Parul® University

Computer Networks (203105255)

Unit 4 : Transport Layer

Prof. Prasann Barot

Assistant Professor

Computer Science & Engineering

Parul® University

DIGITAL LEARNING CONTENT

Outline

- Process to Process Communication
- User Datagram Protocol(UDP)
- Transmission Control Protocol (TCP)
- SCTP Congestion Control
- Quality of Service
- QoS improving techniques: Leaky Bucket and Token Bucket algorithm

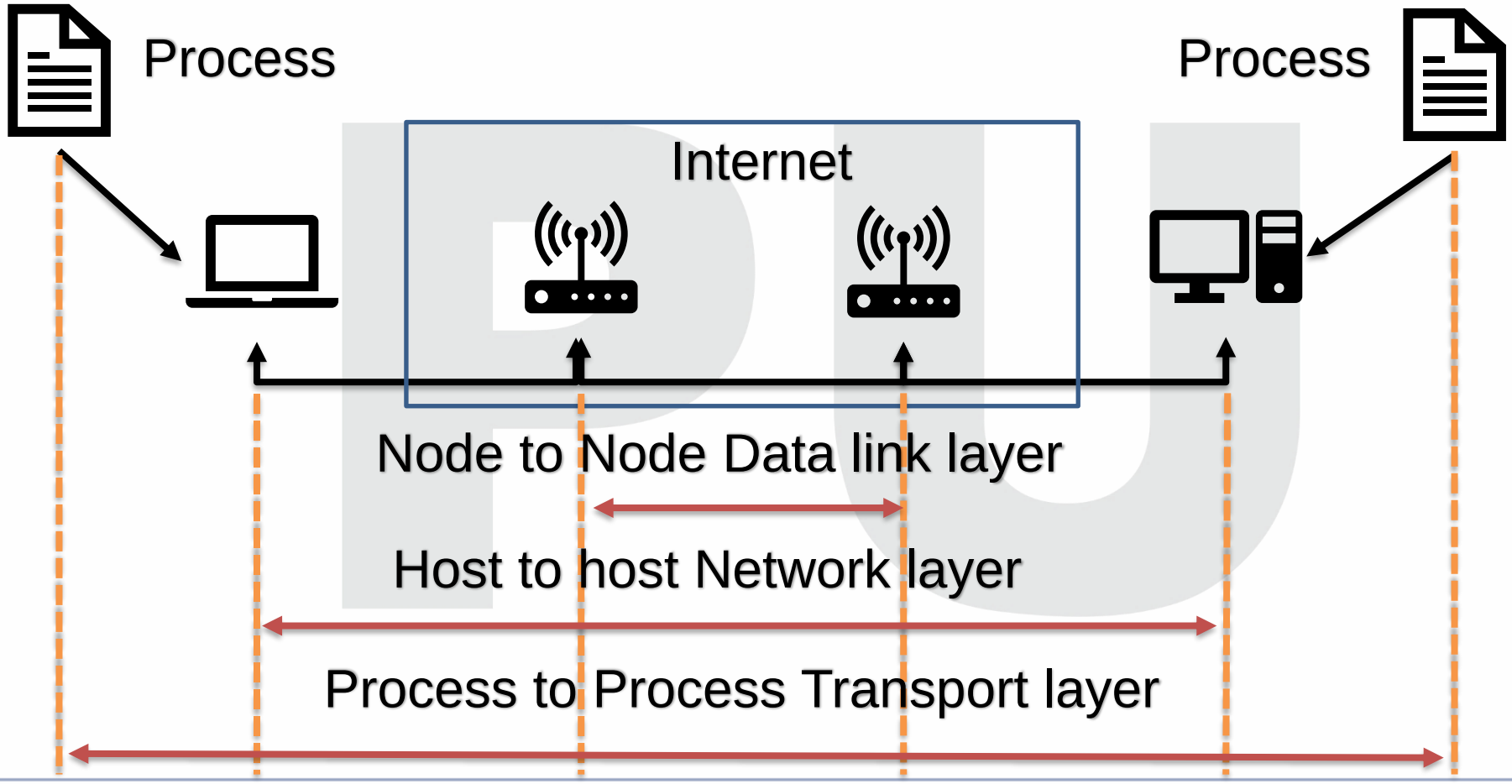
Transport Layer Services and Protocols

- Logical connectivity between application processes running on various hosts is provided.
- In terminal networks, a transport protocol runs.
- Sender side: It breaks application messages into segments, then passes to network layer.
- Receiver side: Reassembles segments into messages, then transfer s them to the layer of the programmed.
- E.g. TCP and UDP

Process to Process Communication

- The data link layer is responsible for the transmission of frames over a bridge between two adjacent nodes.
- This is called distribution from node to node.
- For the delivery of datagrams between two hosts, the network layer is responsible.
- This is called delivery from server to server.
- For two systems (application programmed), actual communication takes place for that, We need process-to-process delivery.
- For process-to - process delivery-the delivery of a packet, part of a message, from one process to another, the transport layer is responsible.

Process to Process Communication



Client/Server Paradigm

- While there are many ways to accomplish connectivity from process to process, the most common one is through the model of the client / server.
- A process on the local host, called a client, involves resources from a process called a server, normally on the remote host.
- They use the same name for all processes (client and server).
- For instance, we need a daytime client process running on the local host and a daytime server process running on a remote machine to get the day and time from a remote machine.

