# Unit IV: Transport Layer


Course: Computer Networks
Instructor: Saurabh Kumar
LNMIIT, Jaipur

March 24, 2021

# Outline

LNMIIT
The LNM Institute of Information Technology

- Transport Layer Service
- Connection less Transport: UDP
- Connection Oriented Transport: TCP
- Congestion Control

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic
  - Congestion

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic
  - Congestion
  - Congestion Control Mechanisms

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic
  - Congestion
  - Congestion Control Mechanisms
  - Congestion Control in TCP

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic
  - Congestion
  - Congestion Control Mechanisms
  - Congestion Control in TCP
  - Quality of Service (QoS)

# Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Congestion control and quality of service are two issues related to the data link layer, the network layer, and the transport layer.
- Topics to Discuss
  - Data Traffic
  - Congestion
  - Congestion Control Mechanisms
  - Congestion Control in TCP
  - Quality of Service (QoS)
  - Techniques to Improve QoS

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Traffic descriptors are qualitative values that represent a data flow.

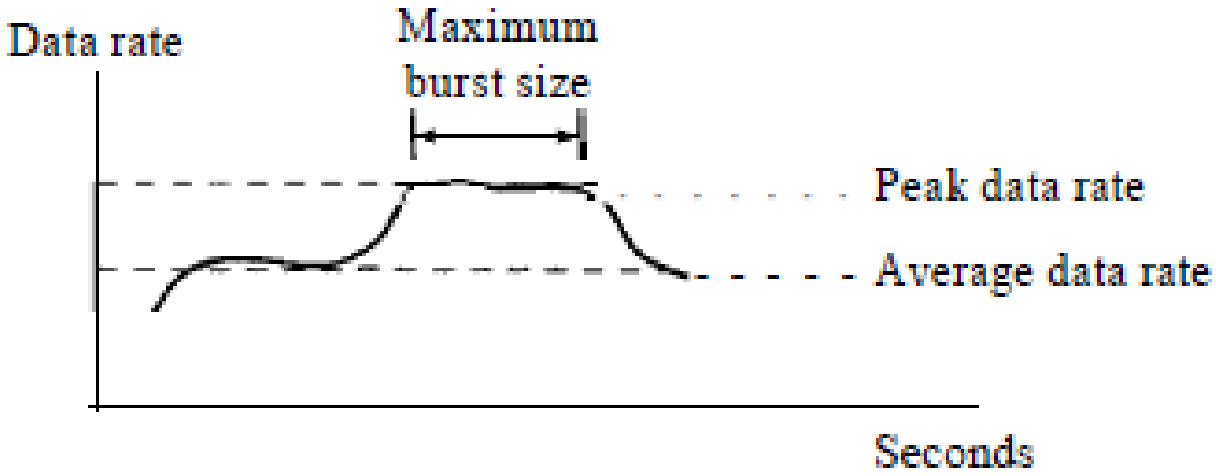



Figure: Traffic Descriptors

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Traffic descriptors are qualitative values that represent a data flow.

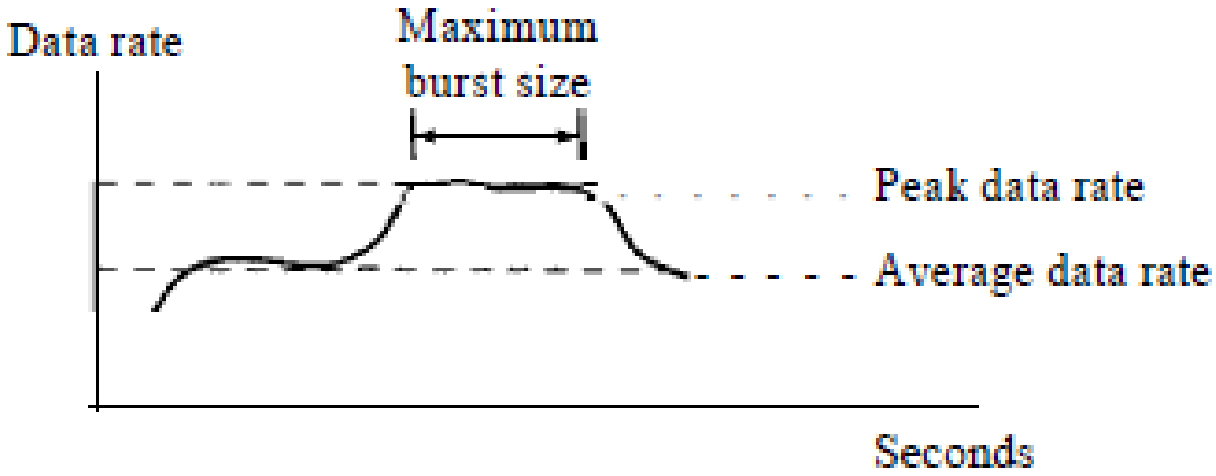



Figure: Traffic Descriptors

  - Average data rate: is the number of bits sent during a period of time, divided by the number of seconds in that period. It signifies the average bandwidth needed by the traffic.

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum burst size: refers to the maximum length of time the traffic is generated at the peak rate.

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum burst size: refers to the maximum length of time the traffic is generated at the peak rate.
  - Effective bandwidth: is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum burst size: refers to the maximum length of time the traffic is generated at the peak rate.
  - Effective bandwidth: is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.
- Traffic Profiles: constant bit rate

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum burst size: refers to the maximum length of time the traffic is generated at the peak rate.
  - Effective bandwidth: is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.
- Traffic Profiles: constant bit rate, variable bit rate

# Data Traffic

LNMIIT
The LNM Institute of Information Technology

- Traffic Descriptor
  - Peak data rate: defines the maximum data rate of the traffic. it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum burst size: refers to the maximum length of time the traffic is generated at the peak rate.
  - Effective bandwidth: is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.
- Traffic Profiles: constant bit rate, variable bit rate, bursty

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues
  - if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues
  - if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.
  - if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues
  - if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.
  - if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.
- Network performance

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues
  - if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.
  - if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.
- Network performance
  - Delay versus load

