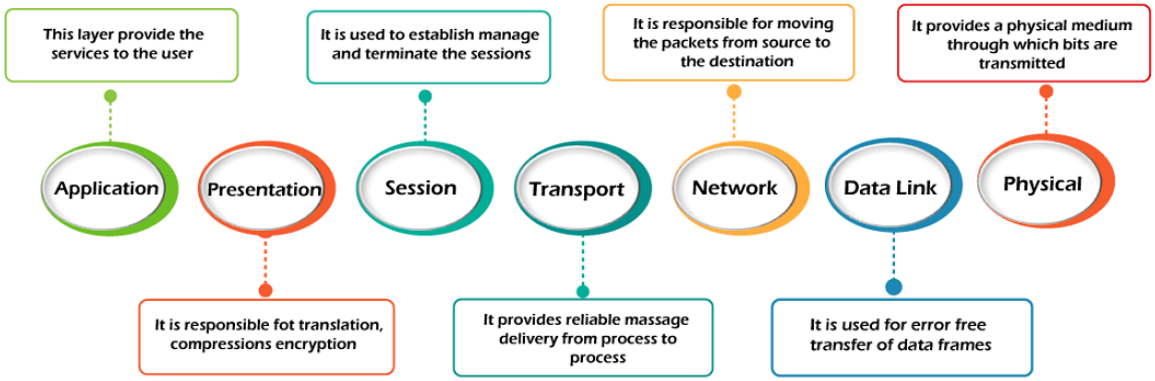
OSI MODEL

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

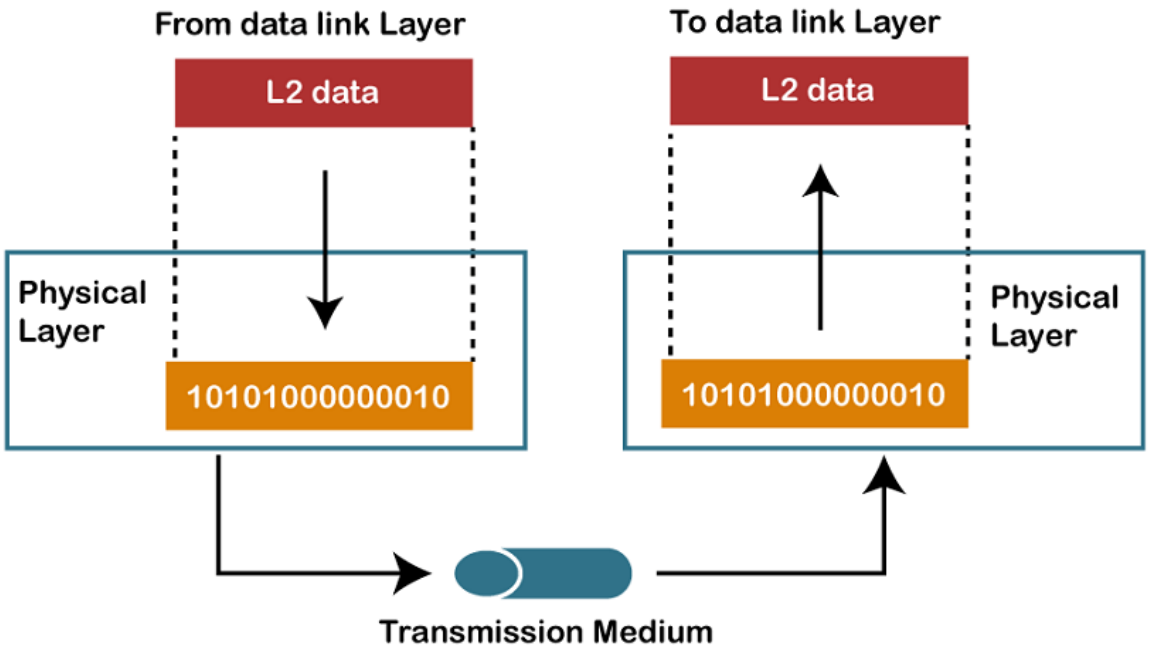
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



