Congestion Control and Quality of Service

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Aim of the session

To familiarize students with the basic concept of Congestion control and Quality of Service

Learning Outcomes

At the end of this session, you should be able to:

- Describe the Congestion control mechanisms and list out various categories of Congestion prevention and removal mechanism
- Describe the concepts of Quality Of Service
- List out different Techniques of QOS

Overview

1. Congestion Control
   - Open loop Congestion Control
   - Closed-Loop Congestion Control
2. Quality of Service
   - Techniques to improve QoS

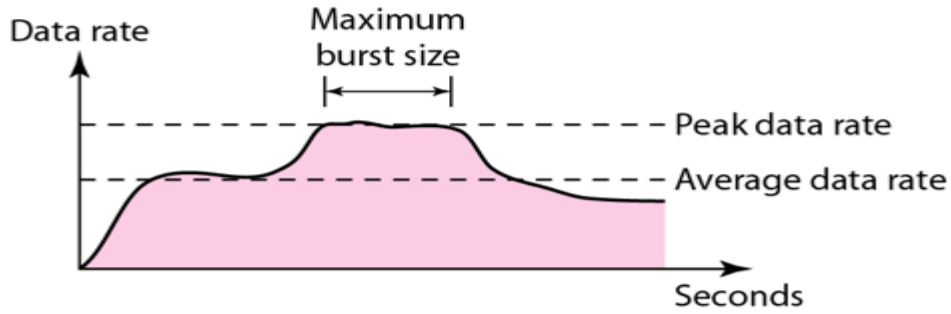
Congestion Control

Congestion Control

- Congestion control and quality of service are two issues so closely bound together
- These issues are related to three layers: the data link layer, the network layer, and the transport layer.
- **Data Traffic**
  - In congestion control: We are trying to avoid traffic congestion
  - In quality of service: we try to create an appropriate environment for the traffic.

Traffic Descriptors

- **Average data rate** = amount of data / time
- **Peak Data Rate**: Defines the maximum data rate of the traffic
- **Maximum Burst Size**: Refers to the maximum length of time the traffic is generated at the peak rate.
- **Effective Bandwidth**: The bandwidth that the network needs to allocate for the flow of traffic
  - Function of the above three parameters



Traffic Profiles

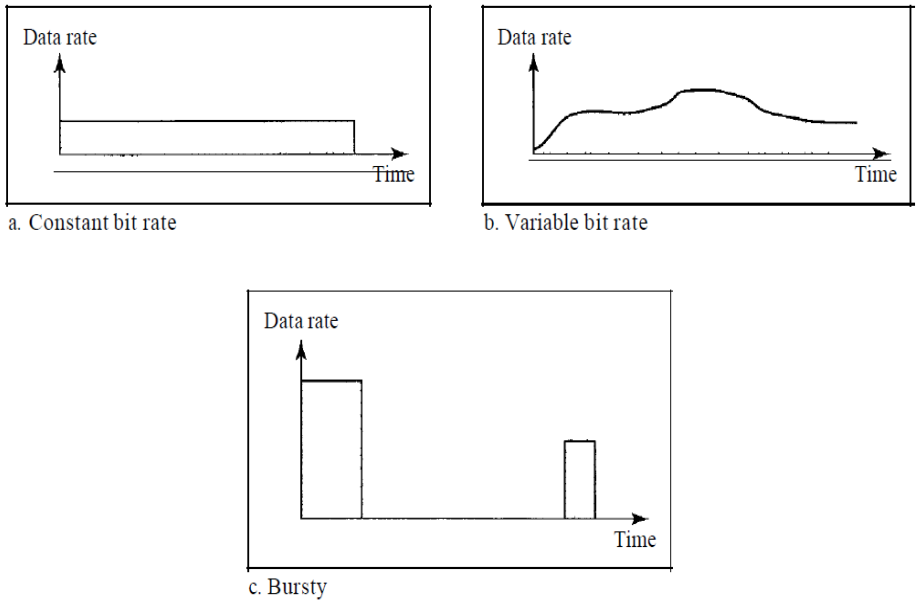


Figure: Traffic Profiles

- Constant Bit Rate: Data rate does not change with time
- Variable Bit Rate: The rate of the data flow changes in time
  - changes are smooth instead of sudden and sharp
- Bursty: Data rate changes suddenly in a very short time

