Lecture Notes on

4AID4-07

Data Communication and Computer Networks

Unit 5

Department of Artificial Intelligence & Data Science

Jaipur Engineering College & Research Centre, Jaipur

Neelkamal Chaudhary

Assistant Professor

AI&DS

Vision of the Institute

To become a renowned centre of outcome based learning and work toward academic, professional, cultural and social enrichment of the lives of individuals and communities.

Mission of the Institute

M1: Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.
M2: Identify, based on informed perception of Indian, regional and global needs, the areas of focus and provide platform to gain knowledge and solutions.
M3: Offer opportunities for interaction between academia and industry.
M4: Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

Vision Of The Department

To prepare students in the field of Artificial Intelligence and Data Science for competing with the global perspective through outcome based education, research and innovation.

Mission Of The Department

1. To impart outcome based education in the area of AI&DS.
2. To provide platform to the experts from institutions and industry of repute to transfer the knowledge to students for providing competitive and sustainable solutions.
3. To provide platform for innovation and research.

Program Outcomes (PO)

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and Artificial Intelligence & Data Science specialization to the solution of complex Artificial Intelligence & Data Science problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex Artificial Intelligence & Data Science problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex Artificial Intelligence & Data Science problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of Artificial Intelligence & Data Science experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex Artificial Intelligence & Data Science activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional Artificial Intelligence & Data Science practice.
7. **Environment and sustainability**: Understand the impact of the professional Artificial Intelligence & Data Science in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the Artificial Intelligence & Data Science practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings in Artificial Intelligence & Data Science
10. **Communication**: Communicate effectively on complex Artificial Intelligence & Data Science activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the Artificial Intelligence & Data Science and management principles and apply these to one" s own work, as a

member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change in Artificial Intelligence & Data Science.

Program Educational Objectives (PEO)

PEO1: To provide students with the fundamentals of Engineering Sciences with more emphasis in Artificial Intelligence & Data Science by way of analyzing and exploiting engineering challenges.

PEO2: To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems in Artificial Intelligence & Data Science

PEO3: To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues for Artificial Intelligence & Data Science.

PEO4: To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career in Artificial Intelligence & Data Science.

PEO5: To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge in Artificial Intelligence & Data Science.

COURSE OUTCOME: After studying this subject, student will be able

CO-1	Understand the principles of Network Protocols and OSI and TCP/IP model.
CO-2	Analyze and implement the concepts of various protocols of Error Detection and Correction
CO-3	Analyze and apply the concept of various Routing algorithms and principles of reliable data transfers along with transactional TCP and associated congestion control.
C0-4	Classify role of application layer, its various elements like WWW, DNS FTP and network security.

CO_PO Mapping

SUBJECT CODE	subject name		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
4AID4-07	Data Communication and Computer Networks	CO1:	3	3	3	2	2	1	1	1	1	1	1	3
		CO2:	3	3	3	3	1	1	1	1	1	2	1	3
		CO3:	3	3	3	2	1	1	1	1	1	2	1	3
		CO4:	3	3	3	2	1	1	1	1	1	1	1	3

