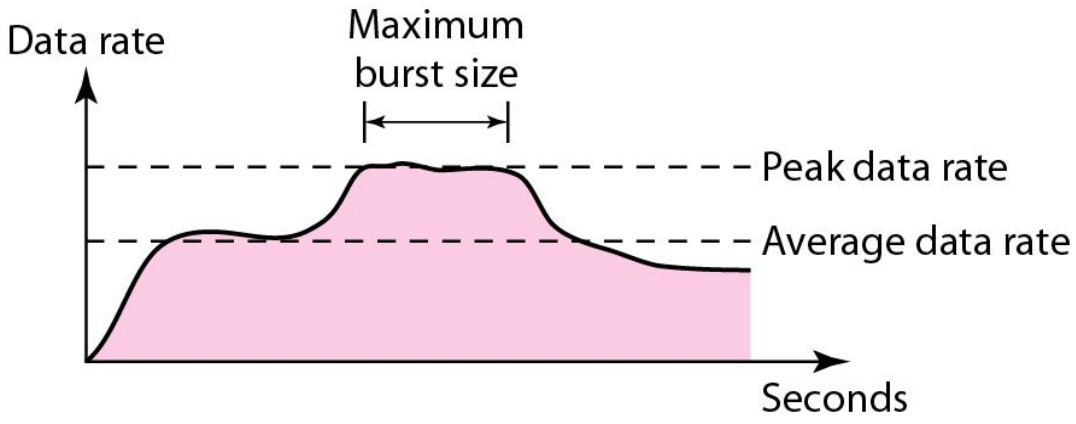
Congestion Control and Quality of Service

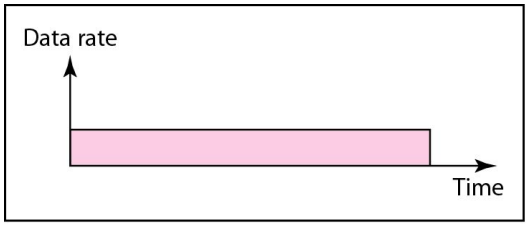
Traffic Descriptors

- Traffic descriptor are qualitative values that represent a data flow
- **Average data rate** = amount of data/time
- **Peak data rate**: the max. data rate of the traffic
- **Max. burst size**: the max. length of time the traffic is generated at the peak rate
- **Effective bandwidth**: bandwidth that the network needs to allocate for traffic flow

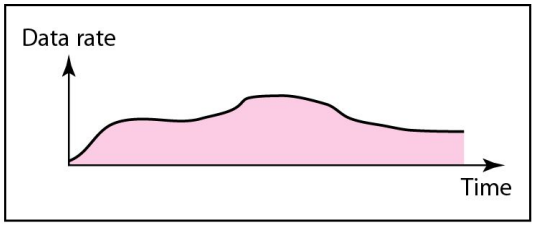


Traffic Profiles

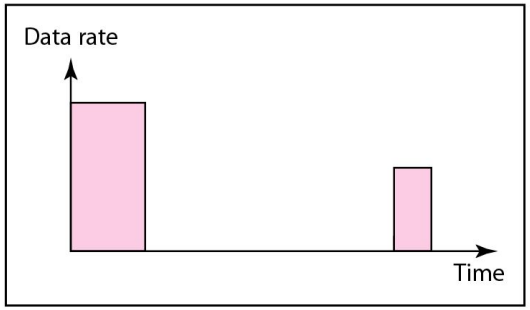
- Constant-bit-rate (CBR)
- Variable-bit-rate (VBR)
- Bursty