Congestion

- **Congestion** in a network may occur if the ***load*** on the network is greater than the ***capacity*** of the network
  - Load: The number of packets sent to the network
  - Capacity : The number of packets a network can handle
- **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity
- Routers and switches have queues (buffers) that hold the packets before and after processing
- When does congestion occur?
  - If the rate of packet arrival is higher than the packet processing rate
    - Input queues become longer and longer
  - If the packet departure rate is less than the packet processing rate
    - Output queues become longer and longer

Congestion Control

- Congestion control refers to techniques and mechanisms that can
  - Prevent congestion before it happens or
  - Remove congestion after it has happened

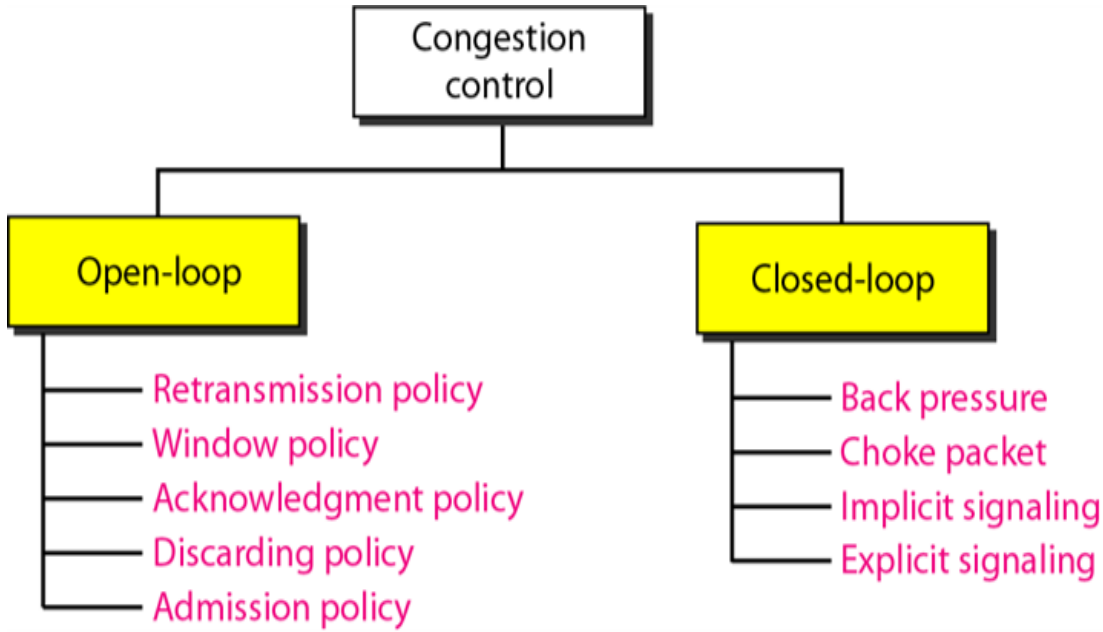


Figure: Congestion control categories

Open loop Congestion Control

Open-loop congestion control policies are applied **to prevent congestion before it happens**.

- Handled by either the source or the destination.
- **Retransmission Policy**: If the sent packet is lost or corrupted, the packet needs to be retransmitted.
  - Retransmission in general may increase congestion in the network
  - **Retransmission timers** must be designed to optimize efficiency and at the same time prevent congestion
- **Window Policy**: The Selective Repeat window is better than the Go-Back-N window for congestion control
  - In the Go-Back-N window, several packets may be resent although some may have arrived safe and sound at the receiver
    - Duplication may make the congestion worse
  - Selective Repeat window tries to send the specific packets that have been lost or corrupted.