Syllabus

4AID4-07: Data Communication and Computer Networks

Credit: 3 **Max. Marks: 100(IA:30,ETE:70)**
3L+0T+0P **End Term Exam: 3**

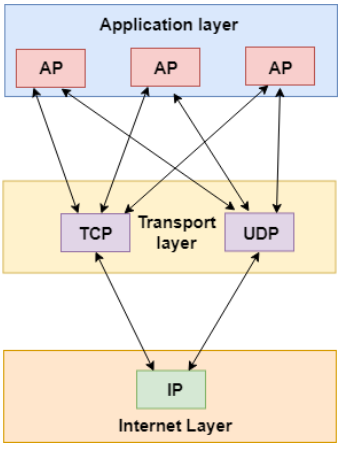
Hours

SN	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	1
2	Introductory Concepts: Network hardware, Network software, topologies, Protocols and standards, OSI model, TCP model, TCP/IP model, Physical Layer: Digital and Analog Signals, Periodic Analog Signals, Signal Transmission, Limitations of Data Rate, Digital Data Transmission, Performance Measures, Line Coding, Digital Modulation, Media and Digital Transmission System	7
3	Data Link Layer: Error Detection and Correction, Types of Errors, Two dimensional parity check, Detection verses correction, Block Coding, Linear Block Coding, Cyclic Codes, Checksum, Standardized Polynomial Code, Error Correction Methods, Forward Error Correction, Protocols: Stop and wait, Go-back-N ARQ, Selective Repeat ARQ, Sliding window, Piggy backing, Pure ALOHA, Slotted ALOHA, CSMA/CD, CSMA/CA	9
4	Network Layer: Design issues, Routing algorithms: IPV4, IPV6, Address mapping:ARQ,RARQ,Congestion control, Unicast,Multicast, Broadcast routing protocols, Quality of Service, Internetworking	8
5	Transport Layer: Transport service, Elements of transport protocols, User Datagram Protocol, Transmission Control Protocol, Quality of service, Leaky Bucket and Token Bucket algorithm	8
6	Application Layer**:** WWW, DNS, Multimedia, Electronic mail, FTP, HTTP, SMTP, Introduction to network security	7
	Total	40

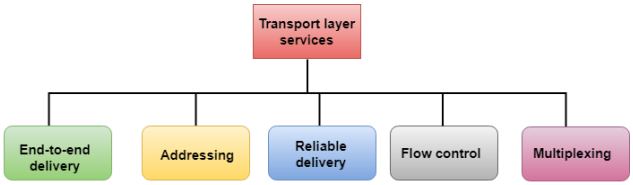
UNIT:5

Transport Layer

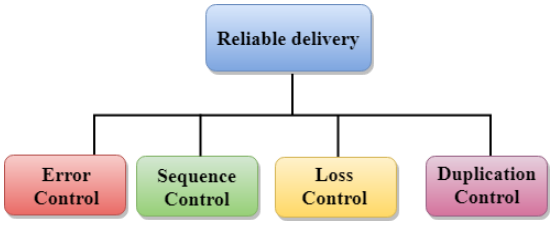
- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.



The services provided by the transport layer protocols can be divided into five categories:

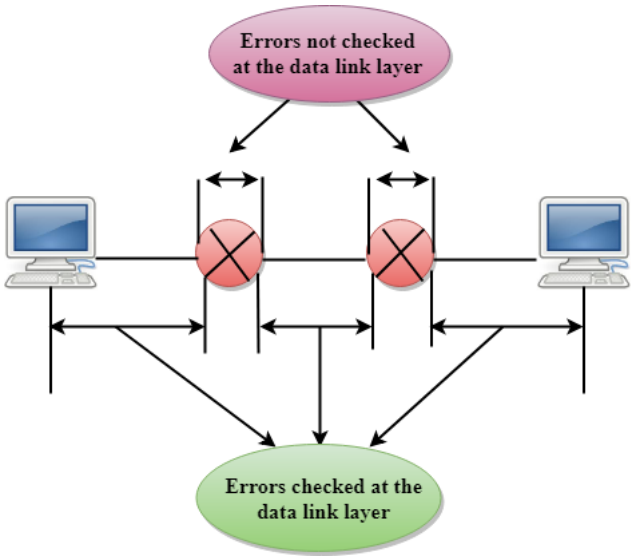


The reliable delivery has four aspects:



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.