# Congestion

LNMIIT
The LNM Institute of Information Technology

- Preliminaries
  - Load: the number of packets sent to the network.
  - Capacity: the number of packets a network can handle.
  - Congestion: Congestion in a network may occur if the load on the network is greater than the capacity of the network.
  - Congestion control: refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- Two important issues
  - if the rate of packet arrival is higher than the packet processing rate, the input queues become longer and longer.
  - if the packet departure rate is less than the packet processing rate, the output queues become longer and longer.
- Network performance
  - Delay versus load
  - Throughput versus load

# Congestion Control

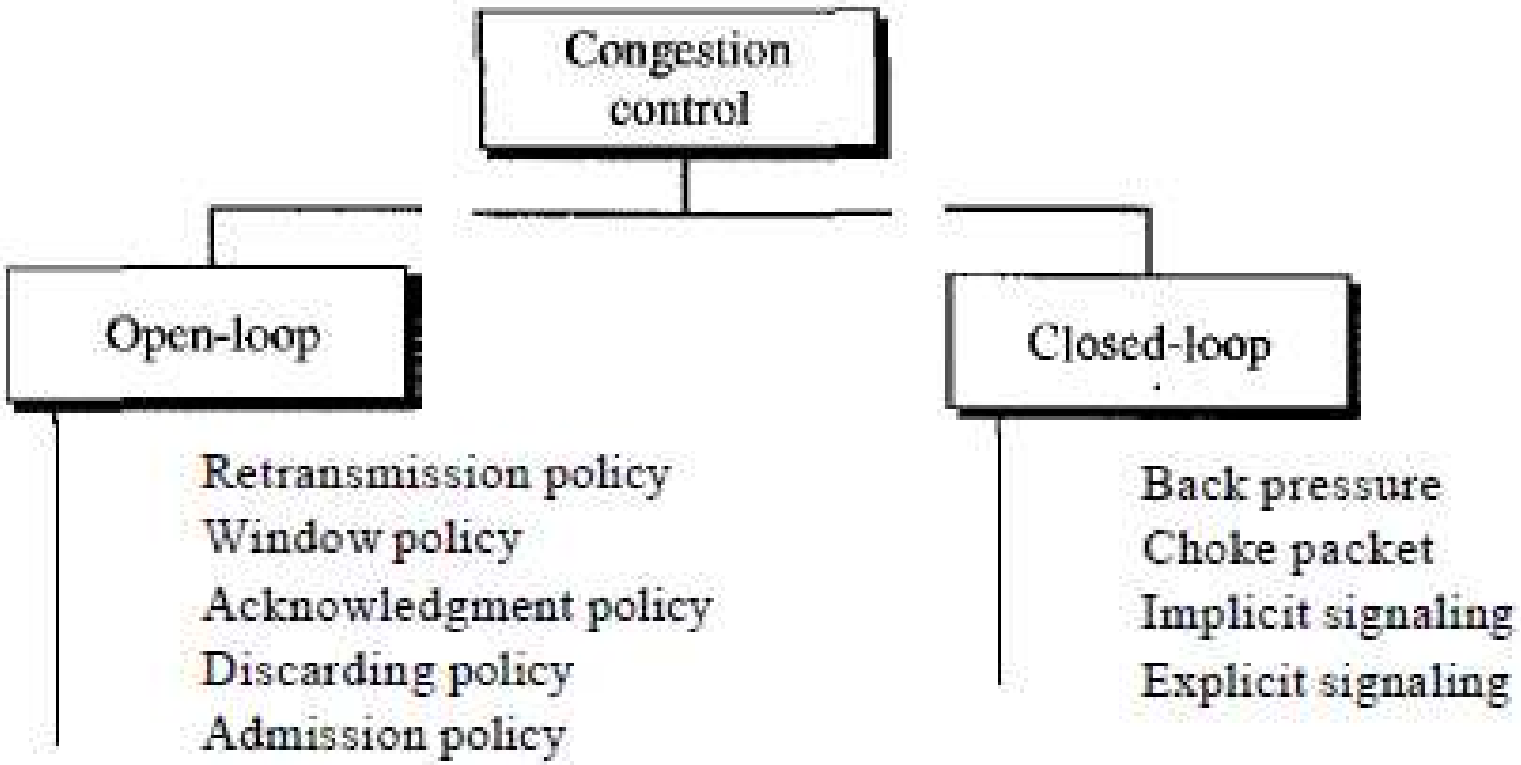



Figure: Congestion control categories

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- In open-loop congestion control, policies are applied to prevent congestion before it happens.
- In these mechanisms, congestion control is handled by either the source or the destination.

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- In open-loop congestion control, policies are applied to prevent congestion before it happens.
- In these mechanisms, congestion control is handled by either the source or the destination.
- Retransmission Policy
  - Retransmission is sometimes unavoidable.
  - If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.
  - Retransmission in general may increase congestion in the network.
  - However, a good retransmission policy can prevent congestion.
  - The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.
  - Example: the retransmission policy used by TCP is designed to prevent or alleviate congestion.

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Window Policy
  - The type of window at the sender may also affect congestion.
  - The Selective Repeat window is better than the Go-Back-N window for congestion control.
  - In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver.
  - This duplication may make the congestion worse.
  - The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Window Policy
  - The type of window at the sender may also affect congestion.
  - The Selective Repeat window is better than the Go-Back-N window for congestion control.
  - In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver.
  - This duplication may make the congestion worse.
  - The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.
- Acknowledgment Policy
  - If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
  - A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires.
  - A receiver may decide to acknowledge only N packets at a time. We need to know that the acknowledgments are also part of the load in a network.
  - Sending fewer acknowledgments means imposing less load on the network.

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Discarding Policy
  - A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
  - For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

# Open-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Discarding Policy
  - A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
  - For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.
- Admission Policy
  - An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks.
  - Switches in a flow first check the resource requirement of a flow before admitting it to the network.
  - A router can deny establishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion.

# Closed-Loop Congestion Control

- Closed-loop congestion control mechanisms try to alleviate congestion after it happens.
- Backpressure
  - In this technique, a congested node stops receiving data from the immediate upstream node or nodes.
  - This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes.
  - Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source.
  - Application: can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is coming.