Open loop congestion Control

- **Acknowledgment Policy** imposed by the receiver may also affect congestion
  - Sender may slow down if acknowledgment is not received
  - A receiver may decide to acknowledge only N packets at a time
  - Sending fewer acknowledgments means imposing less load on the network.
- **Discarding Policy**: A good discarding policy by the routers may prevent congestion without harming the integrity of the transmission
  - Eg: In audio transmission, discard less sensitive packets when congestion is likely to happen
    - Quality of sound is still preserved and congestion is prevented
- **Admission Policy**: is a quality-of-service mechanism used to prevent congestion in virtual-circuit 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.

Closed-Loop Congestion Control

Closed-loop congestion control policies are applied **to prevent congestion after it happens**.

- **Backpressure**: refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

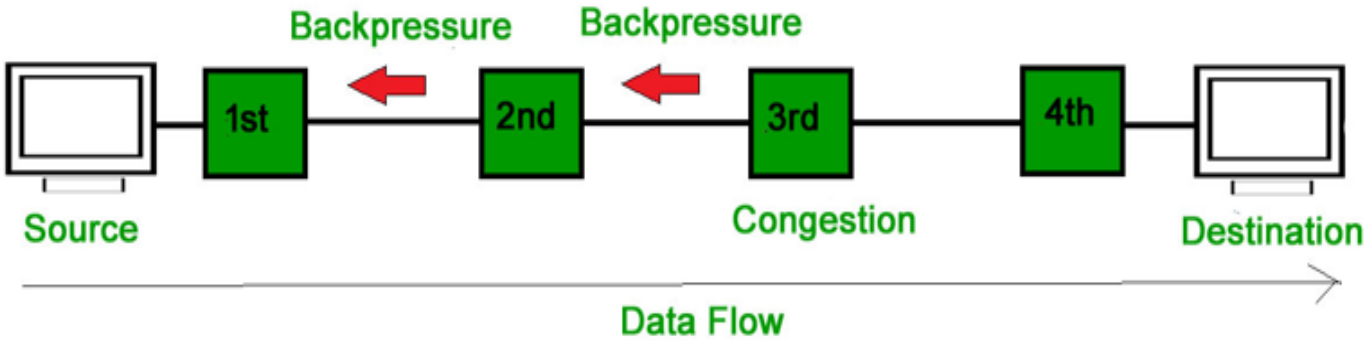


Figure: Backpressure method for reducing congestion

Closed-Loop Congestion Control

- **Choke Packet**:is a packet sent by a node to the source to inform it of congestion.
  - In backpressure, the warning is from one node to its upstream node
  - In the choke packet method, the warning is from the router(encountered congestion) to the source station directly
  - The intermediate nodes through which the packet has traveled are not warned about congestion