a. Constant bit rate



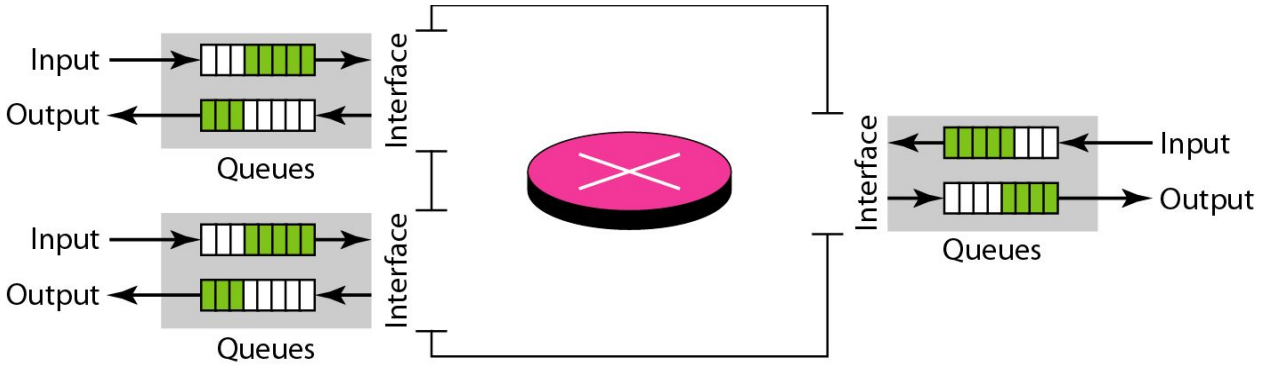
b. Variable bit rate



c. Bursty

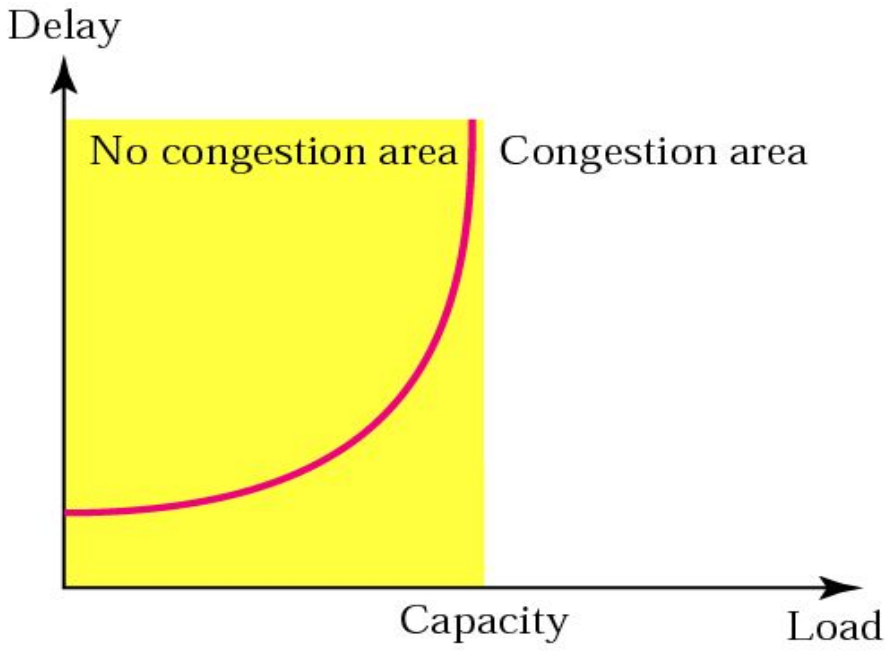
Congestion

- Congestion: the load on the network is greater than the capacity of the network
- Congestion control: the mechanisms to control the congestion and keep the load below the capacity
- Congestion occurs because routers and switches have queues- buffers that hold the packets before and after processing
- The rate of packet arrival > packet processing time □ input queue longer
- The packet departure time < packet processing time □ output queue longer



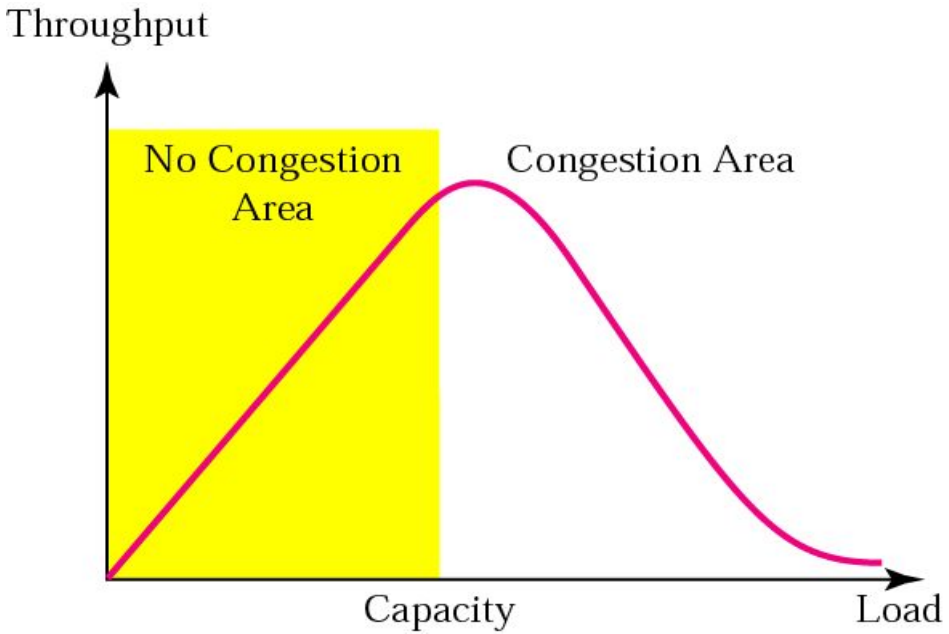
Network Performance-1

- Packet delay versus network load
- Delay id composed of propagation delay and processing delay



Network Performance-2

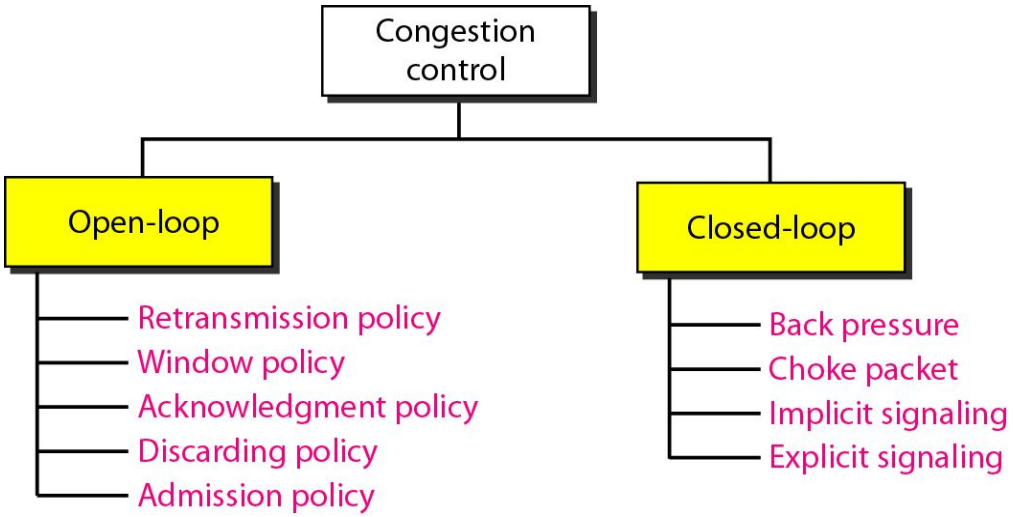
- Throughput versus network load
- Throughput: the number of packets passing through the network in a unit of time



Congestion Control

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

- Two broad categories: **open-loop congestion control** (prevention) and **closed-loop congestion control** (removal).