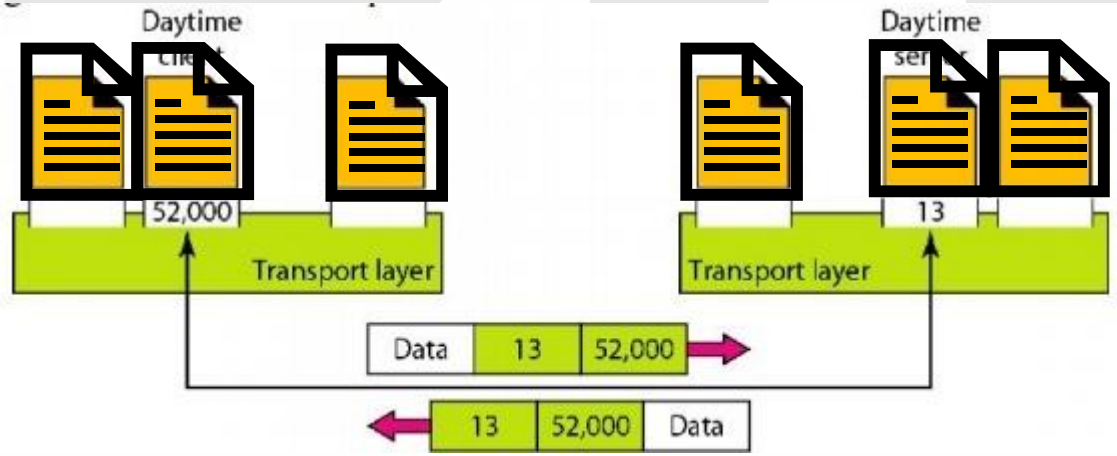
Contd.

- For communication, we must define the following:

1. Local host
2. Local process
3. Remote host
4. Remote process

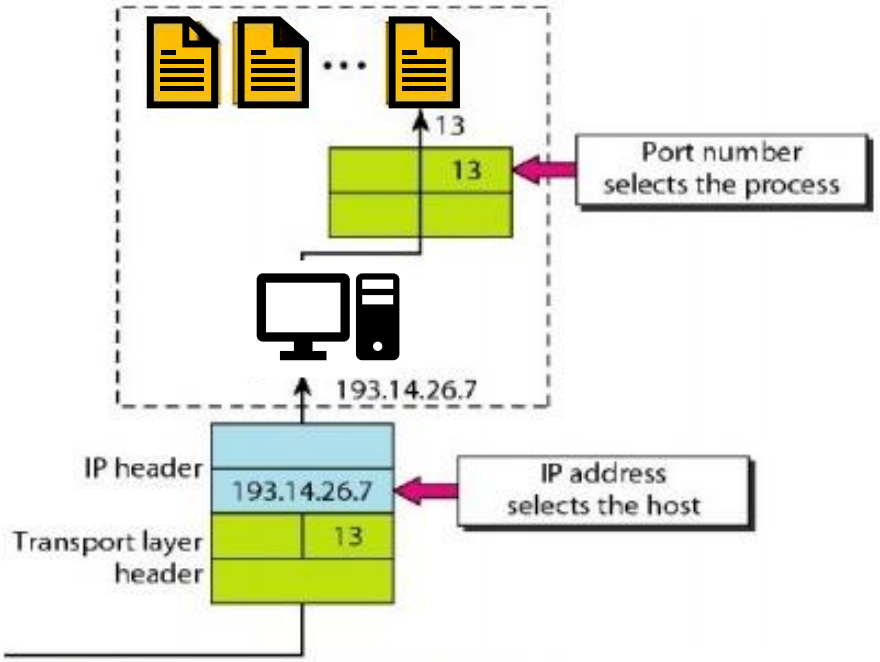
Addressing

- We need an address if we need to send something to one of several unique destinations.
- We need a MAC address at the data link layer to select one node from multiple nodes if the connexon is not point-to-point. For delivery, a frame in the data link layer requires a destination MAC address and a source address for the response of the next node.



Contd.

- In the selection of the final destination of the data, IP addresses and port numbers play different roles.
- The IP address for the destination determines the host among the multiple hosts in the world.
- The port number determines one of the processes for this specific host after the host has been chosen.