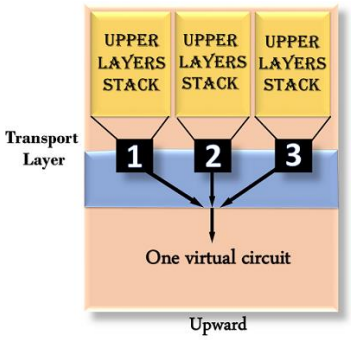


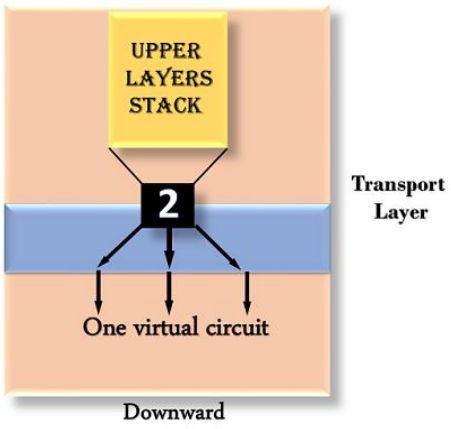
Loss Control

- 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.

Multiplexing: **The transport layer uses the multiplexing to improve transmission efficiency.**

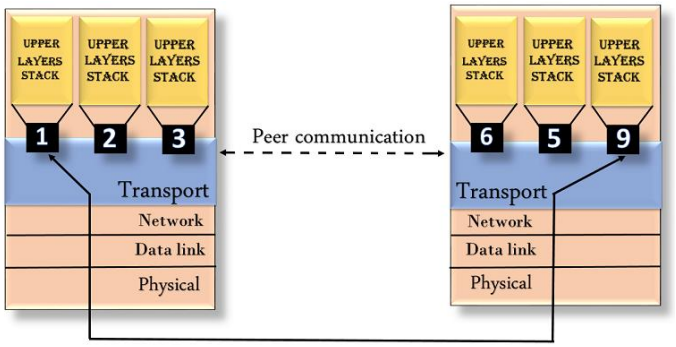
Multiplexing can occur in two ways: Upward multiplexing: Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through 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.



Transport Layer protocols

- **The transport layer is represented by two protocols: TCP and UDP.**

UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:

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

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.

- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

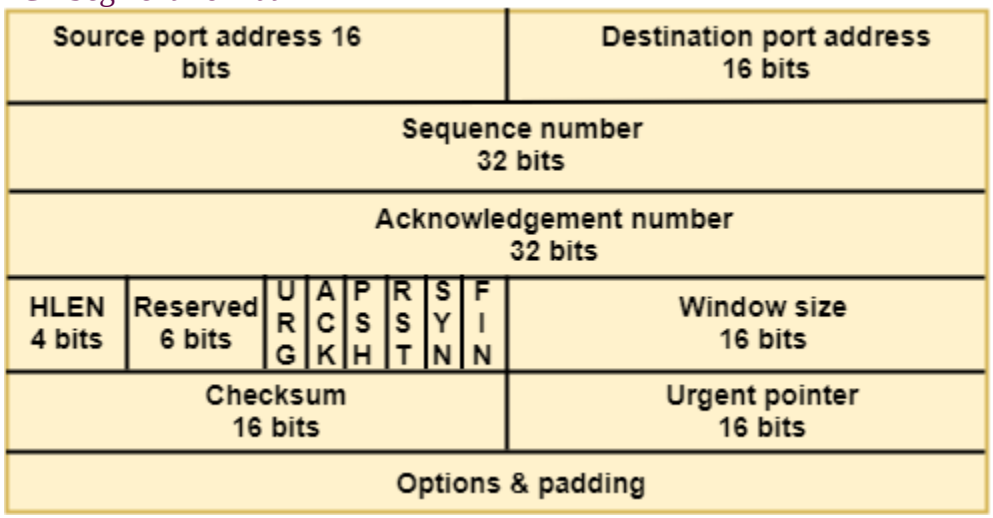
Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination. The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can

receive without any problem. This mechanism is also referred to as a window mechanism.

- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

TCP Segment Format



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.

- **Checksum:** The checksum is a 16-bit field used in error detection.
- **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
- **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

Quality of Service (QOS) determines a network's capability to support predictable service over various technologies, containing frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET IP-routed networks. The networks can use any or all of these frameworks.