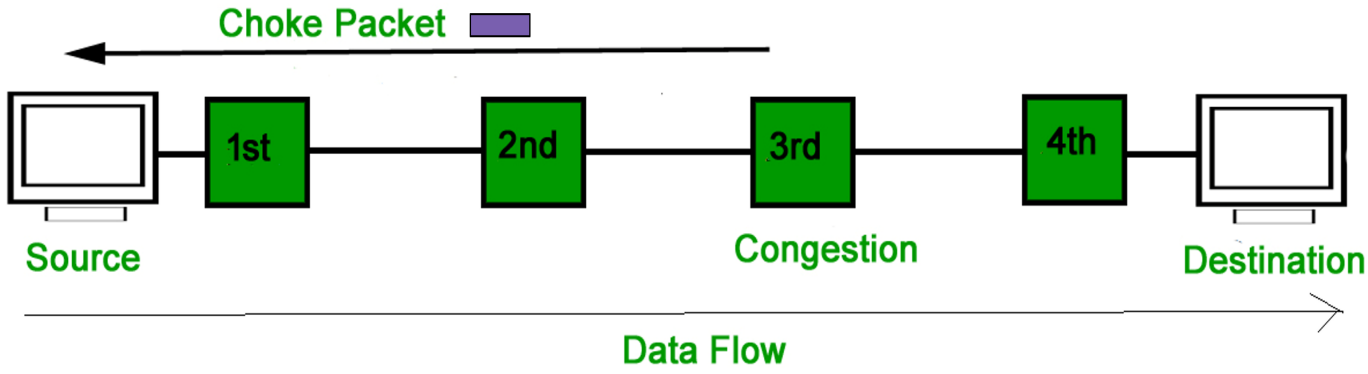


Figure: Choke packet method for reducing congestion

Closed-Loop Congestion Control

- **Implicit Signaling** In this mechanism, there is no communication between the congested node(s) and the source.
  - Example: when a source sends several packets and there is no acknowledgment for a while $\Longrightarrow$ network is congested.
- **Explicit Signaling**: The node experiencing congestion can explicitly send a signal to the source or destination.
  - **Backward Signaling**: A bit is set (as 1) in a packet moving in the direction opposite to the congestion.
    - Bit warns the source about the congestion.
  - **Forward Signaling**: A bit is set (as 1) in a packet moving in the direction of the congestion.
    - Bit warns the destination about congestion

Quality of Service

Quality of Service

- A stream of packets from a source to destination is called a flow.
- In a connection-oriented network, all the packets belonging to a flow follow the same route.
- In a connectionless network, they may follow different routes.
- The needs of each flow can be characterized by four primary parameters: Reliability, Delay, Jitter and Bandwidth.
- Together these determine the QOS (Quality Of Service) the flow requires.

Flow Characteristics

- **Reliability**: How critical is it that all packets reach the destination without error.
  - Lack of reliability means losing a packet or acknowledgment
  - Sensitivity of application programs to reliability is not the same
    - Eg: Electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.
- **Delay**: The maximum acceptable time a packet takes to reach the destination.
  - Telephony, audio conferencing, video conferencing, and remote log-in need minimum delay
  - Delay in file transfer or e-mail is less important.

- **Jitter** is the variation in delay for packets belonging to the same flow
- Packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23 $\Longrightarrow$ 20 seconds delay (same for all)
- If the above four packets arrive at 21, 23, 21, and 28 $\Longrightarrow$ different delays: 21,22, 19, and 24
- In audio and video applications, jitter is not acceptable
- **Bandwidth**: The range of frequencies contained in a composite signal is its bandwidth
  - Different applications need different bandwidths.
  - video conferencing: Send millions of bits/sec
  - Email: No of bits may not reach even a million

Techniques to improve QoS

- Overprovisioning
- Packet Scheduling
  - FIFO Queuing
  - Priority Queuing
  - Weighted Fair Queuing
- Traffic Shaping
  - Leaky Bucket
  - Token Bucket
- Integrated Services
- Differentiated Services

Techniques to improve QoS

- **Overprovisioning**: Build a network with enough capacity for whatever traffic will be thrown at it.
  - The Capacity available can always meet the demand.
  - It is expensive
- **Packet Scheduling**: Regulate the shape of the offered traffic
  - A good scheduling technique treats the different flows in a fair and appropriate manner
  - Concentrate on flow control to improve QoS

Packet Scheduling: FIFO Queuing

- **First-in First-out Queuing**: Packets wait in a buffer (queue) until the node (router or switch) is ready to process them.
  - If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded
  - **Tail drop**: FIFO routers usually drop newly arriving packets when the queue is full. This behavior is called tail drop.