Socket Addresses

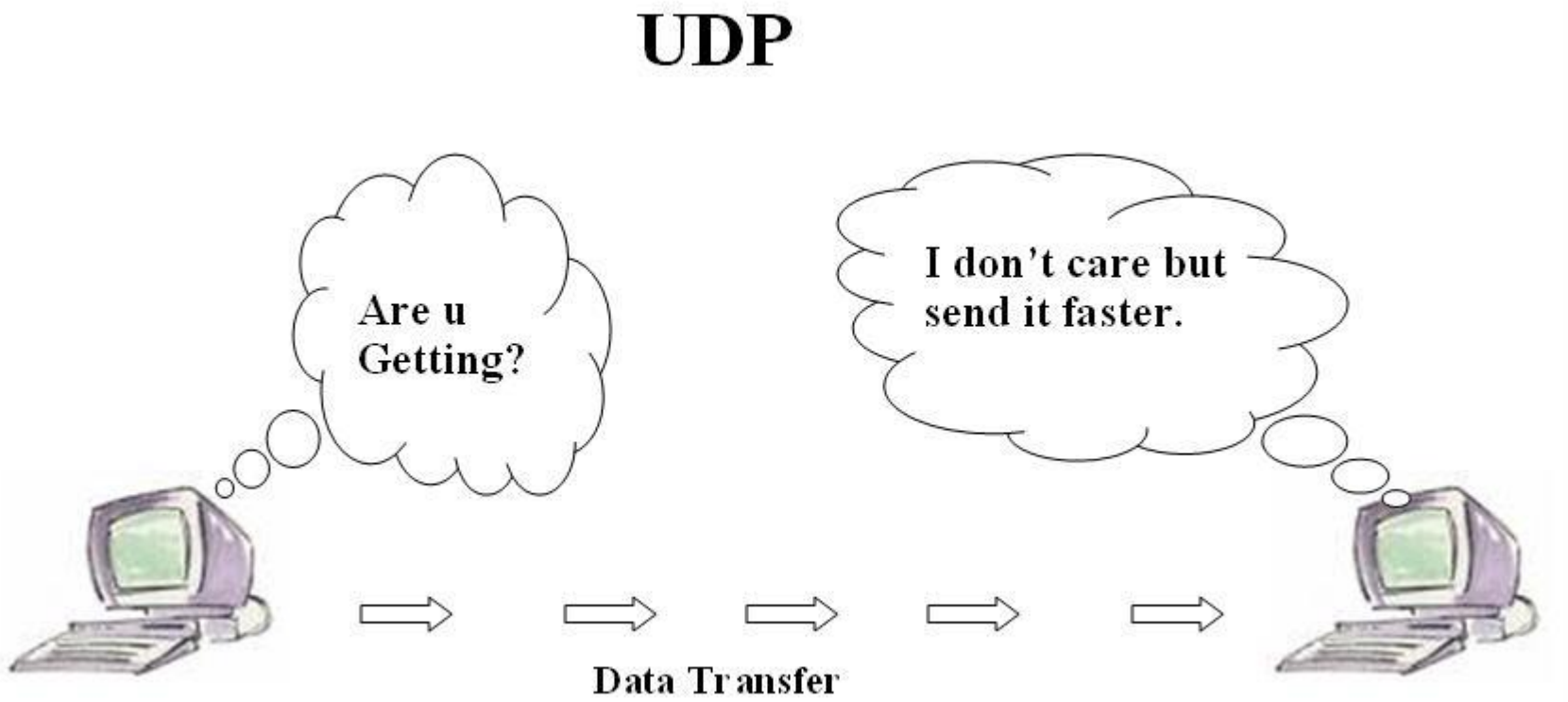
- Process-to - process distribution involves two identifiers, an IP address and a port number, to create a connexon at either end. A socket address is considered the combination of an IP address and a port number.
- The network socket address uniquely defines the client process, just as the application socket address uniquely defines the server process.

User Datagram Protocol

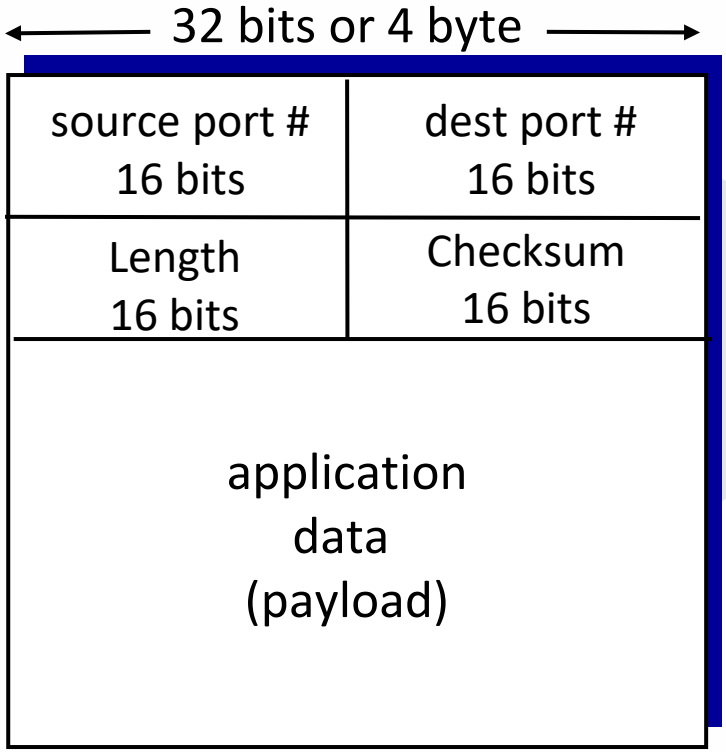
- User Datagram Protocol – Transport layer protocol.
- This requires a sufficient number of methods for correspondence.
- It needs an application process message, adds the source & destination port number for multiplexing or demultiplexing, and then passes to the network layer.
- In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent **(connection less)**.
- There is no handshaking between sender and receiver at transport layer.

Contd.