1) Physical layer



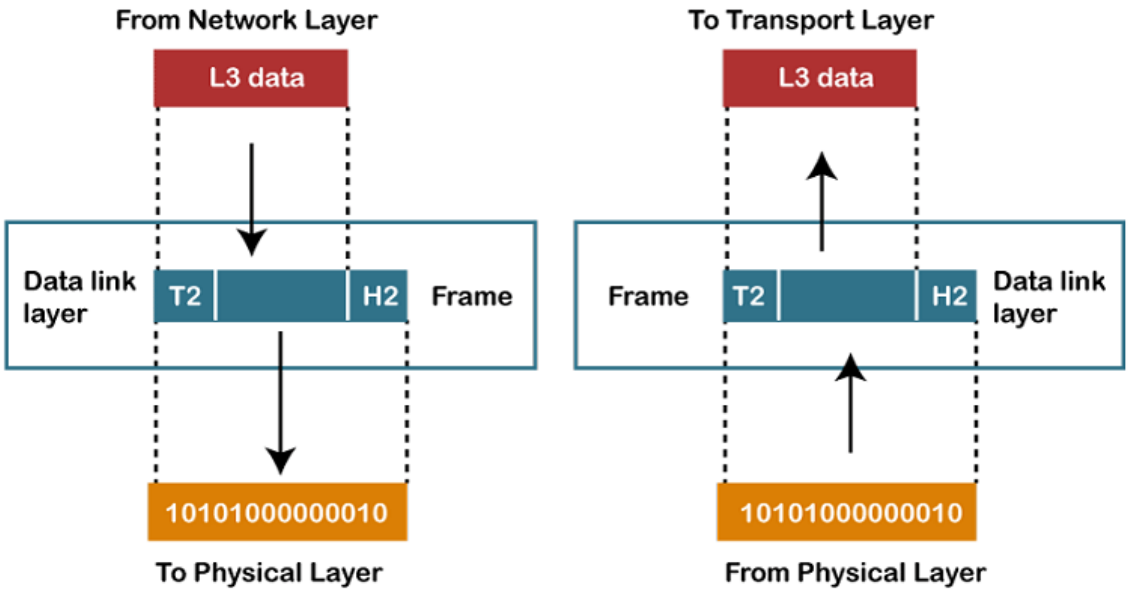
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- Line Configuration: It defines the way how two or more devices can be connected physically.

- Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- Topology: It defines the way how network devices are arranged.
- Signals: It determines the type of the signal used for transmitting the information.

2) Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - Logical Link Control Layer
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.

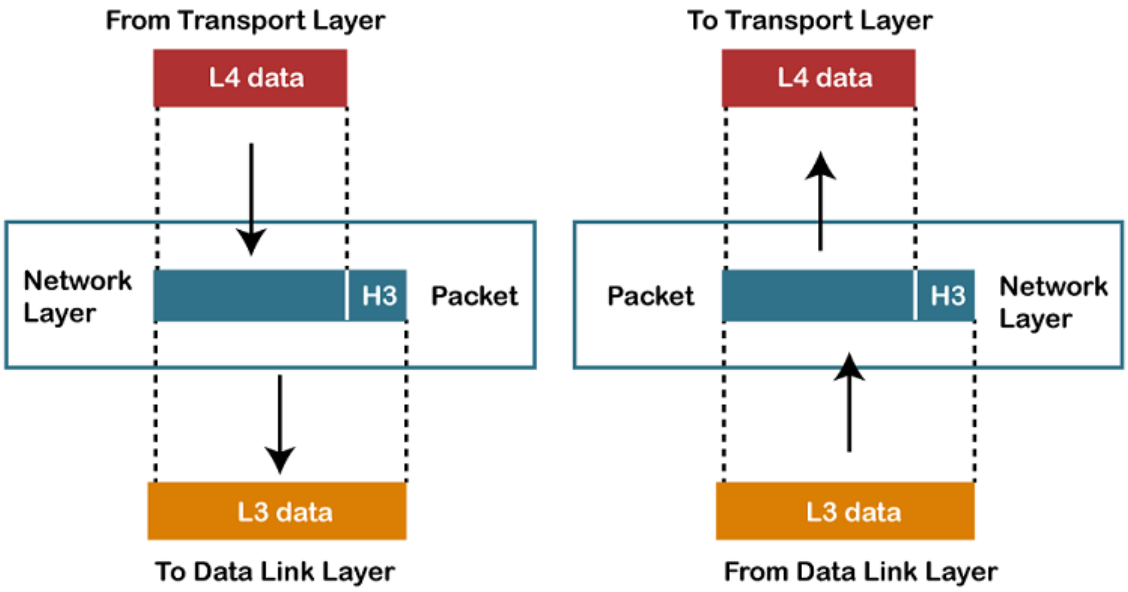
        - It also provides flow control.
    - Media Access Control Layer
        - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - It is used for transferring the packets over the network.

Functions of the Data-link layer

- Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer



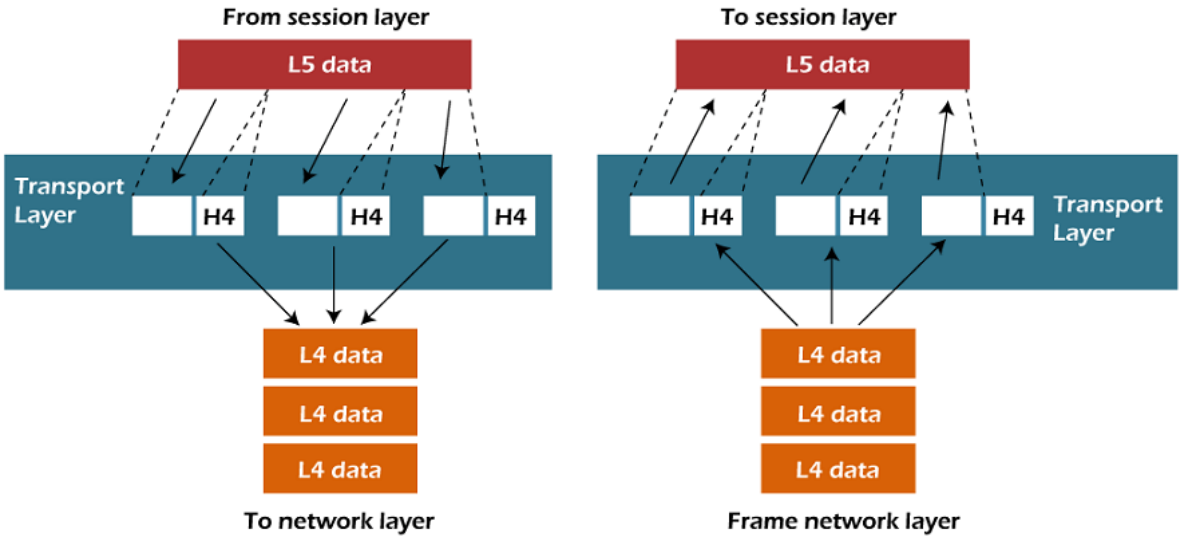
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

- Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- Transmission Control Protocol
    - It is a standard protocol that allows the systems to communicate over the internet.
    - It establishes and maintains a connection between hosts.
    - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission

control protocol reorders the packets in the correct order at the receiving end.

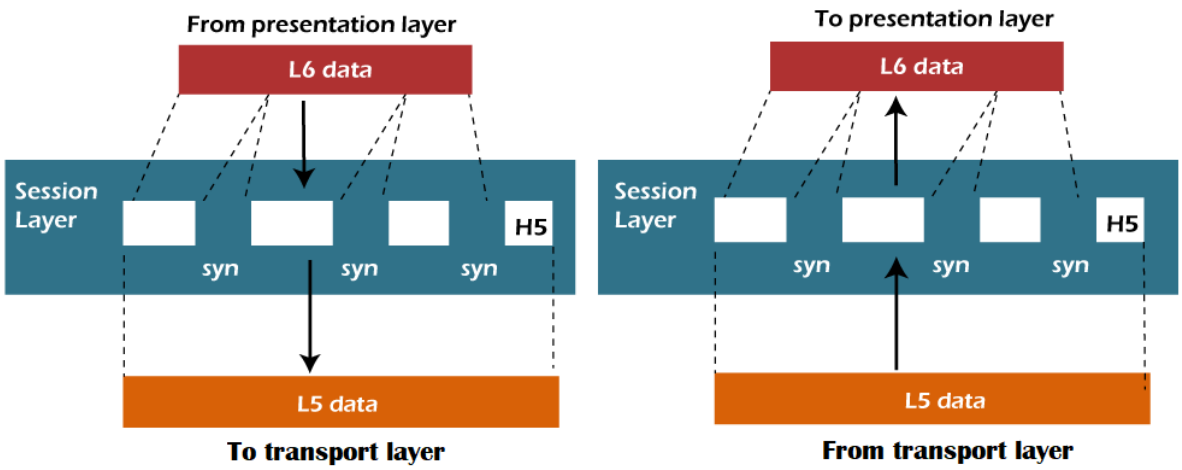
- User Datagram Protocol
    - User Datagram Protocol is a transport layer protocol.
    - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- Service-point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- Flow control: The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link.