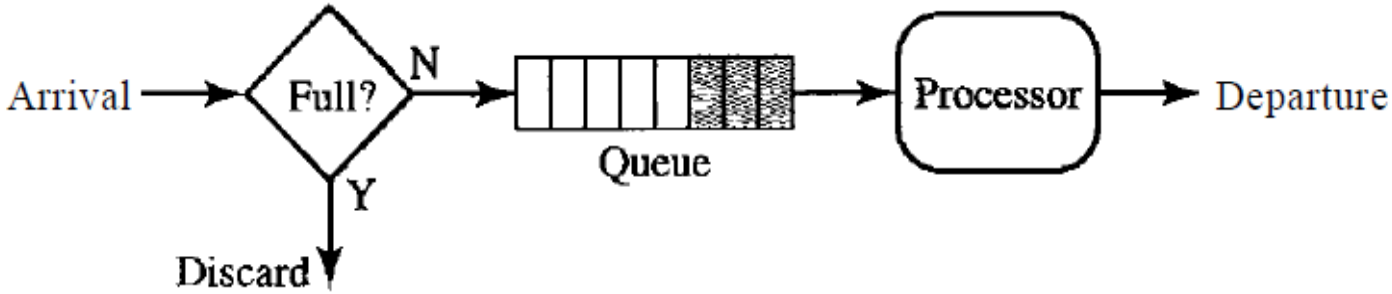


Figure: FIFO queue

Packet Scheduling: Priority Queuing

- **Priority Queueing**:
  - Packets are first assigned to a priority class
  - The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last.
  - A priority queue can provide better QoS than the FIFO queue
    - Multimedia can reach the destination with less delay
  - If there is a continuous flow in a high-priority queue, the packets in the lower-priority queues will never have a chance to be processed. This is a condition called **starvation**

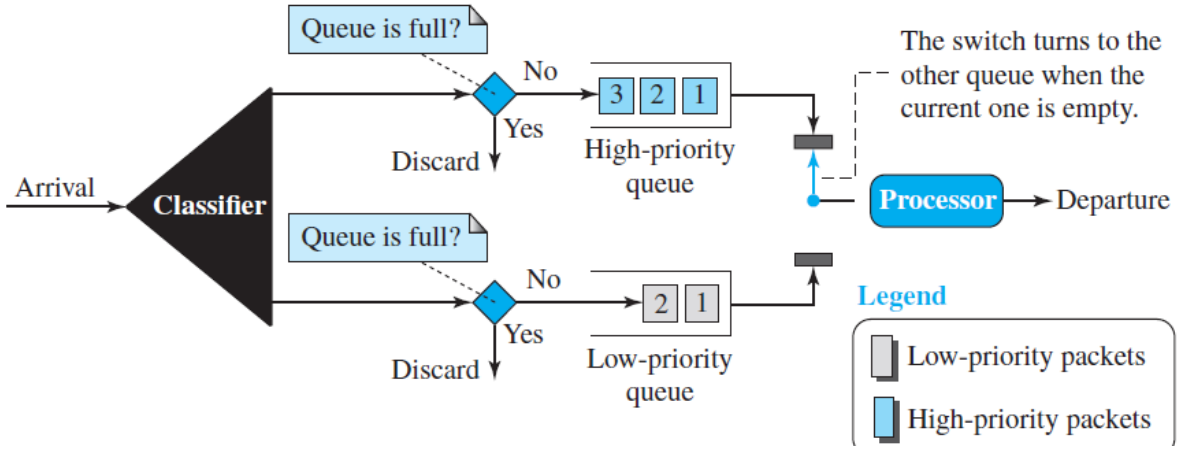


Figure: Priority Queuing

Packet Scheduling: Weighted fair Queuing

In **Weighted Fair Queuing** the packets are still assigned to different classes and admitted to different queues.

- The queues are weighted based on the priority of the queues
  - Higher priority means a higher weight
  - System processes packets in each queue in a round-robin fashion