So, that UDP is connectionless protocol. E.g. DNS, SNMP, RIP



UDP Segment - Header



UDP segment format

UDP

- no connection establishment (which can add delay)
- simple: no connection state at sender, receiver
- small header size
- no congestion control: UDP can blast away as fast as desired

Contd.

1.Source Port : Source Port is 16 bits long field used to identify port number of source.

2.Destination Port : It is 16 bits long field, used to identify the port of destined packet.

3.Length : Length is the length of UDP including header and the data. It is 16-bits field.

4.Checksum : Checksum is 16 bits long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets. Checksum calculation is not mandatory in UDP.

UDP - Checksum

Checksum is used to detect errors in transmitted segment.

Sender:

Treat segment contents, including header fields, as sequence of 16-bit integers.

Checksum: addition (one's complement sum) of segment contents.

Sender puts checksum value into UDP checksum field.

Receiver:

Compute checksum of received segment.

Check if computed checksum equals checksum field value:

- NO - error detected
- YES - no error detected

Contd.

Sender

	1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
	1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
wraparound	1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
	+
sum	1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 0
checksum	0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1

Receiver

	1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
1	1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1	1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
	+
1	1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 0
1	0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

sum

If one of the bits is a 0, then we can say that error introduced into packet

Note: A carryout from the most important bit has to be added to the result when adding numbers

Applications of UDP

Here are few applications where UDP is used to transmit data:

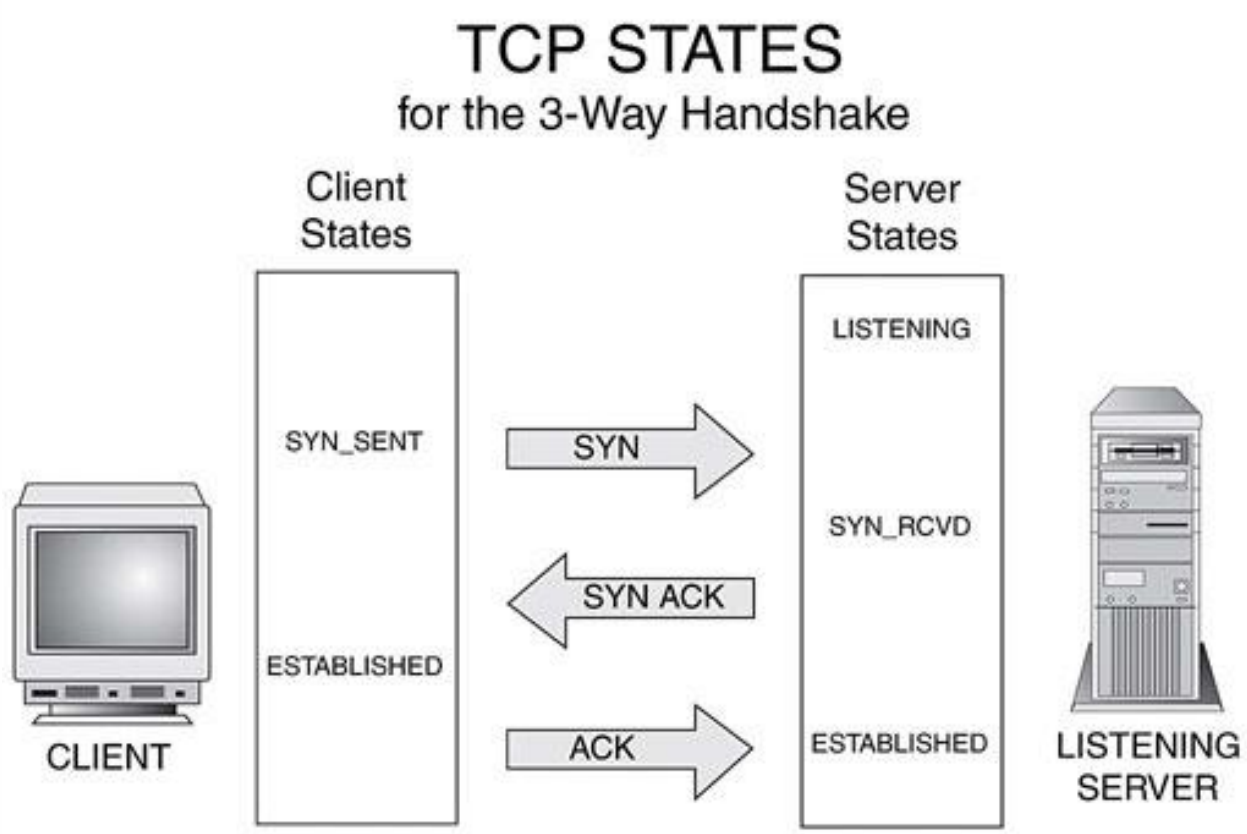
- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

Transmission Control Protocol/ Internet Protocol

- Transmission Control Protocol/ Internet Protocol = TCP/IP

- It is a collection of protocols or guidelines and procedures used on the Internet to interconnect network computers.
- As the basic protocols in the suite are Transmission Control Protocol and Internet Protocol, the internet protocol suite is generally known as TCP / IP.
- It chooses how the data is traded on the web by end - to - end interactions that integrate how the data can be structured into packets, addressed, sent, and collected at the target.