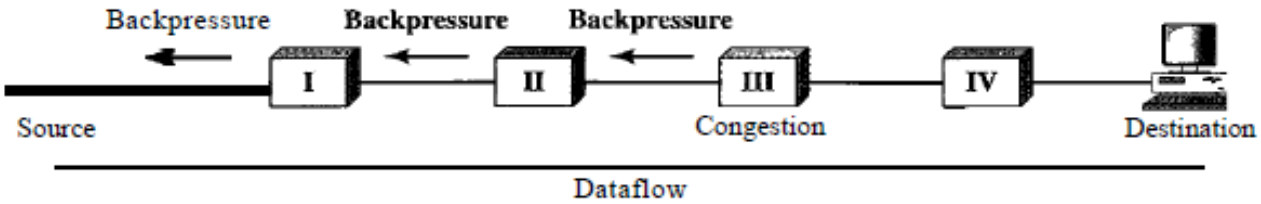



Figure: Backpressure method for alleviating congestion

# Closed-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Choke Packet
  - A choke packet is a packet sent by a node to the source to inform it of congestion.
  - In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly.
  - The intermediate nodes through which the packet has traveled are not warned.
  - Application: ICMP

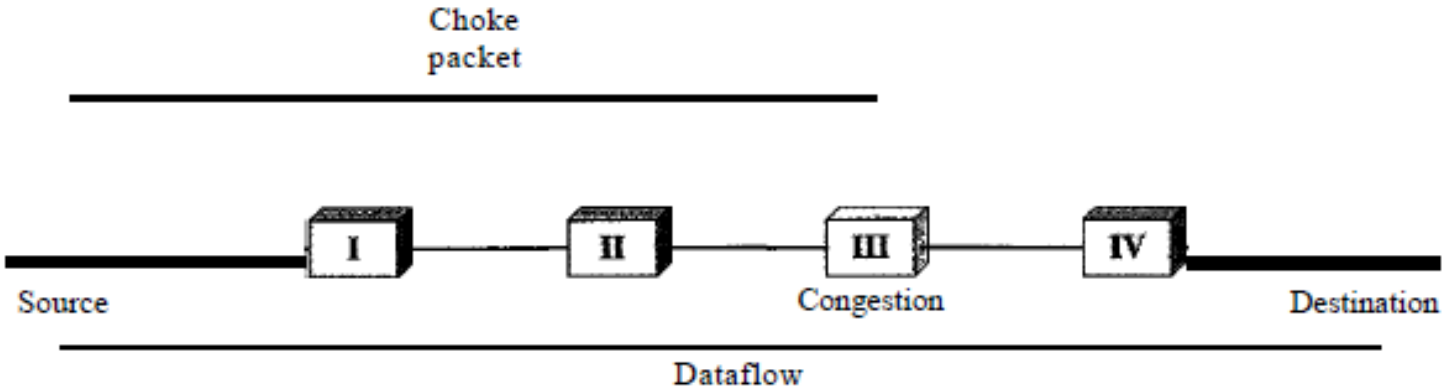



Figure: Choke packet

# Closed-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Implicit Signaling
  - There is no communication between the congested node or nodes and the source.
  - The source guesses that there is a congestion somewhere in the network from other symptoms.
  - Example: sending too many packet without acknowledgment, delay in acknowledgment reception, etc.

# Closed-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Implicit Signaling
  - There is no communication between the congested node or nodes and the source.
  - The source guesses that there is a congestion somewhere in the network from other symptoms.
  - Example: sending too many packet without acknowledgment, delay in acknowledgment reception, etc.
- Explicit Signaling
  - The node that experiences congestion can explicitly send a signal to the source or destination.
  - In the explicit signaling method, the signal is included in the packets that carry data.

# Closed-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Implicit Signaling
  - There is no communication between the congested node or nodes and the source.
  - The source guesses that there is a congestion somewhere in the network from other symptoms.
  - Example: sending too many packet without acknowledgment, delay in acknowledgment reception, etc.
- Explicit Signaling
  - The node that experiences congestion can explicitly send a signal to the source or destination.
  - In the explicit signaling method, the signal is included in the packets that carry data.
  - Types:
    - Backward signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

# Closed-Loop Congestion Control

LNMIIT
The LNM Institute of Information Technology

- Implicit Signaling
  - There is no communication between the congested node or nodes and the source.
  - The source guesses that there is a congestion somewhere in the network from other symptoms.
  - Example: sending too many packet without acknowledgment, delay in acknowledgment reception, etc.
- Explicit Signaling
  - The node that experiences congestion can explicitly send a signal to the source or destination.
  - In the explicit signaling method, the signal is included in the packets that carry data.
  - Types:
    - Backward signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.
    - Forward Signaling: A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Window
  - The sender window size is determined by
    - buffer space in the receiver, and
    - congestion in the network
  - *Actual window size = minimum (rwnd, cwnd)*, where *rwnd* is the receiver window size, and *cwnd* is the congestion window.

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Window
  - The sender window size is determined by
    - buffer space in the receiver, and
    - congestion in the network
  - *Actual window size = minimum (rwnd, cwnd)*, where *rwnd* is the receiver window size, and *cwnd* is the congestion window.
- Congestion Policy
  - TCP's general policy for handling congestion is based on three phases: slow start, congestion avoidance, and congestion detection.

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Window
  - The sender window size is determined by
    - buffer space in the receiver, and
    - congestion in the network
  - *Actual window size = minimum (rwnd, cwnd)*, where *rwnd* is the receiver window size, and *cwnd* is the congestion window.
- Congestion Policy
  - TCP's general policy for handling congestion is based on three phases: slow start, congestion avoidance, and congestion detection.
    - In the slow-start phase, the sender starts with a very slow rate of transmission, but increases the rate rapidly to reach a threshold.
    - When the threshold is reached, the data rate is reduced to avoid congestion.
    - If congestion is detected, the sender goes back to the slow-start or congestion avoidance phase based on how the congestion is detected.

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Slow Start: Exponential Increase
  - Idea: the size of the congestion window (cwnd) starts with one maximum segment size (MSS).
  - The MSS is determined during connection establishment by using an option of the same name.
  - The size of the window increases one MSS each time an acknowledgment is received.
  - The window starts slowly, but grows exponentially until it reaches a threshold.
  - If there is delayed ACKs, the increase in the size of the window is less than power of 2.
  - The sender keeps track of a variable named *ssthresh (slow-start threshold)* (most implementation: 65,535 bytes).
  - When the size of window in bytes reaches this threshold, slow start stops and the next phase starts.