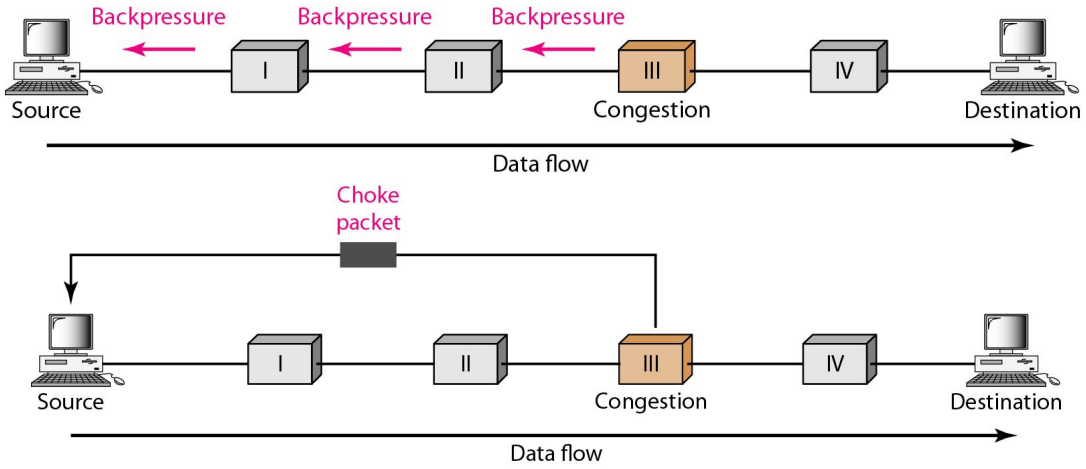


Open Loop Control: Prevention

- ***Retransmission*** policy and timers must to be designed to optimize efficiency and at the same time prevent congestion
- ***Window*** policy: Selective Repeat is better than Go-back-N
- ***Acknowledgement*** policy: does not ACK every packet
- ***Discard*** policy: prevent congestion and at the same time may not harm the integrity of the transmission
- ***Admission*** policy: Switch first check the resource requirement of a flow before admitting it to the network

Closed-Loop Congestion Control: Removal

- ***Back pressure***: inform the previous upstream router to reduce the rate of outgoing packets if congested
- ***Choke point***: a packet sent by a router to the source to inform it of congestion, similar to ICMP's source quench packet
- ***Implicit signaling***: slow down its sending rate by detecting an implicit signal concerning congestion
- ***Explicit signaling***: Backward signaling / Forward signaling



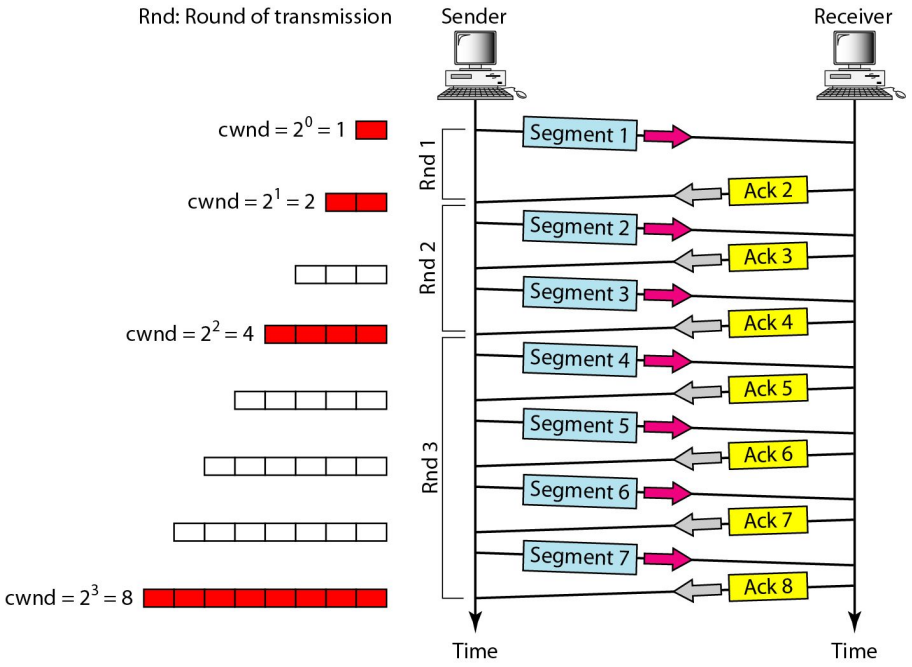
Congestion Control in TCP

- TCP assumes that the cause of a lost segment is due to congestion in the network.
- If the cause of the lost segment is congestion, retransmission of the segment does not remove the cause—it aggravates it.
- The sender has two pieces of information: the receiver-advertised window size and the congestion window size
- TCP Congestion window
  - ***Actual window size = minimum (rwnd, cwnd)***

    (where rwnd = receiver window size, cwnd = congestion window size)