The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

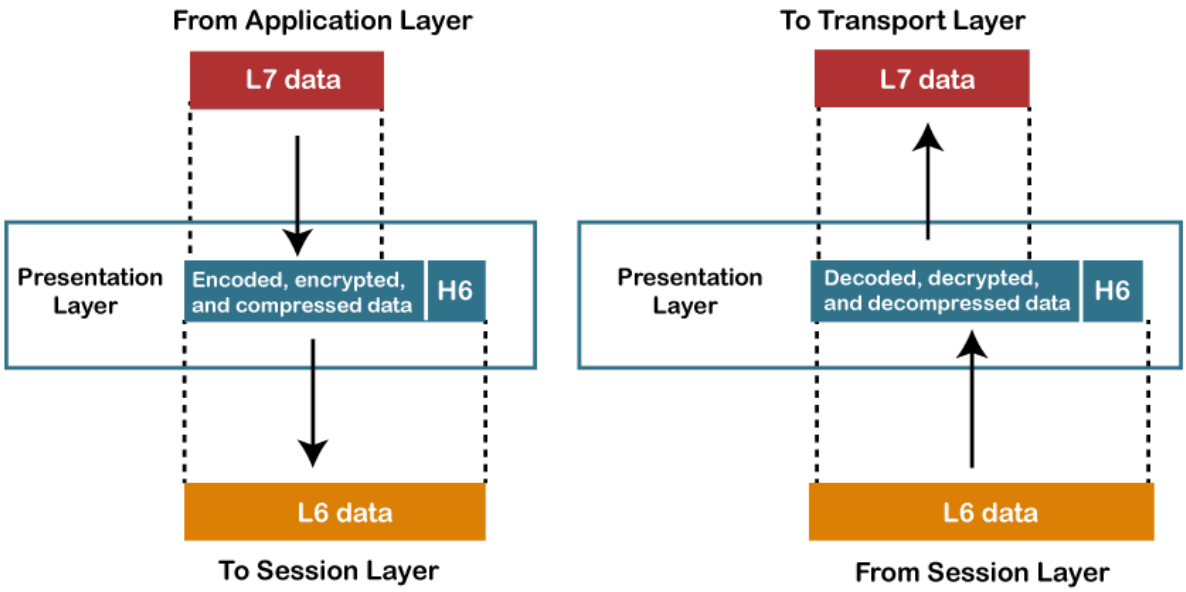


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer

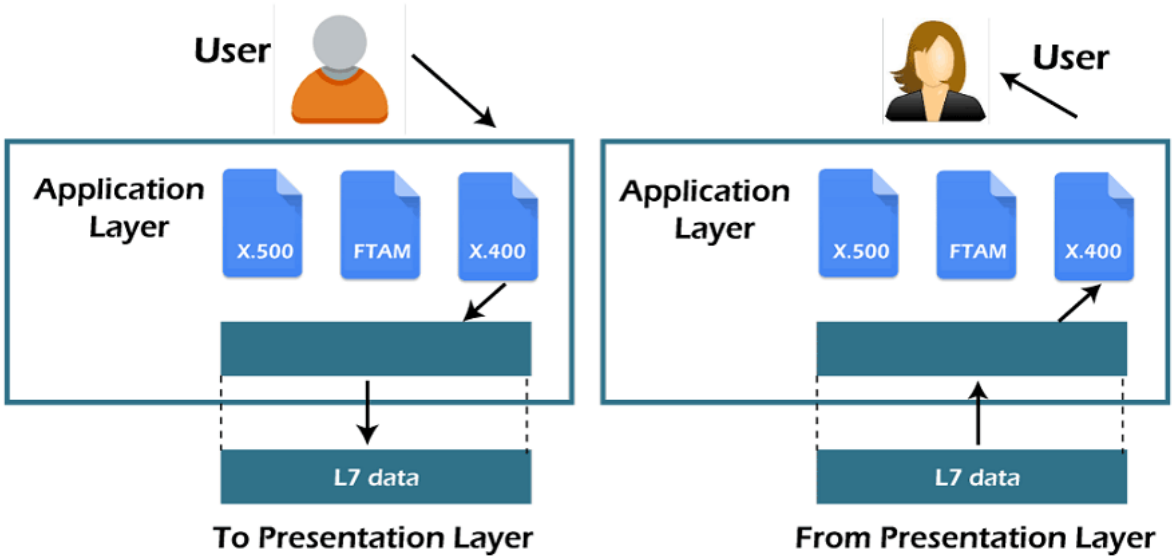


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- Translation: The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- Encryption: Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- Compression: Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- Mail services: An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

Network Layer Design Issues

The network layer comes with some design issues that are described as follows:

1. Store and Forward packet switching

The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called “Store and Forward packet switching.”

2. Services provided to the Transport Layer

Through the network/transport layer interface, the network layer transfers its **patterns** services to the transport layer. These services are described below. But before providing these services to the transfer layer, the following goals must be kept in mind:-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number, and topology of the available router.
- The network addresses for the transport layer should use uniform numbering patterns**,** also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into the subnet are done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service

Packets are termed as “datagrams” and corresponding subnets as “datagram subnets”. When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to the router via. a few protocols. Each data packet has a destination address and is routed independently irrespective of the packets.

4. Implementation of Connection-Oriented service:

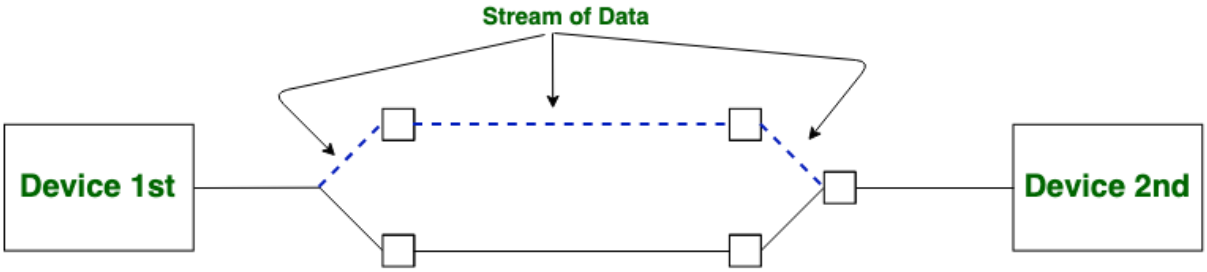
To use a connection-oriented service, first, we establish a connection, use it, and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender. It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then the data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Connection-less vs Connection-Oriented

Both Connection-less and Connection-Oriented are used for the connection establishment between two or more devices. These types of services are provided by the Network Layer.