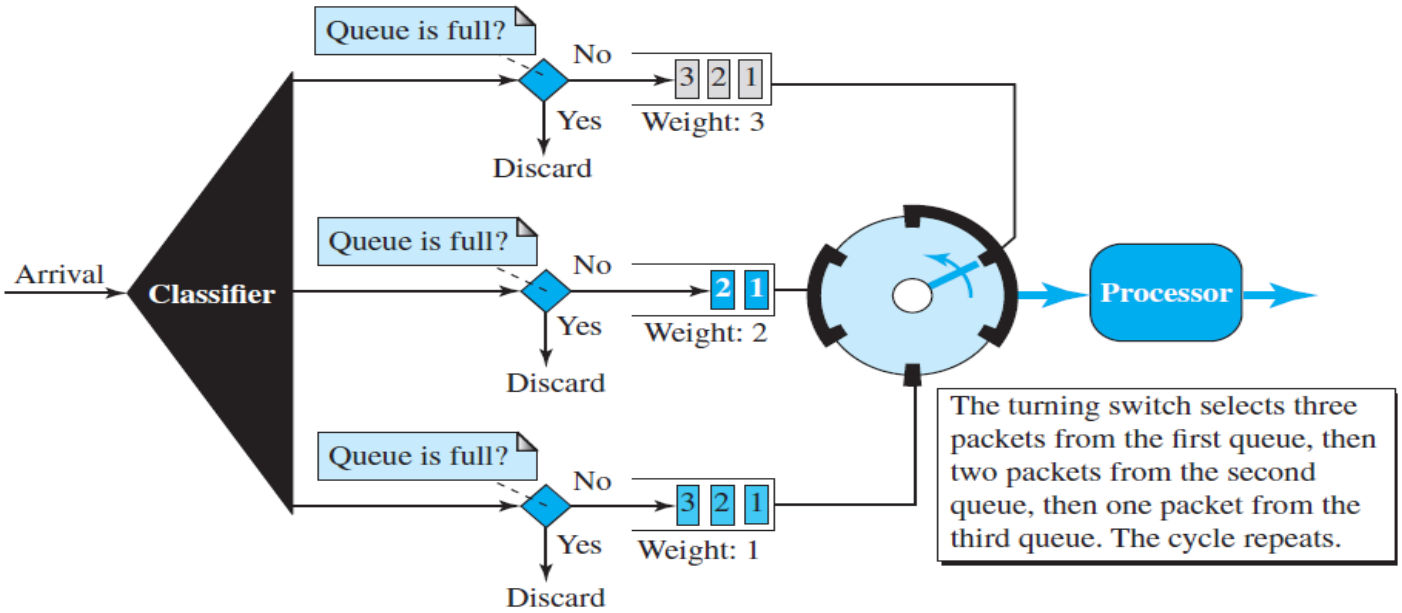


Figure: Weighted fair Queuing

Traffic Shaping: Leaky Bucket Algorithm

- To control the amount and the rate of traffic is called **traffic shaping** or **traffic policing**
  - *Traffic shaping* is used when the traffic leaves a network
  - *Traffic policing* is used when the data enters the network
- **Leaky Bucket**:
  - Consider a bucket with a small hole at the bottom
  - Water leaks from the bucket at a constant
  - The rate at which the water leaks does not depend on the rate at which the water is input rate
  - The input rate can vary, but the output rate remains constant.
  - Leaky bucket can smooth out bursty traffic.
  - Bursty chunks are stored in the bucket and sent out at an average rate