The QOS also provides that while supporting priority for one or more flows does not create other flows fail. A flow can be a combination of source and destination addresses, source and

destination socket numbers, session identifier, or packet from a specific application or an incoming interface.

The QOS is primarily used to control resources like bandwidth, equipment, wide-area facilities etc. It can get more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc.

QOS Concepts

The QOS concepts are explained below−

Congestion Management

The bursty feature of data traffic sometimes bounds to increase traffic more than a connection speed. QoS allows a router to put packets into different queues. Servicespecific queues more often depend on priority than buffer traffic in an individual queue and let the first packet by the first packet out.

Queue Management

The queues in a buffer can fill and overflow. A packet would be dropped if a queue is complete, and the router cannot prevent it from being dropped if it is a high priority packet. This is referred to as tail drop.

Link Efficiency

The low-speed links are bottlenecks for lower packets. The serialization delay caused by the high packets forces the lower packets to wait longer. The serialization delay is the time created to put a packet on the connection.

Elimination of overhead bits

It can also increase efficiency by removing too many overhead bits.

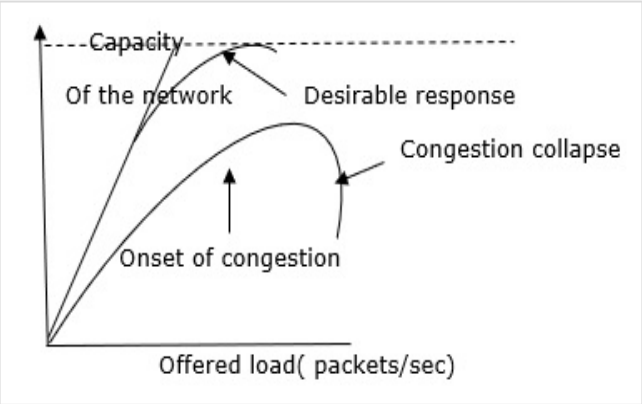
Traffic shaping and policing

Shaping can prevent the overflow problem in buffers by limiting the full bandwidth potential of the applications packets. Sometimes, many network topologies with a highbandwidth link connected with a low-bandwidth link in remote sites can overflow low bandwidth connections.

Therefore, shaping is used to provide the traffic flow from the high bandwidth link closer to the low bandwidth link to avoid the low bandwidth link's overflow. Policing can discard the traffic that exceeds the configured rate, but it is buffered in the case of shaping.

In the network layer, before the network can make Quality of service When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called congestion.

The network layer and transport layer share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network. To maintain this, the network and transport layers have to work together.



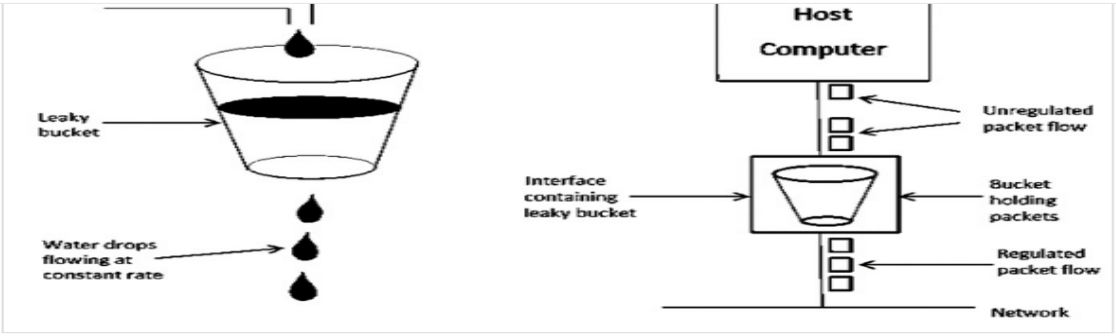
With too much traffic, performance drops sharply.

There are two types of Congestion control algorithms, which are as follows −

- Leaky Bucket Algorithm
- Token Bucket Algorithm

Leaky Bucket Algorithm

Let see the working condition of Leaky Bucket Algorithm –



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.