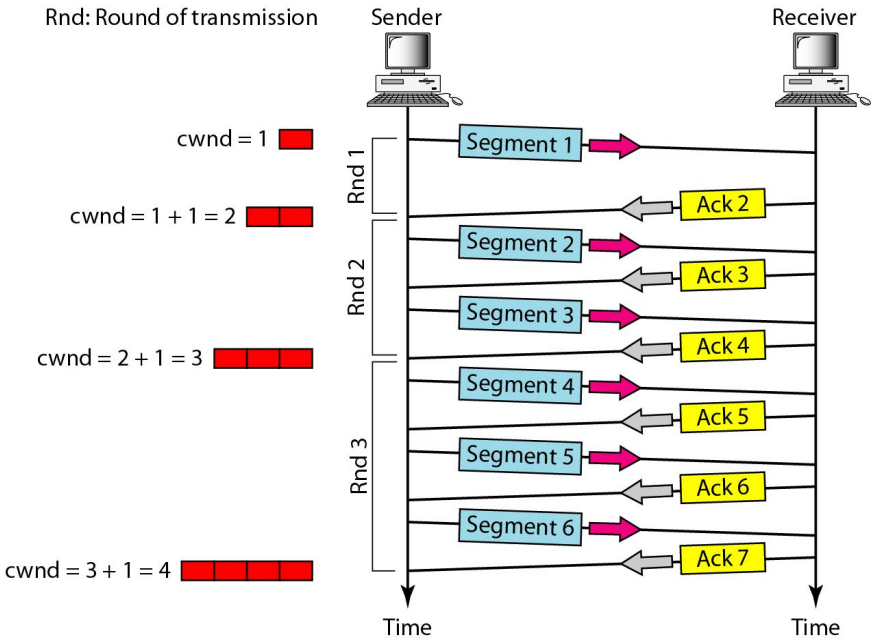
TCP Congestion Policy

- Based on three phases: slow start, congestion avoidance, and congestion detection
- **Slow Start: Exponential Increase**
  - In the slow-start algorithm, the size of the congestion window increases exponentially until it reaches a threshold



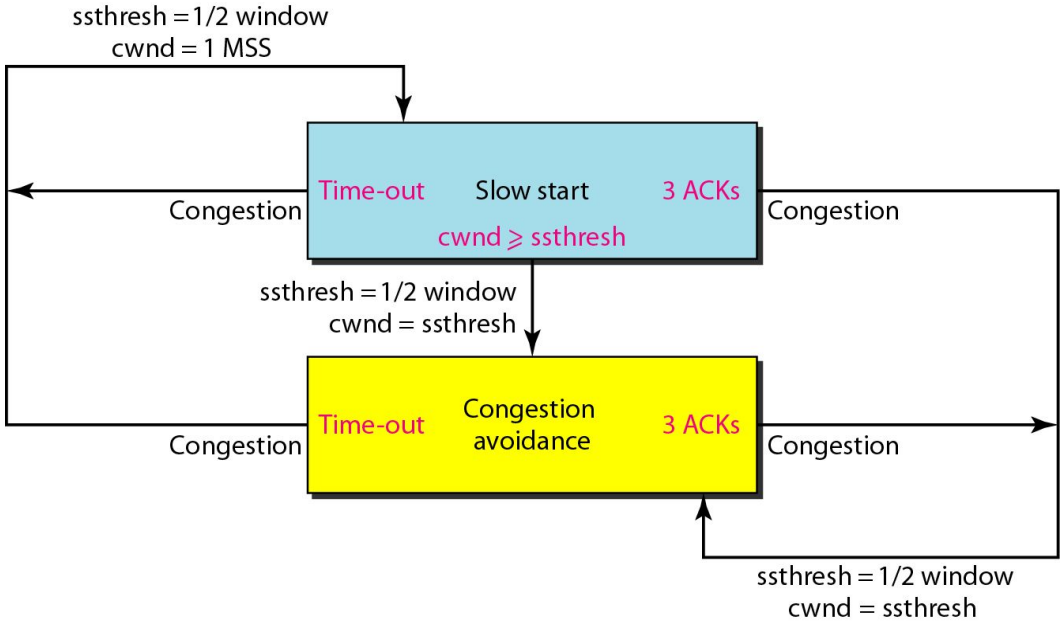
TCP Congestion Policy

- **Congestion Avoidance: Additive Increase**
  - The size of the congestion window increases additively until congestion is detected