# Congestion Control in TCP

- Slow Start: Exponential Increase

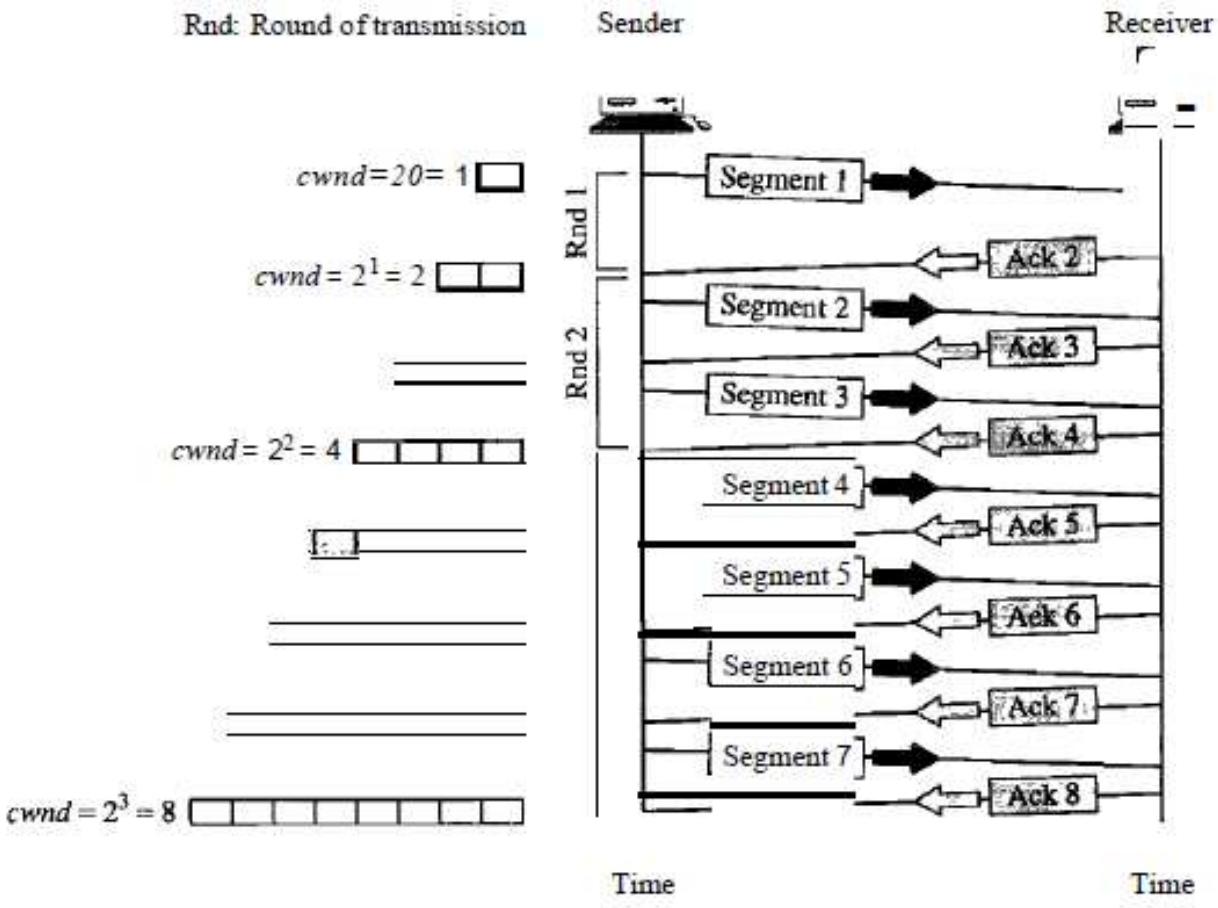



Figure: Slow start, exponential increase

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Avoidance: Additive Increase
  - TCP defines another algorithm called congestion avoidance, which undergoes an additive increase instead of an exponential one.
  - When the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins.
  - In this algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1.
  - The size of the congestion window increases additively until congestion is detected.