Leaky Bucket

A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

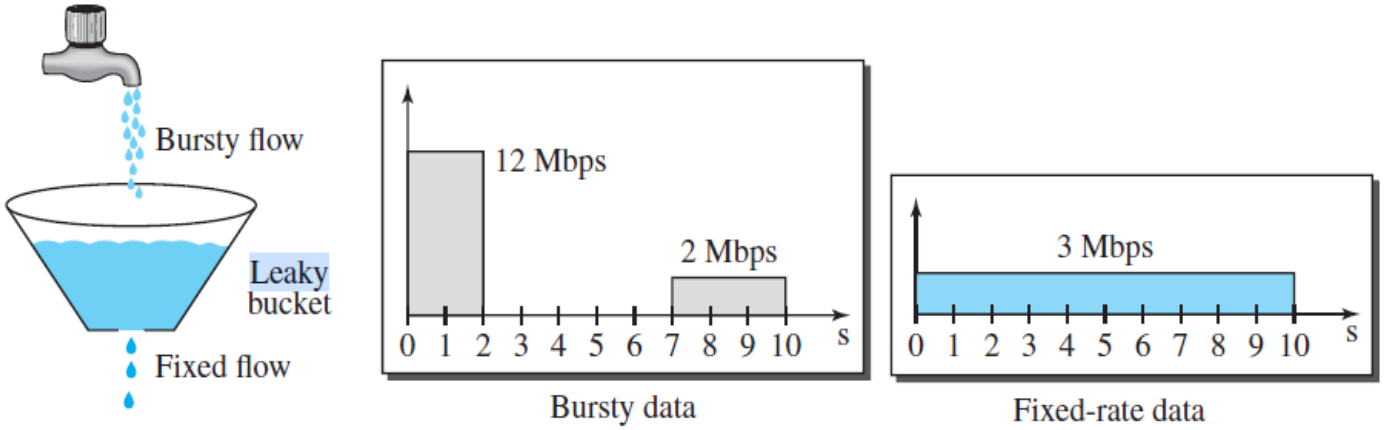


Figure: Leaky Bucket

Traffic Shaping: Token Bucket Algorithm

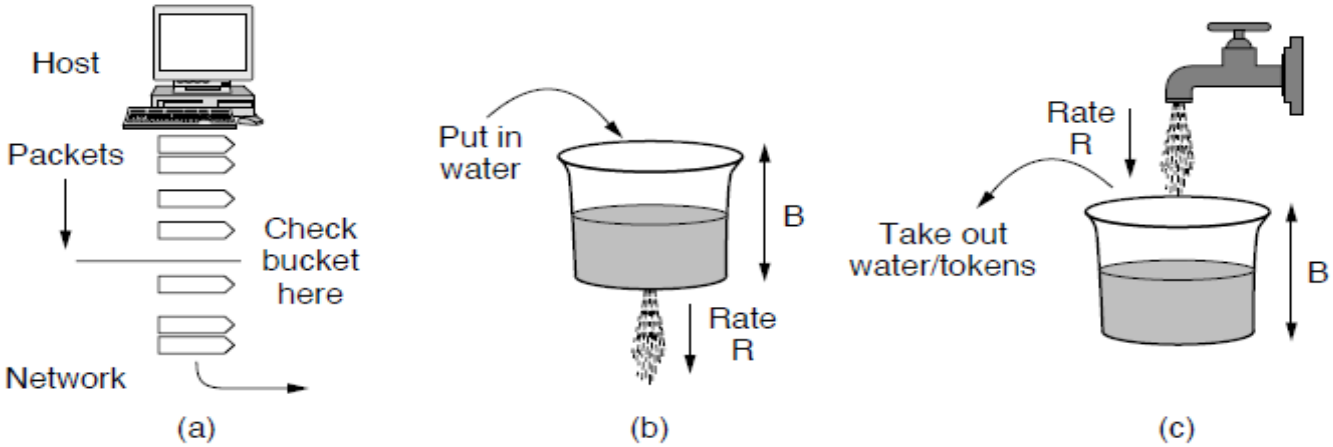


Figure: Leaky and Token Buckets

- The token bucket algorithm **allows bursty traffic and prevents data overflow**
- To send a packet we must be able to take water/tokens
- The system removes one token for every cell of data sent.
- If the bucket is empty, we must wait until more tokens arrive before we can send another packet

Token Bucket

The token bucket allows bursty traffic at a regulated maximum rate.