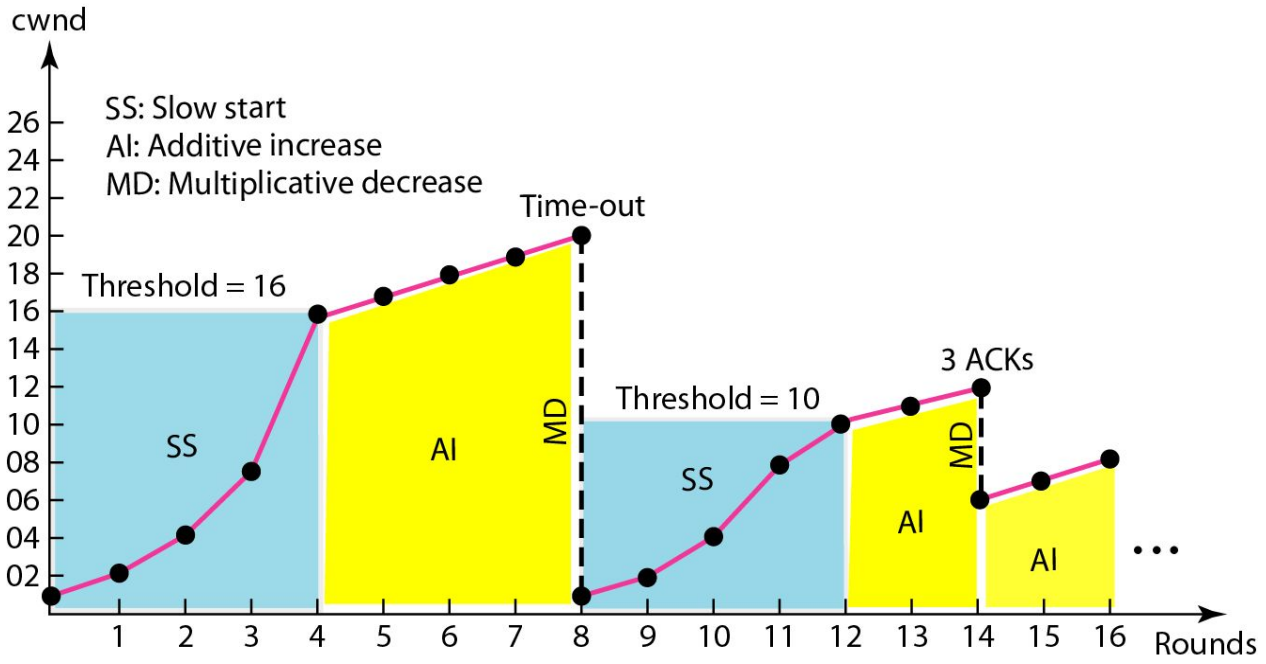


TCP Congestion Policy

- **Congestion Detection: Multiplicative Decrease**
- An implementation reacts to congestion detection in one of two 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
- **Summary**

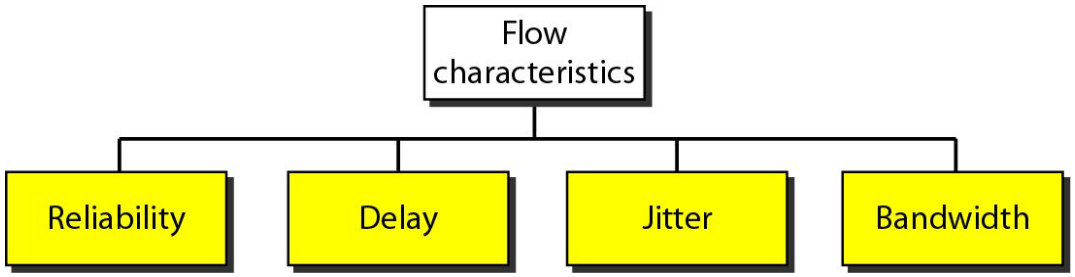


Congestion Example



Quality of Service (QoS)

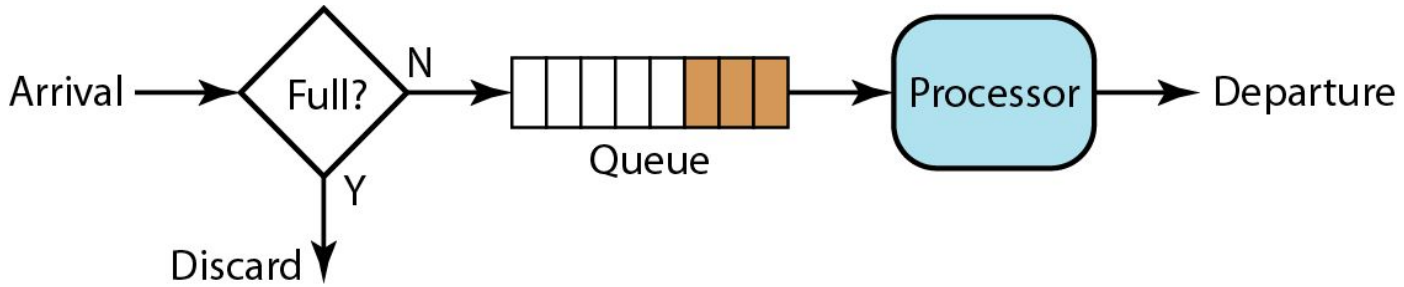
- Flow Characteristics:
  - Reliability
  - Delay
  - Jitter: the variation in delay for packets belonging to the same flow
  - Bandwidth
- Flow Classes:
  - Based on the characteristics, we can classify flows into groups, with each group having similar levels of characteristics



QoS Techniques

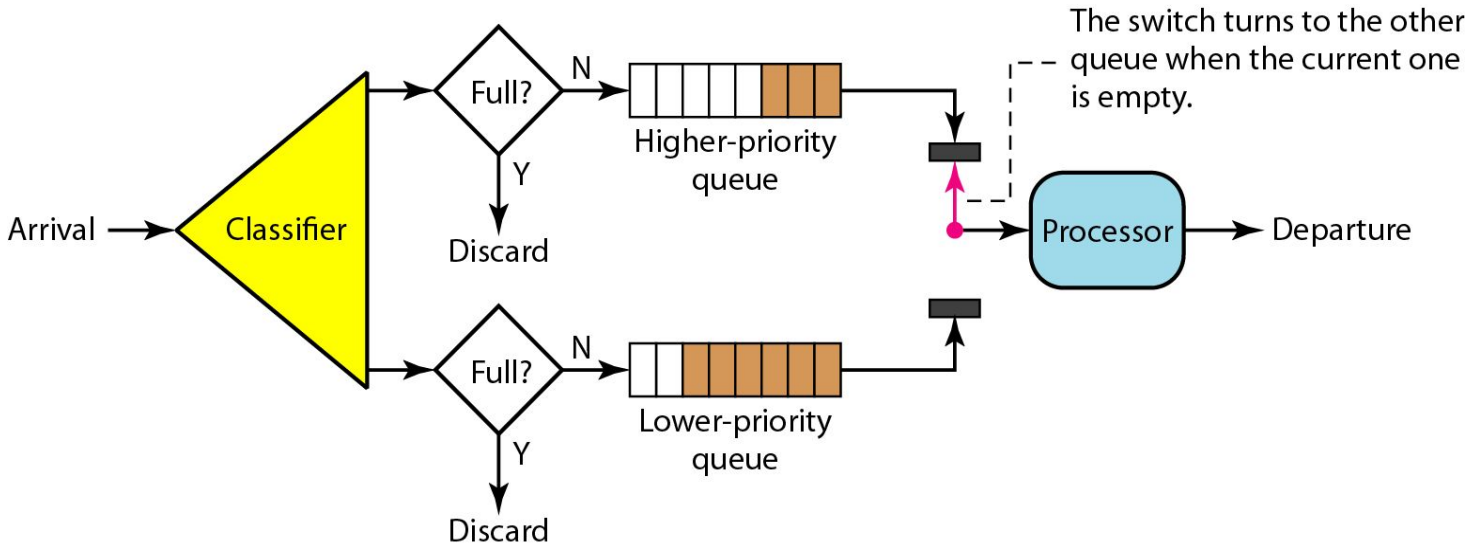
- **Scheduling**: FIFO queuing, priority queuing, and weighted fair queuing
- **Traffic shaping**: Leaky bucket, token bucket
- **Resource reservation**
- **Admission control**: accept or reject a flow based on predefined parameters called flow specification