# Congestion Control in TCP

- Congestion Avoidance: Additive Increase

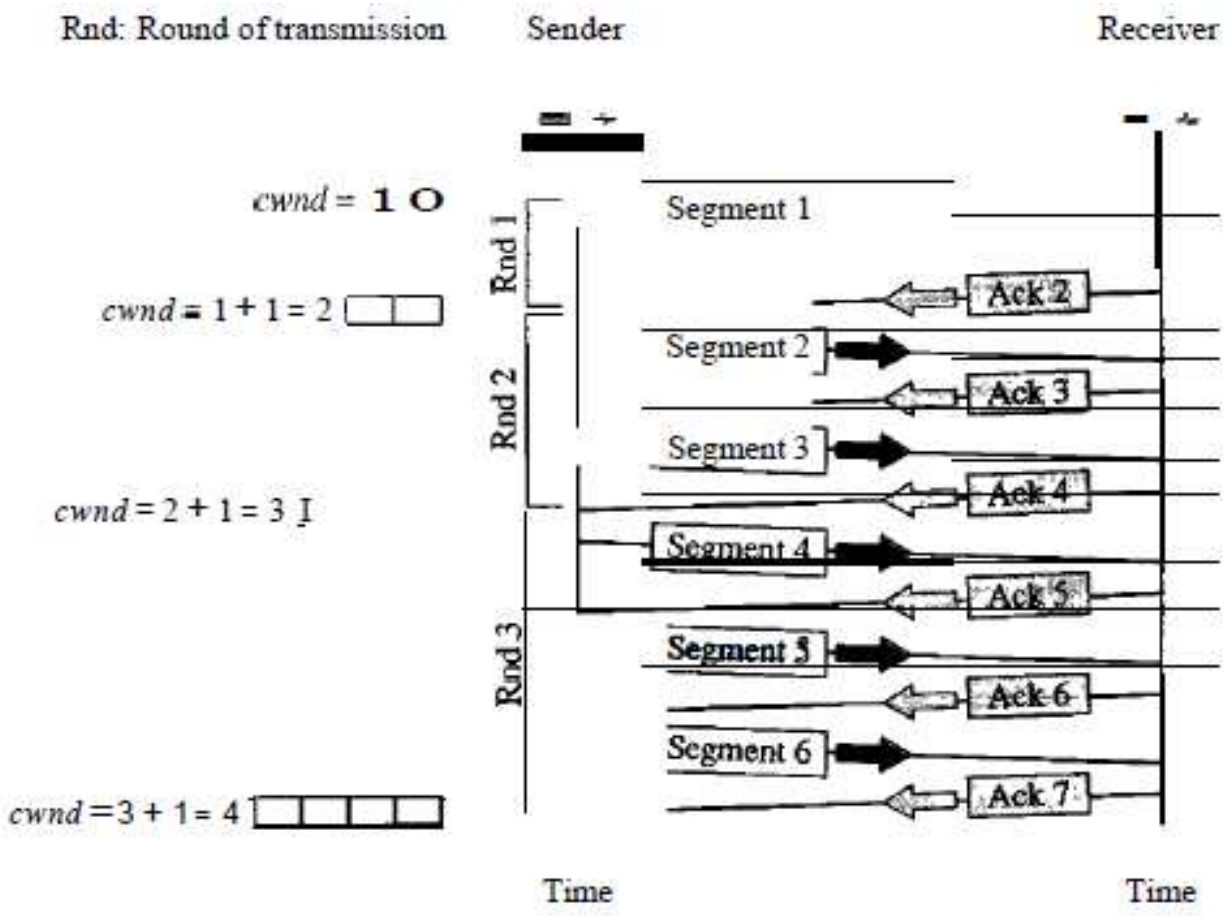



Figure: Congestion avoidance, additive increase

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Detection: Multiplicative Decrease
  - If congestion occurs, the congestion window size must be decreased.
  - The only way the sender can guess that congestion has occurred is by the need to retransmit a segment.
  - Retransmission can occur in one of two cases: when a timer times out or when three ACKs are received.
  - In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease.
  - If a time-out occurs, there is a stronger possibility of congestion; a segment has probably been dropped in the network, and there is no news about the sent segments. In this case TCP reacts strongly:
    - It sets the value of the threshold to one-half of the current window size.
    - It sets cwnd to the size of one segment.
    - It starts the slow-start phase again.

# Congestion Control in TCP

LNMIIT
The LNM Institute of Information Technology

- Congestion Detection: Multiplicative Decrease
  - If three ACKs are received, there is a weaker possibility of congestion; a segment may have been dropped, but some segments after that may have arrived safely since three ACKs are received. This is called fast transmission and fast recovery. In this case, TCP has a weaker reaction:
    - It sets the value of the threshold to one-half of the current window size.
    - It sets cwnd to the value of the threshold (some implementations add three segment sizes to the threshold).
    - It starts the congestion avoidance phase.
  - An implementations reacts to congestion detection in one of the following ways:
    - If detection is by time-out, a new slow-start phase starts.
    - If detection is by three ACKs, a new congestion avoidance phase starts.

# Quality of Service

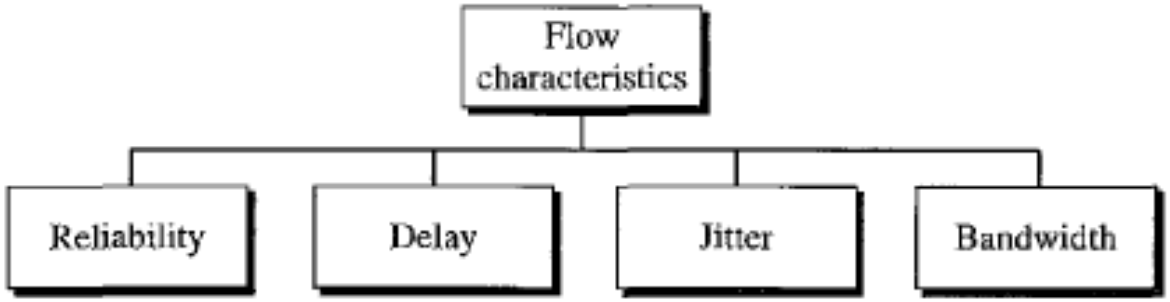



Figure: Flow Characteristics

# Quality of Service

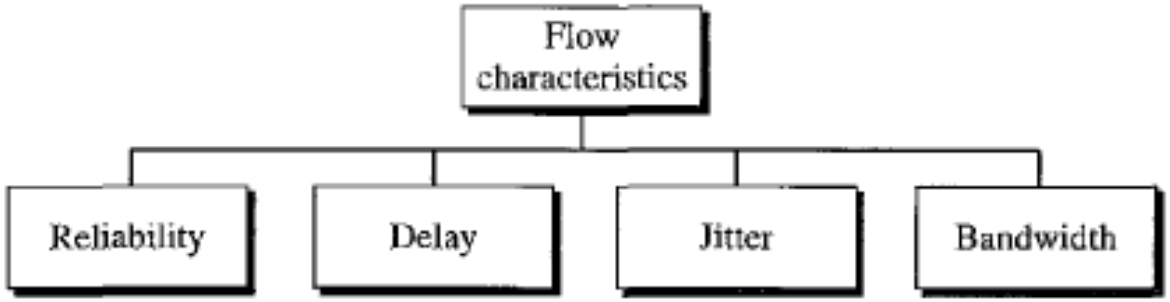



Figure: Flow Characteristics

- Techniques to improve QoS
  - Scheduling
  - Traffic Shaping
  - Resource Reservation
  - Admission Control

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Scheduling
  - Packets from different flows arrive at a switch or router for processing.
  - A good scheduling technique treats the different flows in a fair and appropriate manner.
  - Techniques: FIFO queuing, Priority queuing, Weighted fair queuing.

# Techniques to Improve QoS

- Scheduling
  - Packets from different flows arrive at a switch or router for processing.
  - A good scheduling technique treats the different flows in a fair and appropriate manner.
  - Techniques: FIFO queuing, Priority queuing, Weighted fair queuing.
  - FIFO Queuing
    - In first-in, first-out (FIFO) 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.
    - A FIFO queue is familiar to those who have had to wait for a bus at a bus stop.