Contd.



Characteristics of TCP/IP

- **Share Data Transfer**: The TCP helps programmers to build network-wide networking networks. It also allows a message to be divided into smaller packets before being sent over the internet and then received at the destination address in the correct order. So, it guarantees a strong channel-wide transmission of data.
- **Internet Protocol**: The IP address informs the address and path of the packets so that they meet their right destination. It requires a technique that empowers internet-connected portal computers to plan for the message to be forwarded after the IP address is checked.

Contd.

- Reliability: Strong data distribution is the most vital function of TCP. TCP must retrieve data that is lost, misplaced, copied, or conveyed by the Arrange Layer in order to have unwavering consistency.
- Multiplexing: By the number of ports, multiplexing can be accomplished.
- Connections: The systems have to set up a connection before application types can transmit information using TCP. The contacts are made between the sender's harbour numbers and the equipment of the collector.

Application/Uses of TCP/IP

- Simple Mail Transfer Protocol(SMTP): It helps to send email to another email address.
- File Transfer Protocol(FTP): It is used for sending large files.
- Dynamic Host Configure Protocol(DHCP): It assigns the IP address.
- Telnet: Bi-directional text communication via a terminal application.
- Hyper Text Transfer Protocol(HTTP): Used to transfer the web pages.
- Domain Name System(DNS): It translates the website name to IP addresses.
- Simple Network Time Protocol(SNTP): It provides the time of a day to the network devices.

Stream Control Transfer Protocol

- It is a secure transport protocol that runs on top of a connectionless service that is insecure, such as IP.
- Via the use of checksums, sequence numbers, and limited retransmission mechanisms, it provides known, error-free, non-duplicated message transfers.
- SCTP is designed to allow programs to communicate in a secure way, represented as endpoints, and so is comparable to TCP. It has literally inherited much of its behavior from TCP, such as the setup of associations, management of congestion and algorithms for detecting packet loss.

