagram shows how a reliable connection is established using 3-way handshake. It will support communication between a web browser on the client and server sides whenever a user navigates the Internet.



### Synchronization Sequence Number (SYN) − The client sends the SYN to the server

* + When the client wants to connect to the server, then it sends the message to the server by setting the SYN flag as 1.
  + The message carries some additional information like the sequence number (32-bit random number).
  + The ACK is set to 0. The maximum segment size and the window size are also set. For example, if the window size is 1000 bits and the maximum segment size is 100 bits, then a maximum of 10 data segments can be transmitted in the connection by dividing (1000/100=10).

### Synchronization and Acknowledgement (SYN-ACK) to the client

* + The server acknowledges the client request by setting the ACK flag to 1.
  + The ACK indicates the response of the segment it received and SYN indicates with what sequence number it will start the segments.
  + For example, if the client has sent the SYN with sequence number = 500, then the server will send the ACK using acknowledgment number = 5001.
  + The server will set the SYN flag to '1' and send it to the client if the server also wants to establish the connection.
  + The sequence number used for SYN will be different from the client's SYN.
  + The server also advertises its window size and maximum segment size to the client. And, the connection is established from the client-side to the server-side.

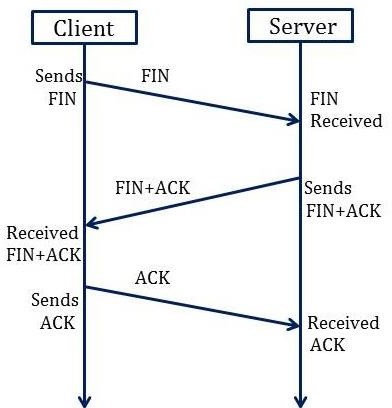
### Acknowledgment (ACK) to the server

* + The client sends the acknowledgment (ACK) to the server after receiving the synchronization (SYN) from the server.
  + After getting the (ACK) from the client, the connection is established between the client and the server.
  + Now the data can be transmitted between the client and server sides.

### 3 -Way Handshake Closing Connection Process

To close a 3-way handshake connection,

* First, the client requests the server to terminate the established connection by sending FIN.
* After receiving the client request, the server sends back the FIN and ACK request to the client.
* After receiving the FIN + ACK from the server, the client confirms by sending an ACK to the server.



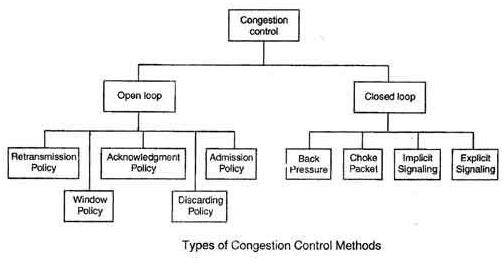
**Congestion Control**

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.). Network congestion occurs in case of traffic overloading.

In other words when too much traffic is offered, congestion sets in and performance degrades sharply

##### How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



##### Open Loop Congestion Control

* In this method, policies are used to prevent the congestion before it happens.
* Congestion control is handled either by the source or by the destination.
* The various methods used for open loop congestion control are:

##### Retransmission Policy

* The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.
* However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.
* The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

##### Window Policy

* To implement window policy, selective reject window method is used for congestion control.
* Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.
* Selective reject method sends only the specific lost or damaged packets.

##### Acknowledgement Policy

* The acknowledgement policy imposed by the receiver may also affect congestion.
* If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.
* Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgements we can reduce load on the network.
* To implement it, several approaches can be used:

1. A receiver may send an acknowledgement only if it has a packet to be sent.
2. A receiver may send an acknowledgement when a timer expires.
3. A receiver may also decide to acknowledge only *N* packets at a time.

##### Discarding Policy

* A router may discard less sensitive packets when congestion is likely to happen.
* Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

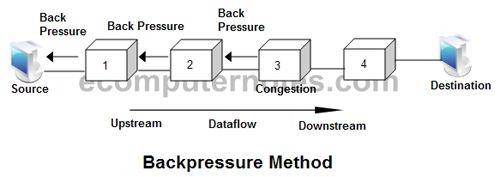
##### Admission Policy

* An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.
* Switches in a flow first check the resource requirement of a flow before admitting it to the network.
* A router can deny establishing a virtual circuit connection if there is congestion in the “network or if there is a possibility of future congestion.