- FIFO queuing



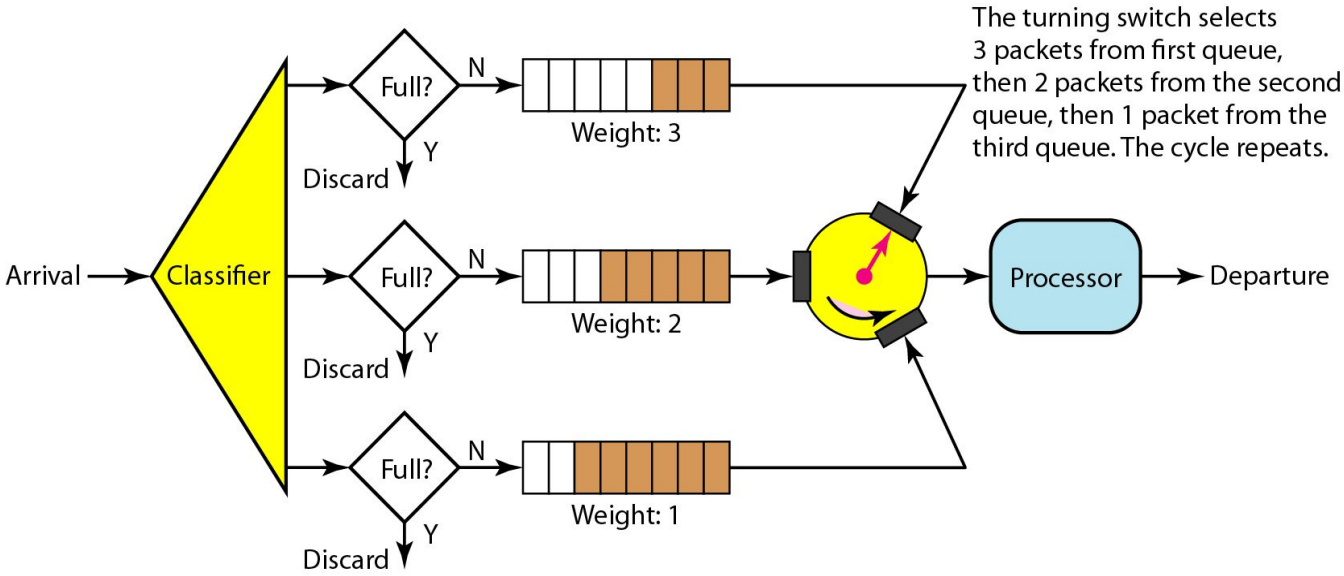
Priority Queuing

- Packets are first assigned to priority class. Each priority class has its own queue
- The packets in the highest-priority queue are processed first



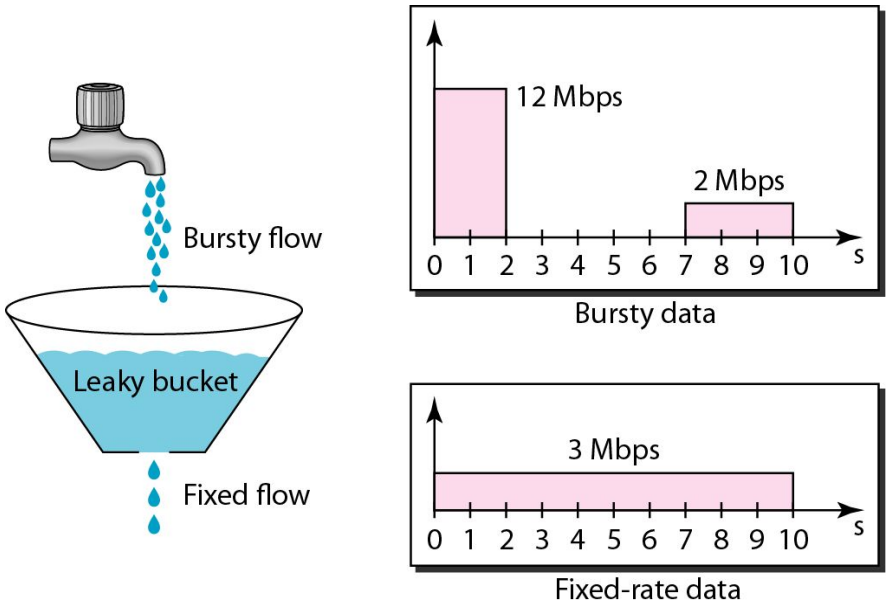
Weighted Fair Queuing

- The queues are weighted based on the priority of the queues
- The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the weight