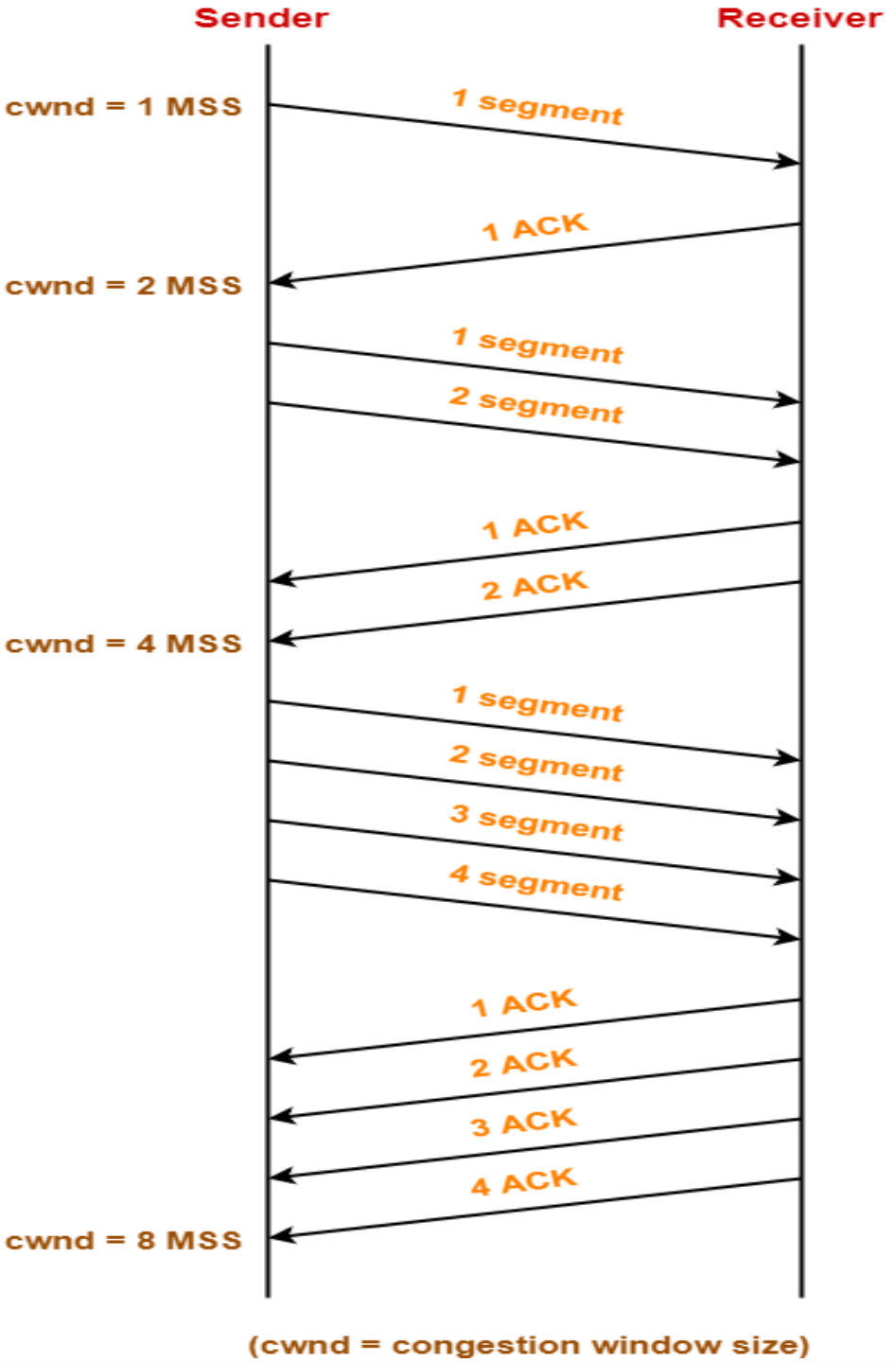
Congestion Control

- Congestion happens when vast volumes of data are fed to a device that is not capable of processing it. Using the Windows mechanism, TCP manages congestion. TCP sets a window size to inform the other end how long to send the data segment.
- For congestion control, TCP may use three algorithms.
  1. Slow Start
  2. Congestion Avoidance
  3. Congestion Detection

Parul®
University

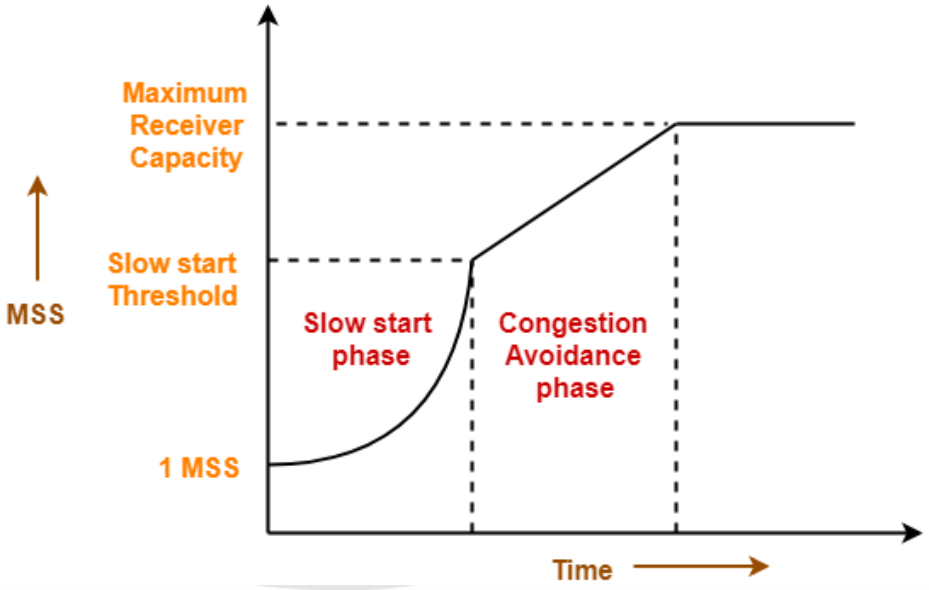
Slow Start

- The sender initially sets the size of the congestion window = Full Segment Size (1 MSS).
- The sender raises the congestion window size by 1 MSS after receiving each acknowledgment.
- The size of the congestion window increases exponentially in this process.



Congestion Avoidance

- After having met the threshold,
- In order to prevent congestion, the sender linearly increases the congestion window duration.
- When each acknowledgment is received, the sender raises the duration of the congestion window by 1.



Congestion Detection

- When the sender senses segment loss, based on how the loss is observed, it responds in various ways.
- Case 1 = Detection On Time Out
  - Before receiving the acknowledgement for a segment the Time Out Timer expires.
  - The greater risk of congestion in the network is implied in this situation.
  - There is a possibility that the network has lost a section.
- Set the slow start threshold at half the current duration of the window for congestion.
- Decreasing the duration of the congestion window to 1 MSS.
- The slow start process returns.

Contd.

- Case 2 = Detection On Receiving 3 Duplicate Acknowledgements
  - For a line, the sender receives 3 duplicate receipts.
  - The lesser probability of network interference is proposed in this situation.
  - There are risks of losing a section, but few segments submitted later could have reached
- Set the slow start threshold at half the current duration of the window for congestion.
- Reduce the duration of the congestion window to slow down the start threshold.
- Resuming the stage of prevention of congestion.

Quality of Service

- 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

- Visual and audio conferencing requires a limited rate of delay and loss.
- Streaming video and audio requires a small packet error rate, and may not be too vulnerable to delay.
- Real-time management (time-critical applications) in which a small delay is considered an important element.
- Better facilities can be offered for useful applications than for less valuable applications.

QoS Specification

QoS requirements can be specified as:

1. Delay
2. Delay Variation(Jitter)
3. Throughput
4. Error Rate

Types of QoS Solutions

1. **Stateless Solutions**
   Routers do not sustain a fine grained traffic condition, but one good aspect is that it is scalable and resilient. But it has bad services and in a specific application that we have to face, there is no guarantee of the type of delay or results.
2. **Stateful Solutions**

In providing quality-of-service , i.e. providing powerful services such as assured services and high use of energy, providing security and is much less flexible and resilient, routers retain per flow state as flow is quite important.