##### ClosedLoop CongestionControl

* Closed loop congestion control mechanisms try to remove the congestion after it happens.
* The various methods used for closed loop congestion control are:

##### Backpressure

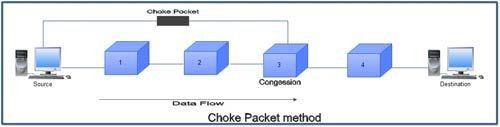
* Back pressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.
  + The

backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.

* In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.
* This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.
* As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is alleviated. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

##### ChokePacket

* In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.
* Here, congested node does not inform its upstream node about the congestion as in backpressure method.
* In choke packet method, congested node sends a warning directly to the source station *i.e.* the intermediate nodes through which the packet has traveled are not warned.



##### Implicit Signaling

* In implicit signaling, there is no communication between the congested node or nodes and the source.
* The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.
* On sensing this congestion, the source slows down.
* This type of congestion control policy is used by TCP.

##### Explicit Signaling

* In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.
* Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .
* Explicit signaling can occur in either the forward direction or the backward direction .
* In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.
* In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

**Leaky bucket algorithm**

In the network layer, before the network can make Quality of service guarantees, it must know what traffic is being guaranteed. One of the main causes of congestion is that traffic is often bursty.

To understand this concept first we have to know little about traffic shaping. **Traffic Shaping** is a mechanism to control the amount and the rate of traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate the rate of data transmission and reduces congestion.

There are 2 types of traffic shaping algorithms:

1. Leaky Bucket
2. Token Bucket

Leaky Bucket Algorithm mainly controls the total amount and the rate of the traffic sent to the network.

**Step 1** − Let us imagine a bucket with a small hole at the bottom where the rate at which water is poured into the bucket is not constant and can vary but it leaks from the bucket at a constant rate.

**Step 2** − So (up to water is present in the bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.

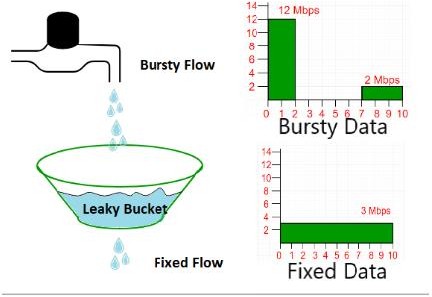
**Step 3** − If the bucket is full, additional water that enters into the bucket that spills over the sides and is lost.

**Step 4** − Thus the same concept applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 10 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 8 Mbps for 2 seconds. Thus, in a time span of 8 seconds, 68 Mb data has been transmitted.

That’s why if a leaky bucket algorithm is used, the data flow would be 8 Mbps for 9 seconds. Thus, the constant flow is maintained.

Suppose we have a bucket in which we are pouring water, at random points in time, but we have to get water at a fixed rate, to achieve this we will make a hole at the bottom of the bucket. This will ensure that the water coming out is at some fixed rate, and also if the bucket gets full, then we will stop pouring water into it.

The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.



In the above figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In the above figure, the host sends a burst of data at a rate of 12 Mbps for 2s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in 10 s. The leaky bucket smooths out the traffic by sending out data at a rate of 3 Mbps during the same 10 s.

Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.

A simple leaky bucket algorithm can be implemented using FIFO queue. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

# Token Bucket Algorithm

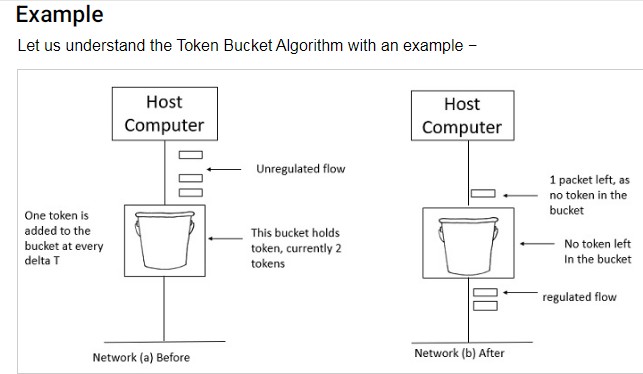
The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is. So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.

Let us understand this algorithm step wise as given below −

* + **Step 1** − In regular intervals tokens are thrown into the bucket f.
  + **Step 2** − The bucket has a maximum capacity f.
  + **Step 3** − If the packet is ready, then a token is removed from the bucket, and the packet is sent.
  + **Step 4** − Suppose, if there is no token in the bucket, the packet cannot be sent.