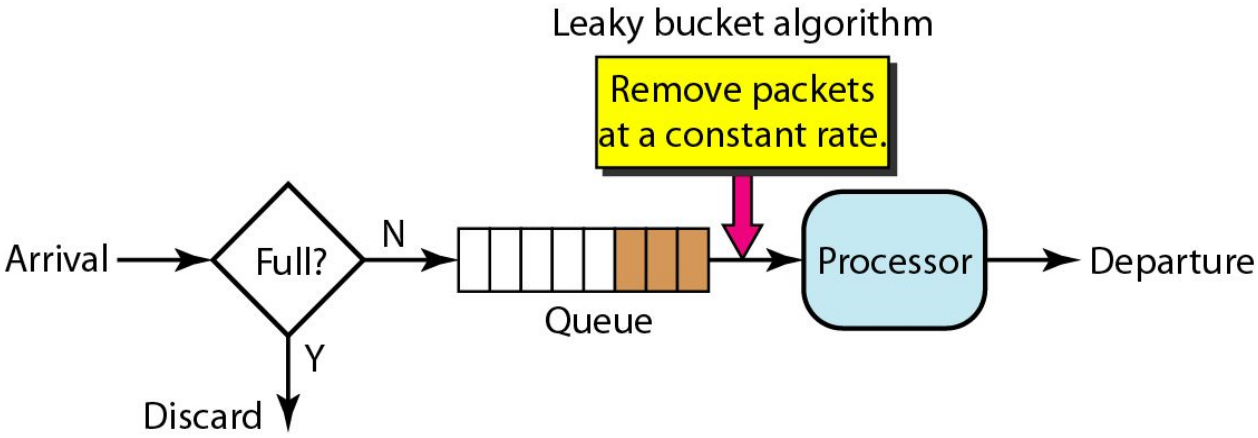


Traffic Shaping: Leaky Bucket

- Traffic shaping: to control the amount and the rate of the traffic sent to network
- Two techniques: *leaky bucket* and *token 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.



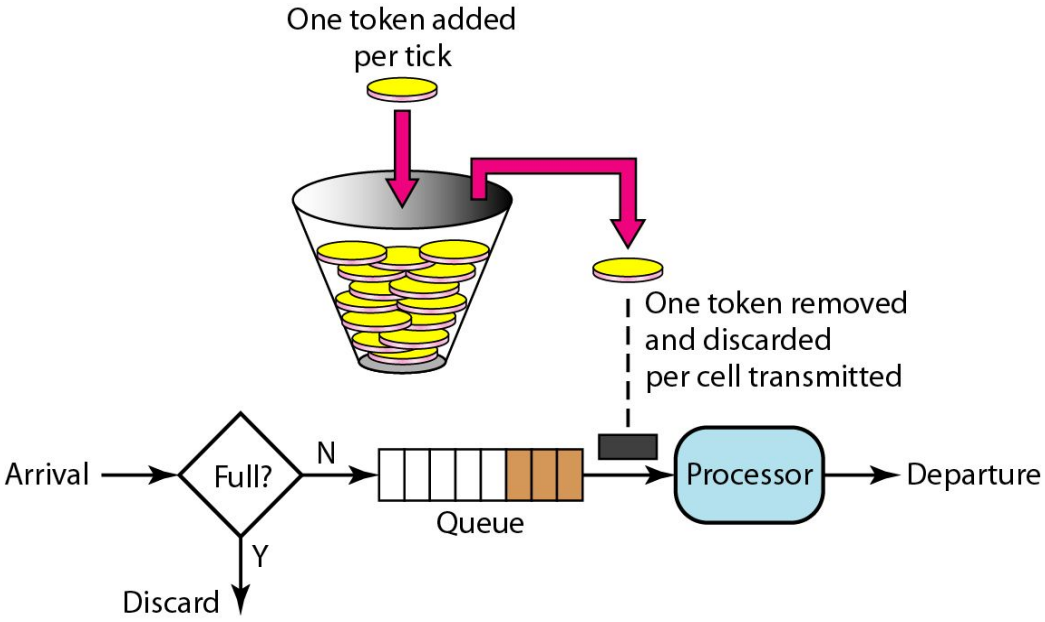
Leaky Bucket Implementation



- Algorithm for variable-length packets:
  1) Initialize a counter to n at the tick of the clock
  2) If n is greater than the size of the packet, send packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size
  3) Reset the counter and go to step 1

Token Bucket

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



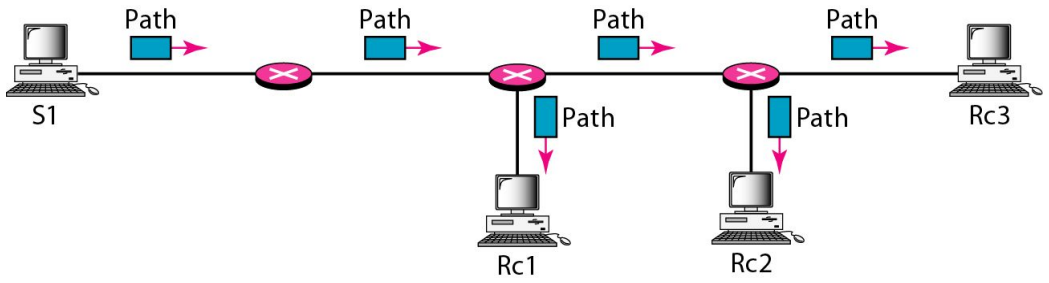
- Token bucket + leaky bucket: leaky bucket after token bucket

Integrated Services (IntServ)

- Integrated Services is a *flow-based* QoS model designed for IP
- Signaling: Resource Reservation Protocol (RSVP)
- Flow specification:
  - Rspec (resource specification) defines the resource that the flow needs to reserve
  - Tspec (traffic specification) defines the traffic characterization of the flow
- Admission: a router decides to admit or deny the flow specification
- Service classes: guaranteed service and controlled-load service
  - Guaranteed service class: guaranteed minimum end-to-end delay
  - Controlled-load service class: accept some delays, but is sensitive to an overloaded network and to the danger of losing packets