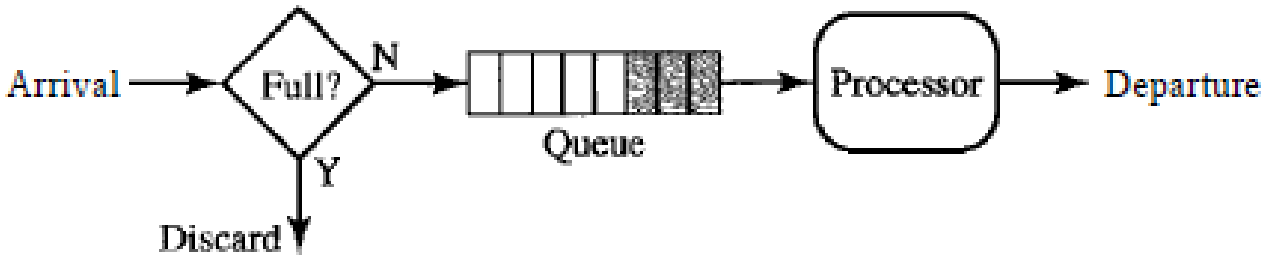
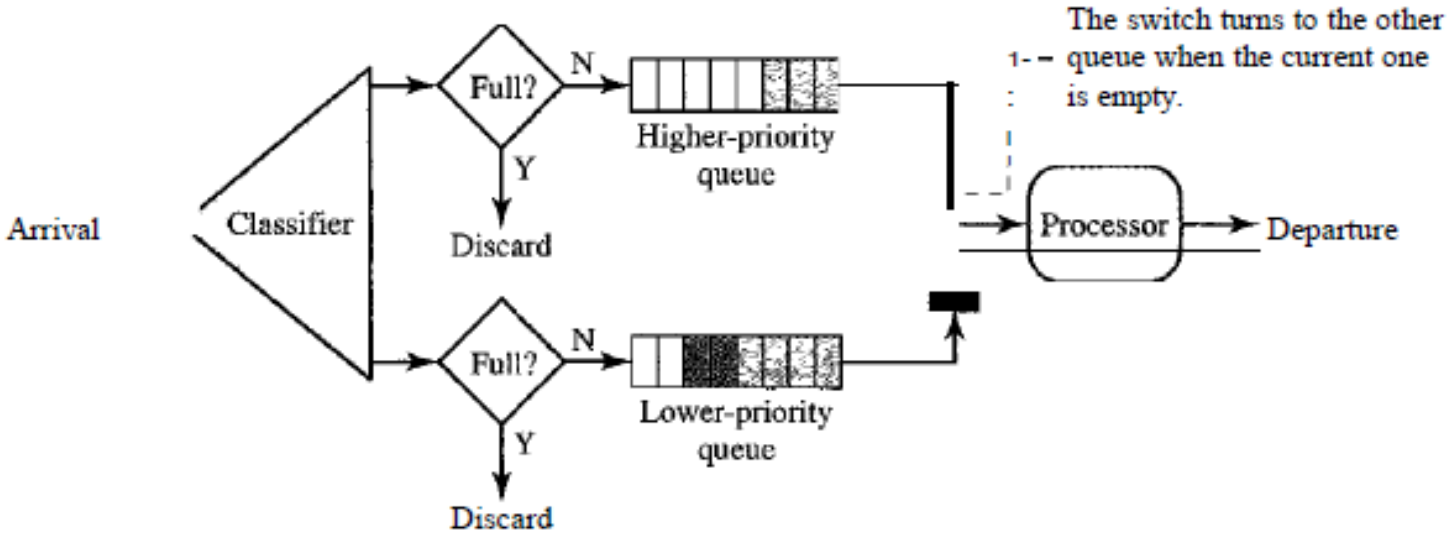



Figure: FIFO queue

# Techniques to Improve QoS

- Priority Queuing
  - In priority queuing, packets are first assigned to a priority class.
  - Each priority class has its own queue.
  - The packets in the highest-priority queue are processed first.
  - Packets in the lowest-priority queue are processed last.
  - Note: the system does not stop serving a queue until it is empty.
  - Advantage: can provide better QoS than the FIFO queue because higher priority traffic, such as multimedia, can reach the destination with less delay.
  - Disadvantage: 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 (starvation).



# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Weighted Fair Queuing
  - In this technique, 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).
  - The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.
  - If the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue.
  - If the system does not impose priority on the classes, all weights can be equaL In this way, we have fair queuing with priority.