# Example

Let us understand the Token Bucket Algorithm with an example −



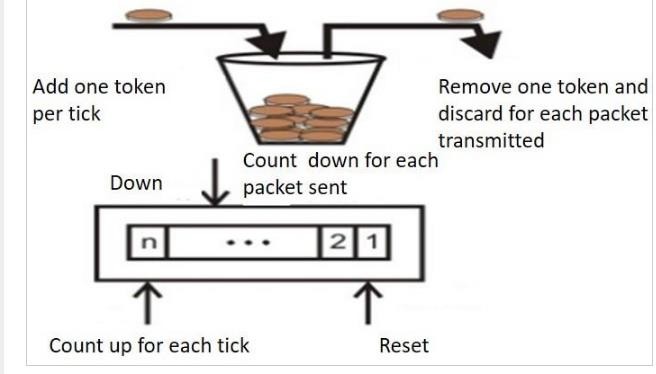
In figure (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface.

In Figure (b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

When compared to Leaky bucket the token bucket algorithm is less restrictive that means it allows more traffic. The limit of busyness is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of the token bucket algorithm is easy − a variable is used to count the tokens. For every t seconds the counter is incremented and then it is decremented whenever a packet is sent. When the counter reaches zero, no further packet is sent out.

This is shown in below given diagram −



##### Difference between Leaky and Token buckets –

|  |  |
| --- | --- |
| Leaky Bucket | Token Bucket |
| When the host has to send a packet , packet is thrown in bucket. | In this, the bucket holds tokens generated at regular intervals of time. |
| Bucket leaks at constant rate | Bucket has maximum capacity. |
| Bursty traffic is converted into uniform traffic by leaky bucket. | If there is a ready packet , a token is removed from Bucket and packet is send. |
| In practice bucket is a finite queue outputs at finite rate | If there is no token in the bucket, then the packet cannot be sent. |

**Some advantage of token Bucket over leaky bucket**

* If a bucket is full in tokens Bucket, tokens are discard not packets. While in leaky bucket, packets are discarded.
* Token Bucket can send large bursts at a faster rate while leaky bucket always sends packets at constant rate.

**Session Layer**

– Session layer allows two systems to enter into a dialog exchange mechanism which can either be full or half-duplex.

* 1. Managing Tokens –

The communicating systems in a network try to perform some critical operations and it is Session Layer

which prevents collisions which might occur while performing these operations which would otherwise result in a loss.

* 1. Synchronization –

Checkpoints are the midway marks that are added after a particular interval during stream of data

transfer. These points are also referred to as synchronization points. The Session layer permits process to add these checkpoints.

For example, suppose a file of 400 pages is being sent over a network, then it is highly beneficial to set up a checkpoint after every 50 pages so that next 50 pages are sent only when previous pages are received and acknowledged.

Design Issues with Session Layer :

1. Establish sessions between machines –

The establishment of session between machines is an important service provided by session layer. This session is responsible for creating a dialog between connected machines. The Session Layer provides mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi- permanent dialogue. This session consists of requests and responses that occur between applications.

1. Enhanced Services –

Certain services such as checkpoints and management of tokens are the key features of session layer and thus it becomes necessary to keep enhancing these features during the layer’s design.

1. To help in Token management and Synchronization –

The session layer plays an important role in preventing collision of several critical operation as well as ensuring better data transfer over network by establishing synchronization points at specific intervals. Thus it becomes highly important to ensure proper execution of these services.

## Timer

TCP uses several timers to ensure that excessive delays are not encountered during communications. Several of these timers are elegant, handling problems that are not immediately obvious at first analysis. Each of the timers used by TCP is examined in the following sections, which reveal its role in ensuring data is properly sent from one connection to another.

## TCP implementation uses four timers –

* **Retransmission Timer –** To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received. If the timer expires timeout occurs and the segment is retransmitted.
* **Deviated RTT(RTTd) –** Most implementations do not use RTTs alone so RTT deviated is also calculated to find out RTO.
* **Persistent Timer –** To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window

size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored in calculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.