The presence of congestion means the load is greater than the resources available over a network to handle. Generally we will get an idea to reduce the congestion by trying to increase the resources or decrease the load, but it is not that much of a good idea.

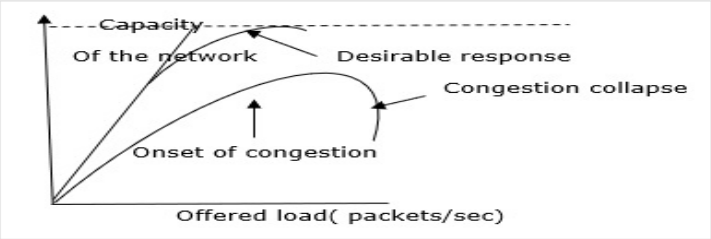
There are some approaches for congestion control over a network which are usually applied on different time scales to either prevent congestion or react to it once it has occurred.

Token bucket algorithm is one of the techniques for congestion control algorithms. When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called congestion.

The network layer and transport layer share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network. To maintain this network and transport layers have to work together.

The Token Bucket Algorithm is diagrammatically represented as follows –

The Token Bucket Algorithm is diagrammatically represented as follows –



With too much traffic, performance drops sharply.

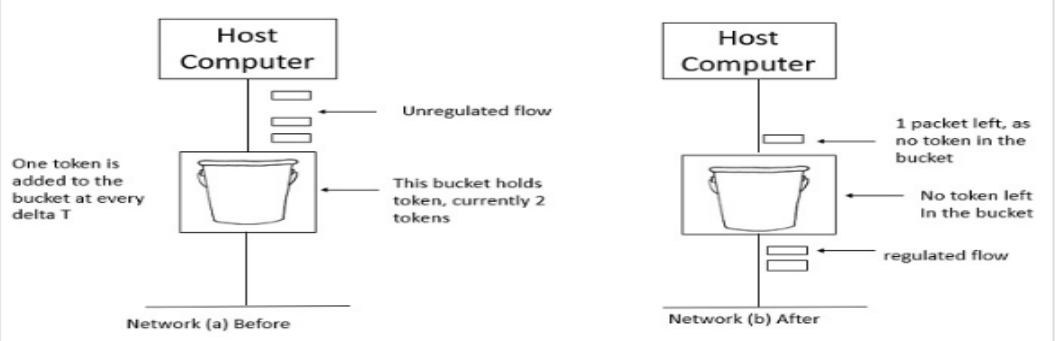
Token Bucket Algorithm

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.

Let us understand the Token Bucket Algorithm with an example –



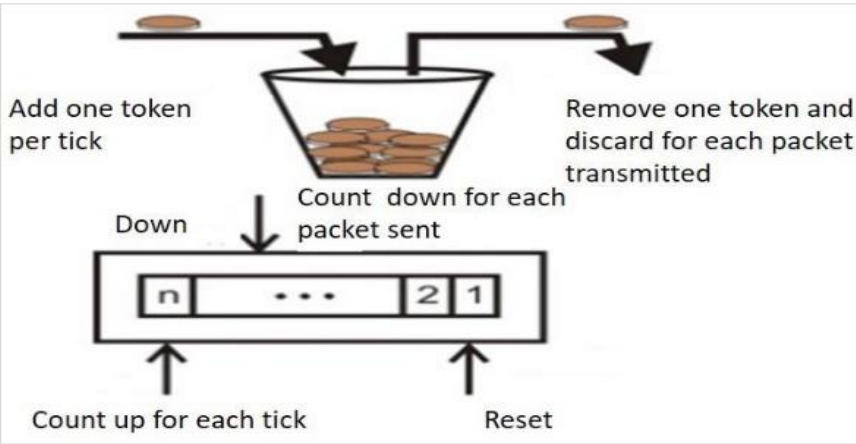
In figure (a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface.

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 leaky 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 a no token in bucket, packet can not be send.