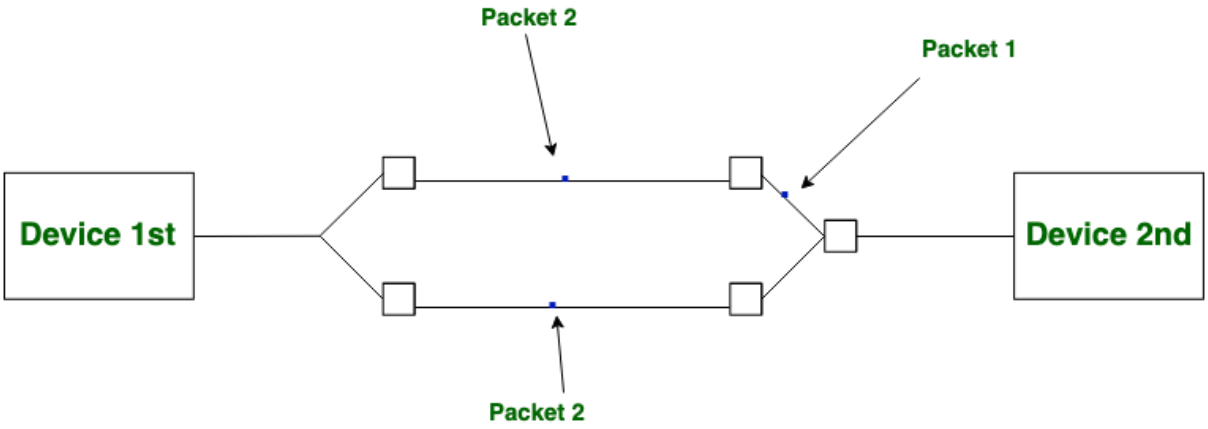
Connection-oriented service: In connection-Oriented service we have to establish a connection between sender and receiver before communication. Handshske method is used to establish a connection between sender and receiver. Connection-Oriented service include both connection establishment as well as connection termination phase. Real life example of this service is telephone service, for conversation we have to first establish a connection**.**



CONNECTION-ORIENTED SERVICE

Connection-Oriented Service

Connection-less service: In Connection-Less service no need of connection establishment and connection termination. This Service does not give a guarantee of reliability. In this service, Packets may follow the different path to reach their destination. Real life examples of this service is postal system, Online gaming, real-time video and audio streaming etc.



CONNECTIONIESS SERVICE

What is a Distance Vector Routing Algorithm?

Distance vector routing algorithm is a type of routing algorithm that is used to determine the best path for data packets to travel through a network. This algorithm is also known as Bellman-Ford Algorithm.

The distance vector routing algorithm works by each router in a network maintaining a table of the distances to all other routers in the network. This table is called the distance vector. The distance vector contains the distance to all the other routers in the network as well as the next hop router that the data packet should be sent to in order to reach its destination.

How Distance Vector Routing Protocol Works

The Distance Vector Routing protocol follows these basic steps:

1. **Initialization:** Each router in the network is configured with its own distance vector table, which lists the distance (in terms of hop count or other metrics) to every other network in the inter-network.
2. **Sending distance vectors:** Each router sends its distance vector table to its immediate neighbors.
3. **Updating distance vectors:** Upon receiving a distance vector from a neighbor, a router updates its own table by comparing the distance to a network via its neighbor with the distance currently listed in its own table. If the new distance is shorter, the router updates its table with the new information.

4. **Calculating best path:** Using the information in its distance vector table, each router calculates the best path to each network and updates its routing table accordingly.
5. **Periodic updates:** The sending and updating distance vectors are repeated periodically, typically every 30 seconds. This allows the network to adapt to changes in topology quickly.
6. **Convergence:** The process of sending and updating distance vectors continues until all routers in the network have the most up-to-date information and have converged on the best path to each network.

AND THEIR EXAMPLE THAT I TEACH IN CLASS.

Link State Routing

Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work.

Link state routing has two phase:

1. **Reliable Flooding: Initial state**– Each node knows the cost of its neighbors. Final state- Each node knows the entire graph.
2. **Route Calculation**: Each node uses Dijkstra' s algorithm on the graph to calculate the optimal routes to all nodes. The link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

EXAMPLE OF LINK STATE: https://youtu.be/kW6zV-040SY

Hierarchical State Routing Protocol

The hierarchical state routing protocol (HSR) is a multi-level and distributed routing protocol. It makes use of clustering, present on different levels. Each

level of cluster has the potential to manage its members efficiently. This improves resource allocation and management. Leaders are elected in each cluster, which form the members of the immediate higher level.