* **Keep Alive Timer –** A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash. In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. If the server does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.
* **Time Wait Timer –** This timer is used during [tcp connection termination](https://www.geeksforgeeks.org/computer-network-tcp-connection-termination/). The timer starts after sending the last Ack for 2nd FIN and closing the connection.
* *After a TCP connection is closed, it is possible for datagrams that are still making their way through the network to attempt to access the closed port. The quiet timer is intended to prevent the just-closed port from reopening again quickly and receiving these last datagrams.*
* The **quiet timer** is usually set to twice the maximum segment lifetime (the same value as the Time-To-Live field in an IP header), ensuring that all segments still heading for the port have been discarded.

## Quality of service (QoS)

**Quality-of-Service (QoS)** refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions, or traffic aggregates. Basic phenomenon for QoS means in terms of packet delay and losses of various kinds.

## Need for QoS –

* Video and audio conferencing require bounded delay and loss rate.
* Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
* Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
* Valuable applications should be provided better services than less valuable applications.

## QoS Specification –

**QoS requirements can be specified as:**

Delay

Delay Variation(Jitter) Throughput

Error Rate

There are two types of QoS Solutions:

## Stateless Solutions –

**Routers maintain no fine-grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about the kind of delay or performance in a particular application which we have to encounter.**

## Stateful Solutions –

**Routers maintain a per-flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, providing protection, and is much less scalable and robust.**

## Integrated Services(IntServ) –

An architecture for providing QoS guarantees in IP networks for individual application sessions.

Relies on resource reservation, and routers need to maintain state information of allocated resources and respond to new call setup requests.

Network decides whether to admit or deny a new call setup request.

## IntServ QoS Components –

* Resource reservation: call setup signaling, traffic, QoS declaration, per-element admission control.
* QoS-sensitive scheduling e.g WFQ queue discipline.
* QoS-sensitive routing algorithm(QSPF)
* QoS-sensitive packet discard strategy.

## RSVP-Internet Signaling –

**It creates and maintains distributed reservation state, initiated by the receiver and scales for multicast, which needs to be refreshed otherwise reservation times out as it is in soft state. Latest paths were discovered through “PATH” messages (forward direction) and used by RESV messages (reserve direction).**

## Call Admission –

* Session must first declare it’s QoS requirement and characterize the traffic it will send through the network.
* **R-specification:** defines the QoS being requested, i.e. what kind of bound we want on the delay, what kind of packet loss is acceptable, etc.
* **T-specification:** defines the traffic characteristics like bustiness in the traffic.
* A signaling protocol is needed to carry the R-spec and T-spec to the routers where reservation is required.
* Routers will admit calls based on their R-spec, T-spec and based on the current resource allocated at the routers to other calls.

## Diff-Serv –

**Differentiated Service is a stateful solution in which each flow doesn’t mean a different state. It provides reduced state services i.e. maintaining state only for larger granular flows rather than end-to-end flows tries to achieve the best of both worlds.**

Intended to address the following difficulties with IntServ and RSVP:

## Flexible Service Models:

**IntServ has only two classes, want to provide more qualitative service classes: want to provide ‘relative’ service distinction.**

## Simpler signaling:

**Many applications and users may only want to specify a more qualitative notion of service.**

## Streaming Live Multimedia –

* **Examples:** Internet radio talk show, Live sporting event.
* **Streaming:** playback buffer, playback buffer can lag tens of seconds after and still have timing constraint.
* **Interactivity:** fast forward is impossible, but rewind and pause is possible.

## Traffic shaping and traffic policing

Traffic shaping, also known as packet shaping, is a congestion management method that regulates network data transfer by delaying the flow of less important or less desired [packets](https://www.techtarget.com/searchnetworking/definition/packet). It is used to optimize network performance by prioritizing certain traffic flows and ensuring the traffic rate doesn't exceed the [bandwidth](https://www.techtarget.com/searchnetworking/definition/bandwidth) limit.

Regulating the flow of packets into a network is known as data transfer throttling. Regulation of the flow of packets out of a network is known as rate limiting.

In addition to bandwidth, three major factors affect the quality of a network: [latency,](https://www.techtarget.com/whatis/definition/latency) [jitter](https://www.techtarget.com/searchunifiedcommunications/definition/jitter) and [loss](https://www.techtarget.com/searchnetworking/definition/packet-loss).