# Techniques to Improve QoS

- Weighted Fair Queuing

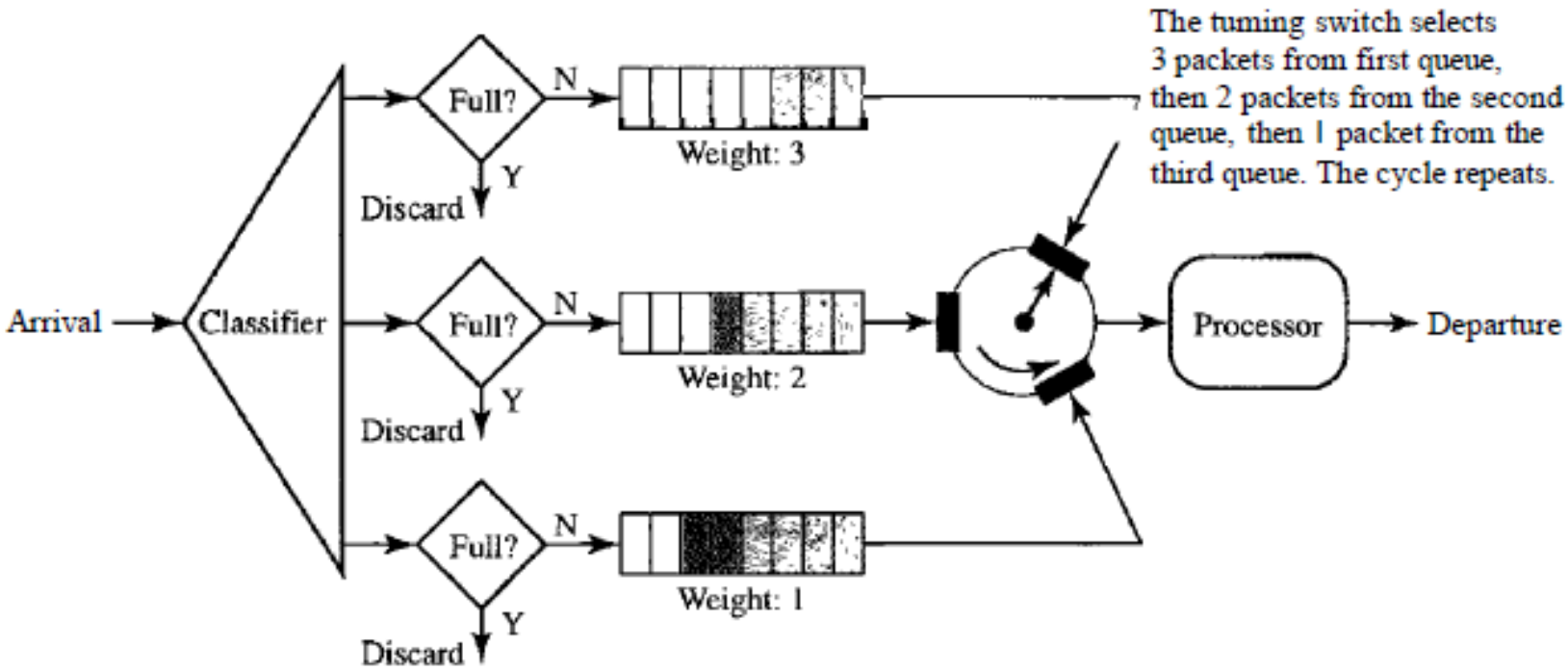



Figure: Weighted fair queuing

# Techniques to Improve QoS

- Traffic Shaping
  - Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.
  - Techniques: leaky bucket and token bucket.
  - Leaky Bucket

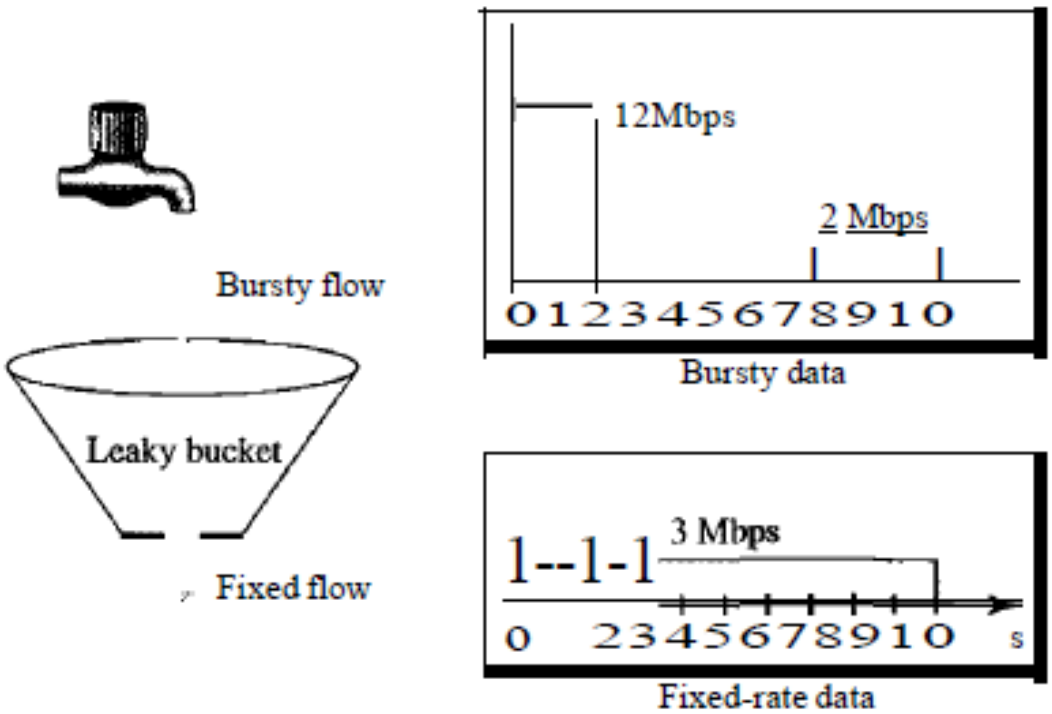



Figure: Leaky Bucket

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Leaky Bucket
  - If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water 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 unless the bucket is empty.
  - The input rate can vary, but the output rate remains constant.
  - Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic.
  - Bursty chunks are stored in the bucket and sent out at an average rate.

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Leaky Bucket Implementation
  - A FIFO queue holds the packets.
  - Fixed-size packets: the process removes a fixed number of packets from the queue at each tick of the clock.
  - Variable-size packets: the fixed output rate must be based on the number of bytes or bits.
  - Algorithm for Variable-size packets
    - Initialize a counter to $n$ at the tick of the clock.
    - If $n >$ size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until $n$ is smaller than the packet size.
    - Reset the counter and go to step 1.

# Techniques to Improve QoS

- Leaky Bucket Implementation
  - Note: 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.