Working of HSRP

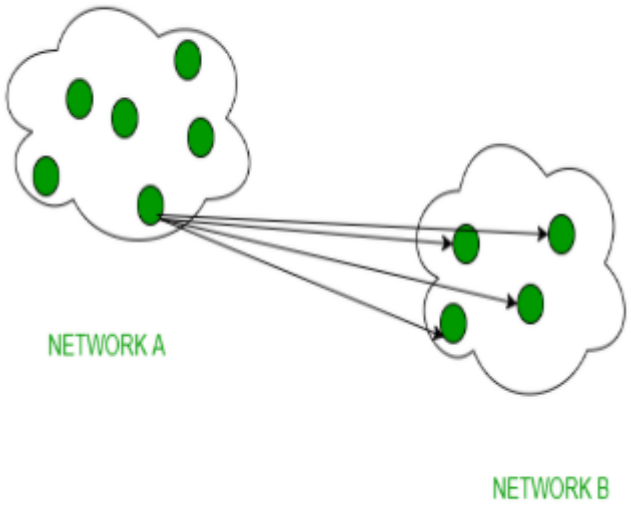
- Each node maintains information about its neighboring node and their link status
- The information regarding the cluster is broadcast in the network at regular intervals.
- The job of the cluster leader is to exchange topology and link state routing information among other cluster leaders of neighborhood clusters.
- The exchange of link state information is carried out over multiple hops that consist of gateway nodes and cluster-heads.
- The path between two cluster-heads which is formed by multiple wireless links is called virtual link.
- The link status for the virtual link(otherwise called tunnel) is obtained from the link status parameters of the wireless links that constitute the virtual link.
- After obtaining information from its peers, the cluster head floods the information to the lower levels.
- Hierarchical addressing in HSR reduces routing information compared to link-state routing. HSR's HID and node ID structure simplifies addressing and topology management.
- HSR tables update with received routing packets, maintaining accurate hierarchy information.

EXAMPLE : https://youtu.be/Y9ZoeWuHk78

Broadcast Routing

Broadcast routing plays a role, in computer networking and telecommunications. It involves transmitting data, messages, or signals from one source to destinations within a network. Unlike routing (one-to-one communication) or multicast routing (one-to-many communication) broadcast routing ensures that information reaches all devices or nodes within the network.

In this article, we will explore the world of broadcast routing in today's era of communication.



Mechanisms for Broadcast Routing

The mechanisms and protocols are employed to efficiently distribute data to multiple recipients through broadcast routing. Here are some important methods:

- **Flooding:** Flooding is an approach to broadcast routing. In this method, the sender broadcasts the message to all connected devices, which then forwards it to their connected devices and so on. This continues until the message reaches all intended recipients or a predefined maximum number of hops is reached. However flooding can lead to network congestion and inefficiency.
- **Spanning Tree Protocol (STP):** STP is utilized in Ethernet networks to prevent loops and ensure broadcast routing. It establishes a tree structure

that connects all devices, in the network while avoiding paths. Reducing network congestion and avoiding broadcast messages are the benefits of implementing this approach.

- **The Internet Group Management Protocol (IGMP):** It is a communication protocol utilized in IP networks to facilitate the management of group memberships. Its purpose is to enable hosts to join or leave groups ensuring that only interested recipients receive the multicast traffic. This not enhances network efficiency. Also prevents unnecessary data transmission.
- **Broadcast Domains:** Segmenting a network into broadcast domains also known as subnetting is a way to manage and control the scope of broadcast messages. By dividing a network into segments we can contain the impact of broadcast traffic within each segment minimizing its overall effect, on the entire network.

CONGESTION CONTROL

Congestion control is a crucial concept in computer networks. It refers to the methods used to prevent network overload and ensure smooth data flow. When too much data is sent through the network at once, it can cause delays and data loss. Congestion control techniques help manage the traffic, so all users can enjoy a stable and efficient network connection. These techniques are essential for maintaining the performance and reliability of modern networks.

What is Congestion?

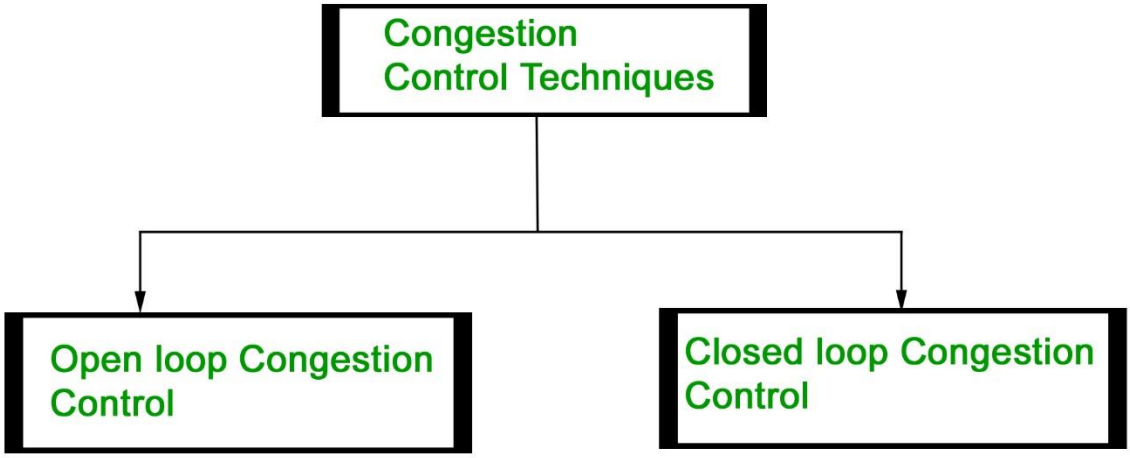
Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss. When the network can't handle all the incoming data, it gets "clogged," making it difficult for information to travel smoothly from one place to another.