QoS improving techniques

- Any methods that can be used to maximize service efficiency, like Traffic Shaping:
- A method for regulating the volume and pace of traffic sent to the network is traffic shaping. Traffic can be formed by two techniques:

1. leaky bucket
2. token bucket

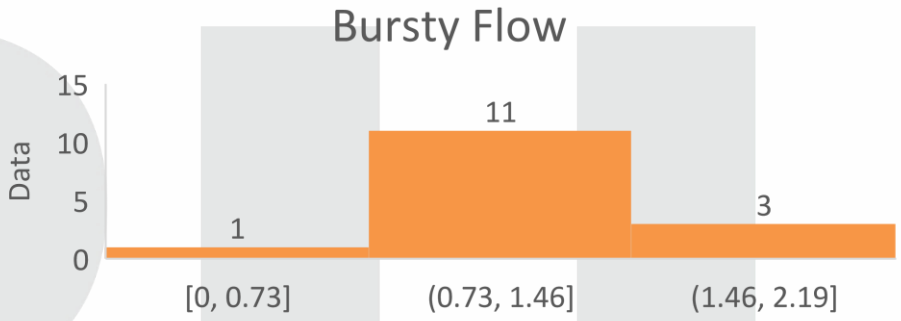
1. Leaky Bucket

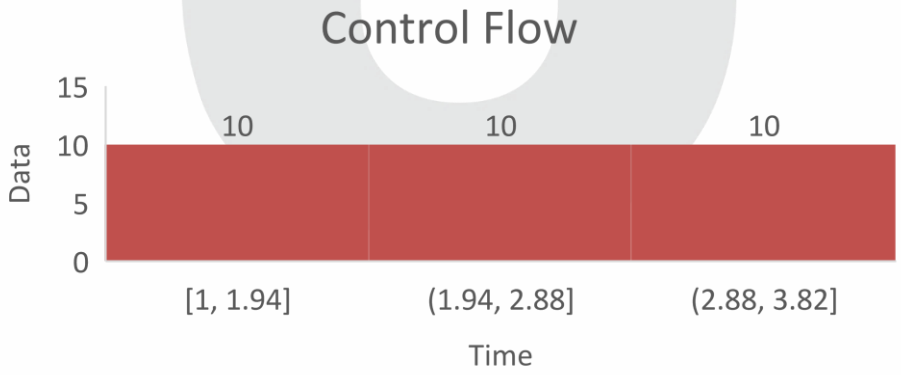
- As long as there is water in the container, if a bucket has a small hole at the bottom, the water spills from the bucket at a steady rate.
- If the bucket is zero, the rate at which the water spills does not depend on the rate at which the water is fed to the bucket.
- The rate of input will vary, but the rate of output remains constant. Similarly, a technique called leaky bucket will smooth out bursty traffic during networking.
- In the bucket, bursty chunks are processed and sent out at an average clip.

Contd.