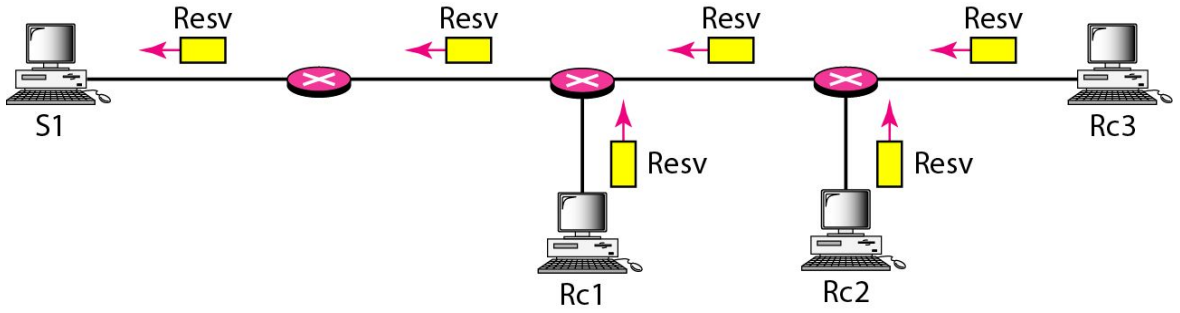
RSVP

- In IntServ, the resource reservation is for a flow, a kind of virtual circuit network out of the IP
- RSVP is a signaling protocol to help IP create a flow and consequently make a resource reservation
- RSVP is a signaling system designed for multicasting
- Receiver-based reservation
- RSVP message: **Path** and **Resv**
- **Path** message: from sender to all receivers

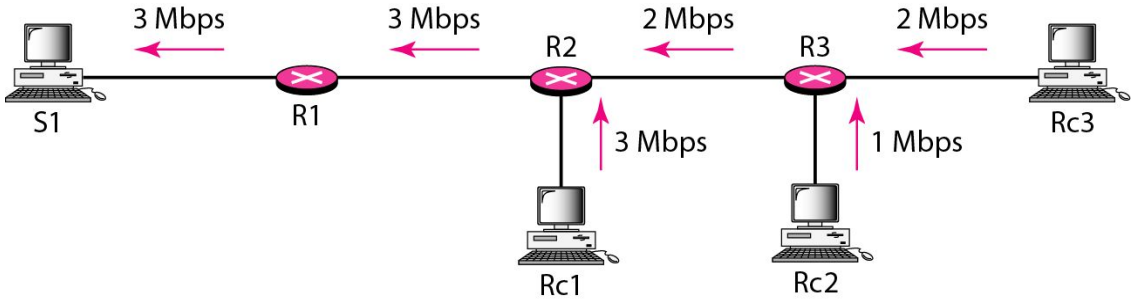


Resv Messages

- Make a resource reservation from each receiver to sender

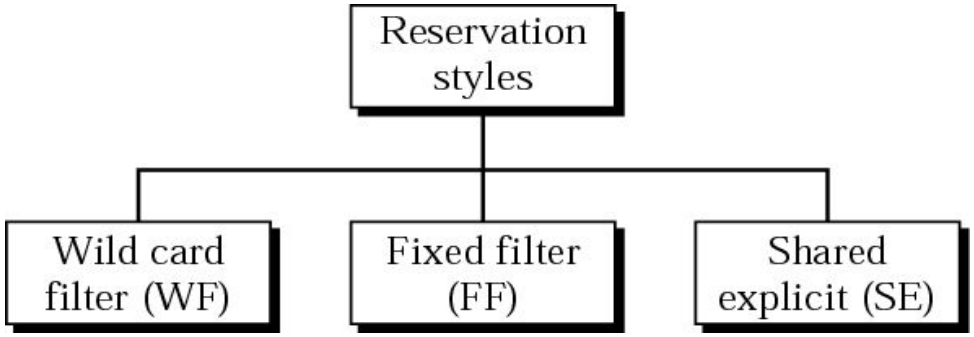


Reservation Merging



Reservation Styles

- Wild card filter style: a single reservation for all senders
- Fixed filter style: a distinct reservation for each flow
- Shared explicit style: a single reservation which can be shared by a set of flow



- Soft state instead of hard state (such as ATM, Frame Relay)
- Reservation information to be refreshed periodically
- IntServ problem: scalability and service-type limitation

Differentiated Service (Diffserv)

- Differentiated Services is a class-based QoS model designed for IP.
- Diffserv handles the shortcomings of IntServ
- Main differences between Diffserv and Intserv
  - Main processing is moved from the core to the edge (scalability)
  - The per-flow is changed to per-class flow service (service-type limitation)
- DS field
  - DSCP (DS Code Point) is a 6-bit field that define per-hop behavior (PHB)
  - CU (currently unused) is 2-bit

Per-hop Behavior (PHB)

- Diffserv defines three PHBs
- **DE PHB** (default PHB) is the same as best-effort delivery
- **EF PHB** (expedited forwarding PHB) provides the following services:
  - Low loss, low latency, ensured bandwidth
- **AF PHB** (assured forwarding PHB) delivers the packet with a high assurance as long as the class traffic does not exceed the traffic profile of the node

Traffic Conditioner

- **Meter** checks to see if the incoming flow matches the negotiated traffic profile
- **Marker** can re-mark a packet with best-effort delivery or down-mark a packet based on the meter information; no up-mark
- **Shaper** use the meter information to reshape the traffic if not compliant with the negotiated profile.
- **Dropper**, like a shaper with no buffer, discard packets if the flow severely violates the profile