Congestion Control techniques in Computer Networks

Last Updated : 26 Jun, 2022

-
-
-

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

1. **Retransmission Policy :**
   It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy :**
   The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. **Acknowledgment Policy :**
   Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

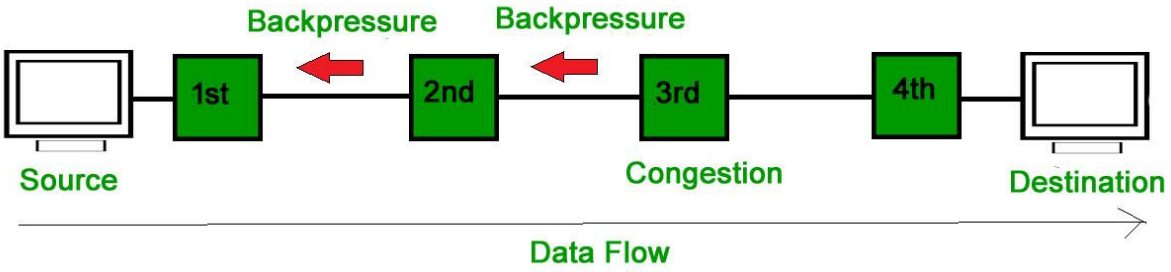
5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

Closed Loop Congestion Control

Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

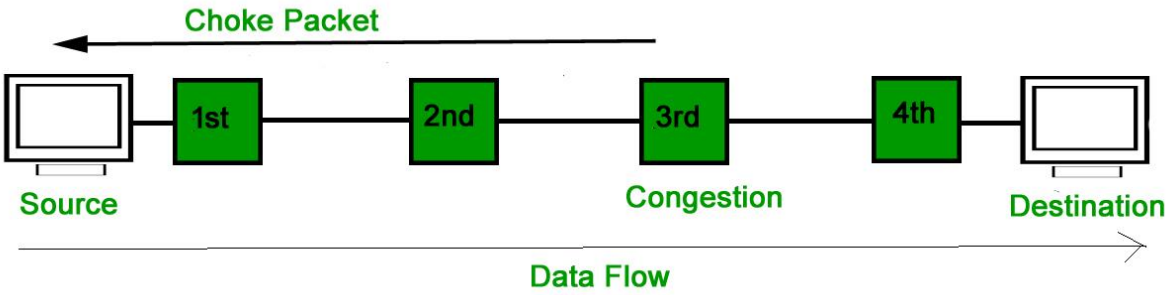
1. Backpressure :
Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique :

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



3. Implicit Signaling :

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling :

In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique.

Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling :** In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signaling :** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

- **Congestion control in data-gram and sub-nets :**
  Some congestion Control approaches which can be used in the datagram Subnet (and also in virtual circuit subnets) are given under.
  1. Choke packets
  2. Load shedding
  3. Jitter control.

Approach-1: Choke Packets :

- This approach can be used in virtual circuits as well as in the datagram sub-nets. In this technique, each router associates a real variable with each of its output lines.
- This real variable says u has a value between 0 and 1, and it indicates the percentage utilization of that line. If the value of the variable goes above the threshold then the output line will enter into a warning state.
- The router will check each newly arriving packet to see if its output line is in the warning state. if it is in the warning state then the router will send back choke packets. Several variations on the congestion control algorithm have been proposed depending on the value of thresholds.

- Depending upon the threshold value, the choke packets can contain a mild warning a stern warning, or an ultimatum. Another variation can be in terms of queue lengths or buffer utilization instead of using line utilization as a deciding factor

Drawback –
The problem with the choke packet technique is that the action to be taken by the source host on receiving a choke packet is voluntary and not compulsory.

Approach-2: Load Shedding :

- Admission control, choke packets, and fair queuing are the techniques suitable for congestion control. But if these techniques cannot make the congestion disappear, then the load-shedding technique is to be used.
- The principle of load shedding states that when the router is inundated by packets that it cannot handle, it should simply throw packets away.
- A router flooded with packets due to congestion can drop any packet at random. But there are better ways of doing this.
- The policy for dropping a packet depends on the type of packet. For file transfer, an old packet is more important than a new packet In contrast, for multimedia, a new packet is more important than an old one So.the policy for file transfer is called wine (old is better than new), and that for the multimedia is called milk (new is better than old).
- An intelligent discard policy can be decided depending on the applications. To implement such an intelligent discard policy, cooperation from the sender is essential.
- The application should mark their packets in priority classes to indicate how important they are.
- If this is done then when the packets are to be discarded the routers can first drop packets from the lowest class (i.e. the packets which are least important). Then the routers will discard the packets from the next lower class and so on. One or more header bits are required to put the priority to make the class of a packet. In every ATM cell, 1 bit is reserved in the header for marking the priority. Every ATM cell is labeled either as a low priority or high priority.