Traffic shaping attempts to prevent delay, jitter and loss by controlling the burst size and using a [leaky bucket algorithm](https://www.techtarget.com/whatis/definition/leaky-bucket-algorithm) to smooth the output rate over at least eight time intervals. If [traffic](https://www.techtarget.com/searchnetworking/definition/network-traffic) is arriving at a rate lower than the configured rate, then it will be forwarded normally. If traffic

arrives faster than the configured rate, then it will be delayed and held in a buffer until it can be sent without going over the limit.

## What is traffic shaping used for?

Traffic shaping is a quality of service ([QoS](https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service)) technique that is configured on network interfaces to allow higher-priority traffic to flow at optimal levels even when the link becomes overutilized. By creating a bandwidth limit for less critical packets, traffic shaping lessens the possibility that more important packets will be delayed or dropped as they leave the interface.

Common uses of traffic shaping include:

* Time-sensitive data may be given priority over traffic that can be delayed briefly, often with little-to-no ill effect.
* In a corporate environment, business-related traffic may be given priority over other traffic.
* A large internet service provider ([ISP](https://www.techtarget.com/whatis/definition/ISP)) may shape traffic based on customer priority.
* An ISP may limit maximum bandwidth consumption for certain applications to reduce costs and create the capacity to take on additional subscribers. This practice can effectively limit a subscriber's "unlimited connection" and is often imposed without notification.
* Traffic shaping is an integral component of the proposed two-tiered internet, in which certain customers or services receive traffic priority for a premium charge.

## Importance of traffic shaping

Traffic shaping is important when network [uplinks](https://www.techtarget.com/searchmobilecomputing/definition/downlink-and-uplink) become overwhelmed with data being sent out of an interface. Without traffic shaping, any excess traffic that cannot be sent out of an interface will either be dropped or queued, which can cause delays in all packets. This can result in poor performance of mission-critical applications. The enablement of traffic shaping allows administrators to specify certain applications that are considered less important -- and, therefore, creates intelligence around which packets will be dropped or delayed first.

Overall, traffic shaping is one of the most important traffic management techniques for ensuring high network performance.

## Traffic shaping methods

Shaping can only occur on packets that are leaving an interface as opposed to coming into the interface. The network device can use several different methods to identify the application that an IP packet exiting an interface belongs to. Based on this information, the interface can drop or hold these specific packets inside a temporary queue until a certain bandwidth limit has been reached. Shaping uses a leaky bucket algorithm to eventually release the delayed packets for delivery. While this may increase latency, it's usually more efficient compared to dropping the packets.

Traffic shaping methods include:

**Generic traffic shaping (GTS).** This method supports traffic shaping of most media and [encapsulation](https://www.techtarget.com/searchnetworking/definition/encapsulation) data types on a router. GTS will

perform traffic shaping on a per-interface basis and use access control lists ([ACLs](https://www.techtarget.com/searchsoftwarequality/definition/access-control-list)) to choose what traffic to shape;

* dynamically adapt to the available bandwidth by integrating shapes and backward explicit congestion notifications (BECNs) at a defined rate; and
* respond to resource reservation protocol ([RSVP](https://www.techtarget.com/searchnetworking/definition/RSVP)) features that are signaled over statically configured asynchronous transfer mode (ATM) permanent virtual circuits ([PVCs](https://www.techtarget.com/searchnetworking/definition/permanent-virtual-circuit)).

**Frame relay traffic shaping (FRTS).** Similar to GTS, FRTS eliminates [bottlenecks](https://www.techtarget.com/searchnetworking/definition/bottleneck) occurring in frame relay networks with high-speed connections at the central site and low speeds at the branch sites.

**Class-based traffic shaping.** This method allows users to configure traffic shaping on a per- traffic-class basis, meaning the shaping can be specified to one or more categories of data. Class-based shaping also enables users to optimize the available bandwidth by specifying an average or peak rate for shaping. This will allow more data than the configured rate to be sent if bandwidth is available. Finally, the class-based shaping method allows users to create a hierarchical policy map structure. This means traffic shaping can be placed in a primary policy map while other QoS features are placed in a secondary policy map.

## Traffic shaping vs. traffic policing

Traffic shaping impacts packets leaving an interface. Packets determined to be less important are temporarily stored in a buffer queue and sent more slowly using a leaky bucket technique. Traffic policing, on the other hand, can be configured for both traffic exiting and entering an interface. Policing will simply drop packets as opposed to storing them in a temporary queue. Thus, policing is considered less efficient in most cases.