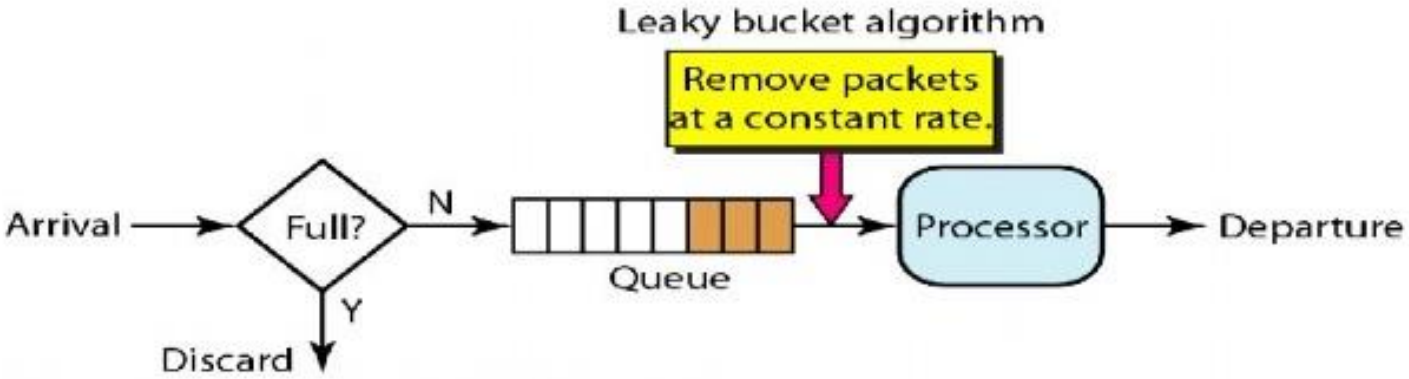
Bursty flow

Control flow





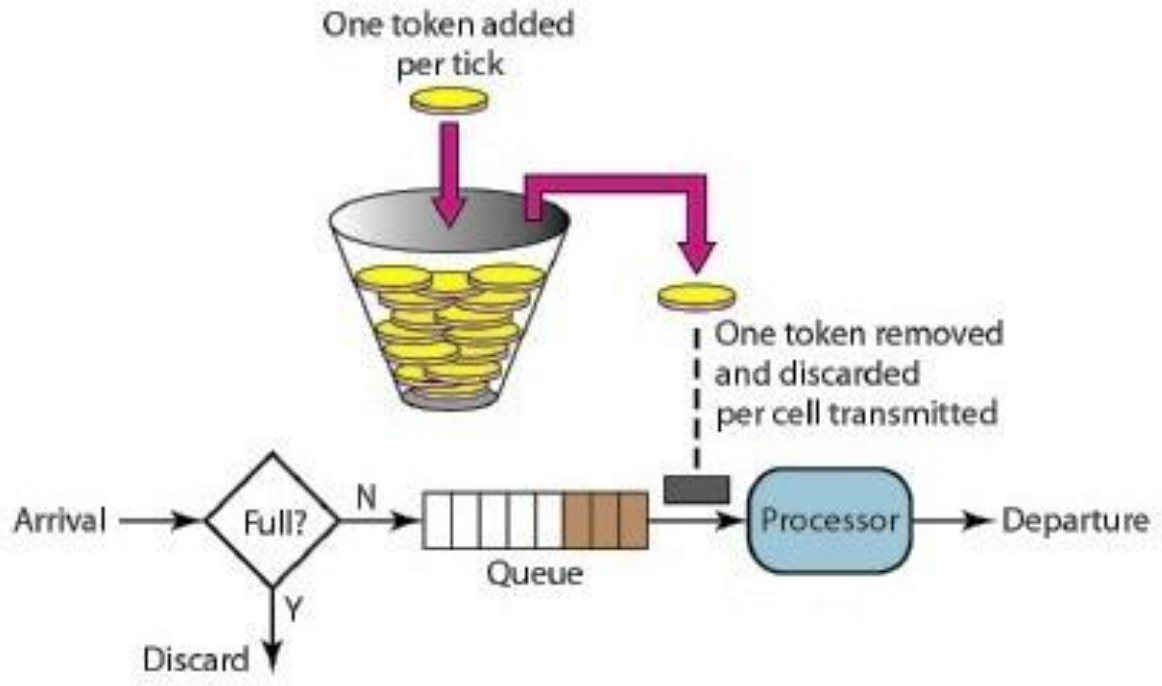
Contd.


Leaky bucket algorithm
Remove packets at a constant rate.
Arrival
Full?
N
Y
Discard
Queue
Processor
Departure

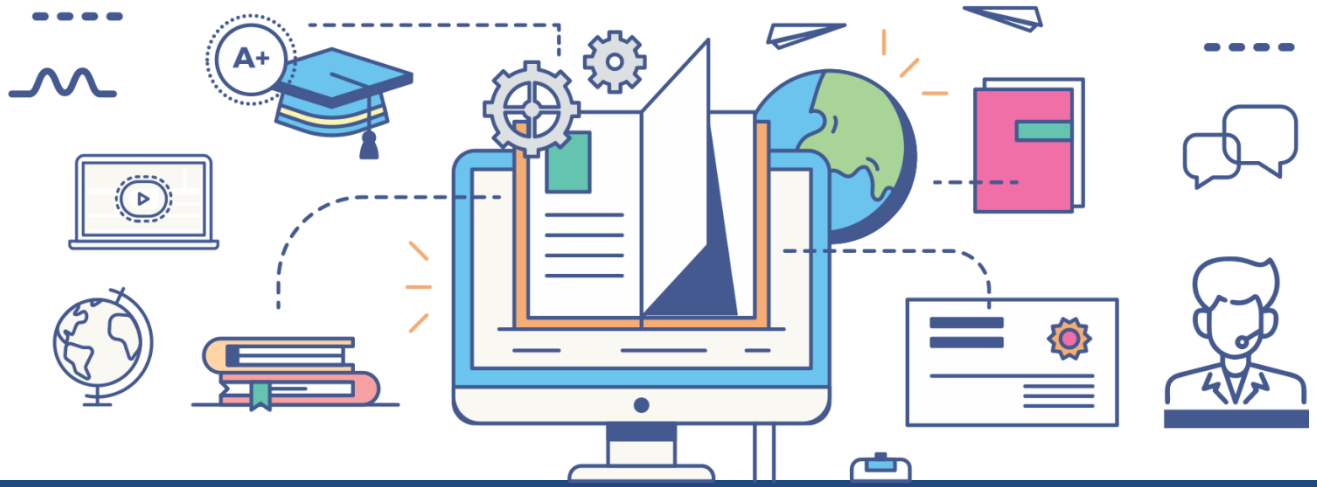
2. Token Bucket

- There's a very restrictive leaky bucket. An idle host is not credited. If a host does not submit for a while, for instance, the bucket becomes null.
- Today, if there is bursty data in the host, the leaky bucket only makes an average rate. No account is taken of the time that the host was idle. The token bucket algorithm, on the other hand , helps idle hosts to collect credit in the form of tokens for the future. The machine sends N tokens to the bucket for each tick of the clock.
- For every cell (or byte) of data sent, the machine eliminates one token. For instance, if n is 100 and the host is idle for 100 ticks, 10,000 tokens are collected from the bucket.

Contd.


One token added
per tick
One token removed
and discarded
per cell transmitted
Arrival
Full?
N
Y
Discard
Queue
Processor
Departure

DIGITAL LEARNING CONTENT



Parul® University

www.paruluniversity.ac.in