Approach-3: Jitter control :

- Jitter may be defined as the variation in delay for the packet belonging to the same flow. The real-time audio and video cannot tolerate jitter on the other hand the jitter doesn't matter if the packets are carrying information contained in a file.
- For the audio and video transmission, if the packets take 20 ms to 30 ms delay to reach the destination, it doesn't matter, provided that the delay remains constant.
- The quality of sound and visuals will be hampered by the delays associated with different packets having different values. Therefore, practically we can say that 99% of packets should be delivered with a delay ranging from 24.5 ms to 25.5 ms.
- When a packet arrives at a router, the router will check to see whether the packet is behind or ahead and by what time.
- This information is stored in the packet and updated at every hop. If a packet is ahead of the schedule then the router will hold it for a slightly longer time and if the packet is behind schedule, then the router will try to send it out as quickly as possible. This will help in keeping the average delay per packet constant and will avoid time jitter.

What is the Leaky Bucket Algorithm?

The Leaky Bucket Algorithm is a simple yet effective algorithm designed to regulate the flow of data through a network. It is often used in scenarios where a constant and controlled data rate is essential. The concept behind the algorithm is analogous to a leaky bucket filled with water. In this analogy, the water represents incoming data, and the bucket represents the buffer or storage.

How Leaky Bucket Algorithm Works?

1. Bucket and Leakage:

- The "bucket" has a fixed capacity, representing the maximum amount of data that can be stored or transmitted at any given time.
- Data is added to the bucket at a variable rate.

- The bucket has a leak, allowing data to flow out at a constant rate, regardless of the input rate.

2. Token-Based System:

- The algorithm employs a token-based system to control data flow.
- Tokens are generated at a fixed rate and added to the bucket.
- For each unit of data to be transmitted, a token must be available in the bucket.

3. Data Transmission:

- When data needs to be transmitted, the algorithm checks if there are enough tokens in the bucket.
- If there are sufficient tokens, the data is transmitted, and the corresponding number of tokens is removed.
- If there are not enough tokens, the data transmission is delayed until enough tokens accumulate.

Applications of Leaky Bucket Algorithm

Below are some of the Applications of Leaky Bucket Algorithm:

1. Traffic Shaping:

- The Leaky Bucket Algorithm is commonly used for traffic shaping in networks to regulate the data flow and prevent congestion.
- It ensures a steady and controlled transmission rate, reducing the risk of network bottlenecks.

2. Rate Limiting:

- Online services often employ the Leaky Bucket Algorithm for rate limiting to control the rate at which requests or data are processed.
- This helps prevent abuse, ensures fair usage, and maintains system stability.

3. Quality of Service (QoS):

- In scenarios where different types of traffic (e.g., voice, video, and data) compete for bandwidth, the Leaky Bucket Algorithm can be used to prioritize and allocate resources based on predefined rules.

Token Bucket Algorithm

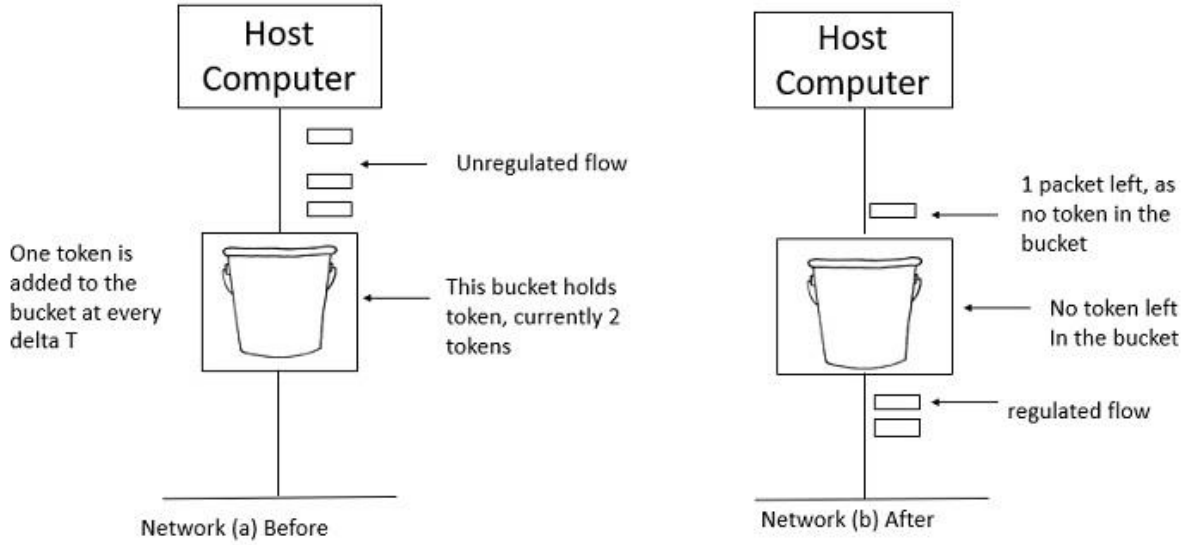
The leaky bucket algorithm enforces output patterns at the average rate, no matter how busy the traffic is. So, to deal with the more traffic, we need a flexible algorithm so that the data is not lost. One such approach is the token bucket algorithm.

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.