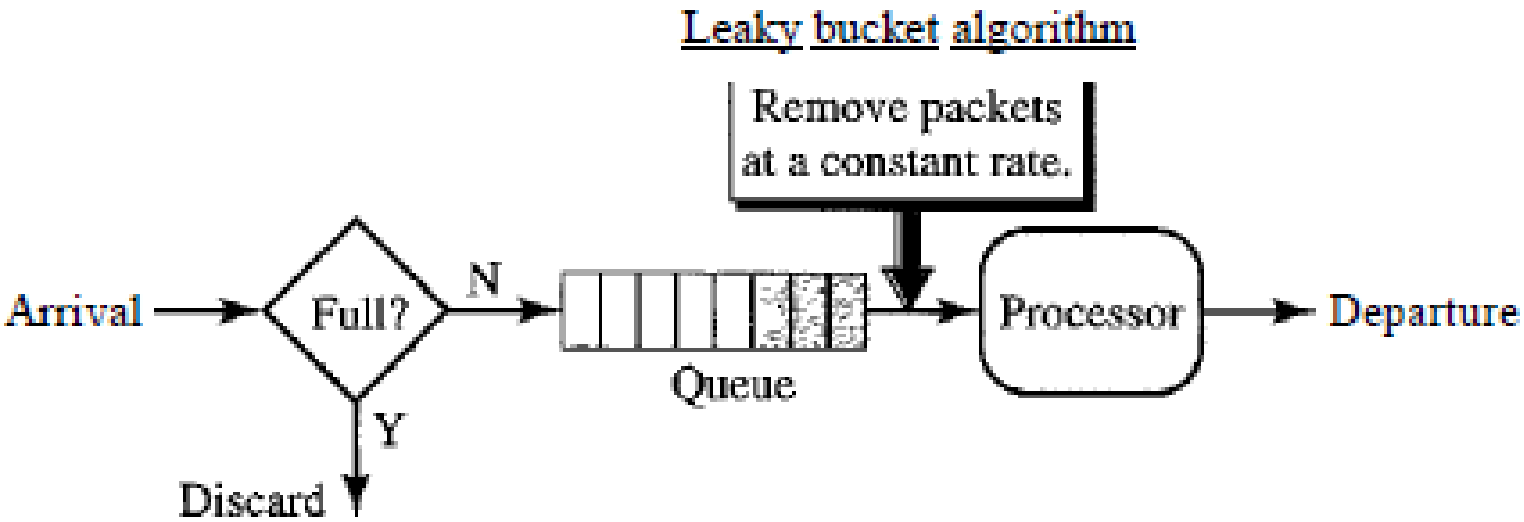



Figure: Leaky Bucket Implementation

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Token Bucket
  - The leaky bucket is very restrictive.
  - It does not credit an idle host.
  - For example, if a host is not sending for a while, its bucket becomes empty.
  - If the host has bursty data, the leaky bucket allows only an average rate.
  - The time when the host was idle is not taken into account.
  - On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens.
  - For each tick of the clock, the system sends $n$ tokens to the bucket.
  - The system removes one token for every cell (or byte) of data sent.
  - For example, if $n$ is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens.
  - The host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick.
  - In other words, the host can send bursty data as long as the bucket is not empty.

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Token Bucket Implementation
  - The token bucket can easily be implemented with a counter.
  - The token is initialized to zero.
  - Each time a token is added, the counter is incremented by 1.
  - Each time a unit of data is sent, the counter is decremented by 1.
  - When the counter is zero, the host cannot send data.

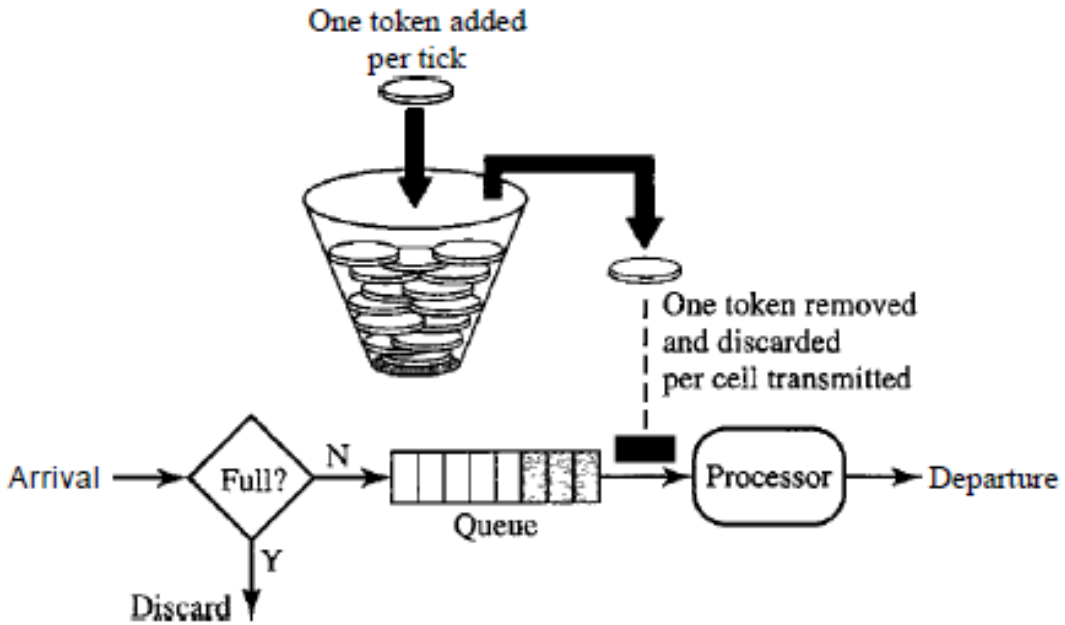



Figure: Token Bucket

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Combination of Leaky bucket and Token bucket
  - The two techniques can be combined to credit an idle host and at the same time regulate the traffic.
  - The leaky bucket is applied after the token bucket.
  - The rate of the leaky bucket needs to be higher than the rate of tokens dropped in the bucket.

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Combination of Leaky bucket and Token bucket
  - The two techniques can be combined to credit an idle host and at the same time regulate the traffic.
  - The leaky bucket is applied after the token bucket.
  - The rate of the leaky bucket needs to be higher than the rate of tokens dropped in the bucket.
- Resource Reservation
  - A flow of data needs resources such as a buffer, bandwidth, CPU time, etc.
  - The quality of service is improved if these resources are reserved beforehand.

# Techniques to Improve QoS

LNMIIT
The LNM Institute of Information Technology

- Combination of Leaky bucket and Token bucket
  - The two techniques can be combined to credit an idle host and at the same time regulate the traffic.
  - The leaky bucket is applied after the token bucket.
  - The rate of the leaky bucket needs to be higher than the rate of tokens dropped in the bucket.
- Resource Reservation
  - A flow of data needs resources such as a buffer, bandwidth, CPU time, etc.
  - The quality of service is improved if these resources are reserved beforehand.
- Admission Control
  - Admission control refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications.
  - Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.