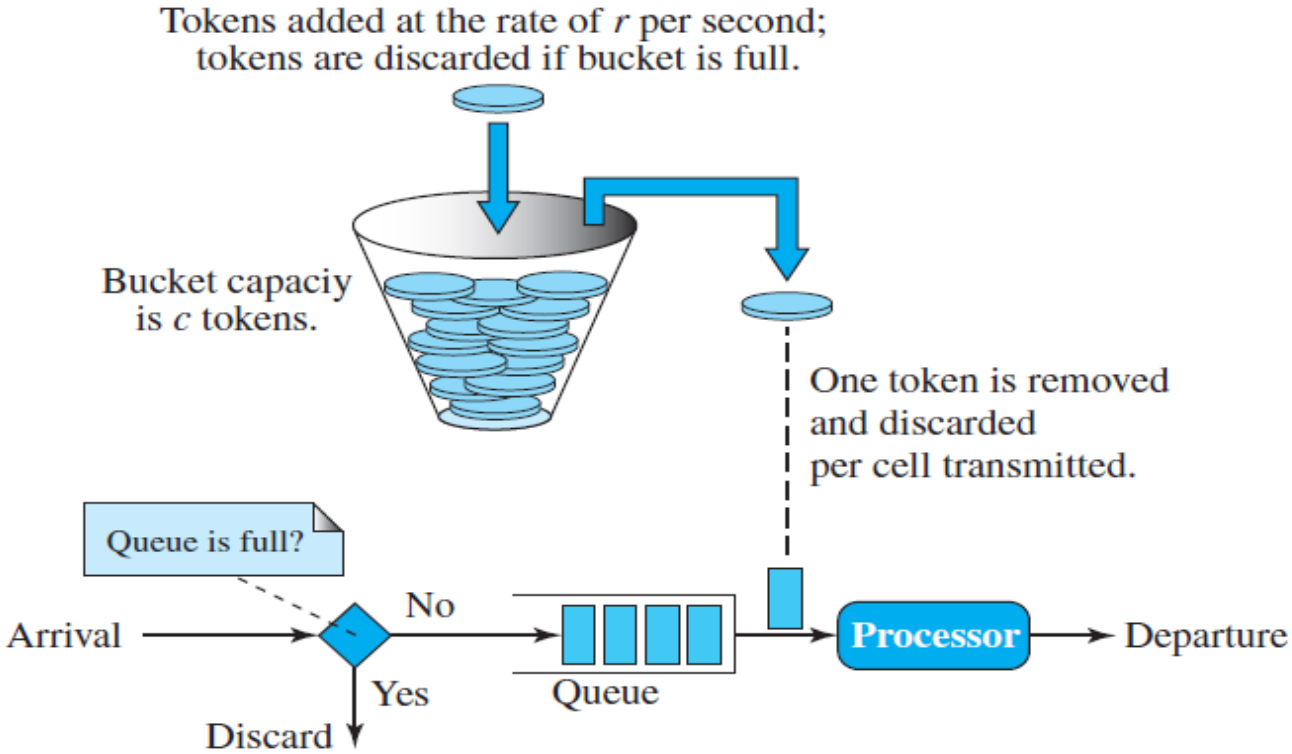


Figure: Token Bucket

In practice, first token bucket is used to prevent loss of data and allow burst traffic. Next the leaky bucket is used to convert bursty traffic to fixed data rate

Integrated Services

- Some applications needed a minimum amount of band width to function
- To provide different QoS for different applications, IETF developed the Integrated Services
- This is a flow-based architecture model where resources such as bandwidth are explicitly reserved for a given data flow
- The model is based on three schemes
  - The packets are first classified according to the service they require
  - Model uses scheduling to forward the packets (according to their flow characteristics)
  - Devices like routers use admission control to determine if available resources are enough to handle the flow.

Integrated Services using RSVP

Resource Reservation Protocol

- Integrated Services is a flow-based QoS model designed for IP.
  - All accommodations need to be made before a flow can start
- We need a connection-oriented service at the network layer
  - IP is currently a connectionless protocol
  - Need another protocol to be run on top of IP
  - RSVP is a connection-oriented protocol that needs to have connection establishment and connection termination phases
- This protocol is used for making the reservations
- **Problems with Integrated services**
  - Scalability: Integrated Services model requires that each router keep information for each flow
    - Keeping information is troublesome as we keep adding routers
  - Service-Type Limitation: Integrated Services model provides only two types of services, guaranteed and control-load
    - Applications that require trade-offs between delay and loss can't use this service

Differentiated services

- This is introduced by the IETF (Internet Engineering Task Force) to handle the shortcomings of Integrated Services
- In this model, **packets are marked by applications into classes** according to their priorities
  - Per-flow service is changed to per-class service
  - The **routing of the packet is based on the class of service** defined in the packet (not the flow)
- Processing was moved from the core of the network to the edge of the network-Solves scalability problem
  - Routers do not have to store information about flows

Review Questions

- Illustrate the different flow characteristics used to describe the quality of service in transport layer?
- Illustrate the techniques to improve QoS in networks
- Describe leaky bucket Algorithm
- Describe token bucket Algorithm
- Compare leaky bucket and token bucket algorithm

Acknowledge various sources for the images.
Thankyou