

Lecture 22:

Buffering & Scheduling

CSE 123: Computer Networks
Stefan Savage





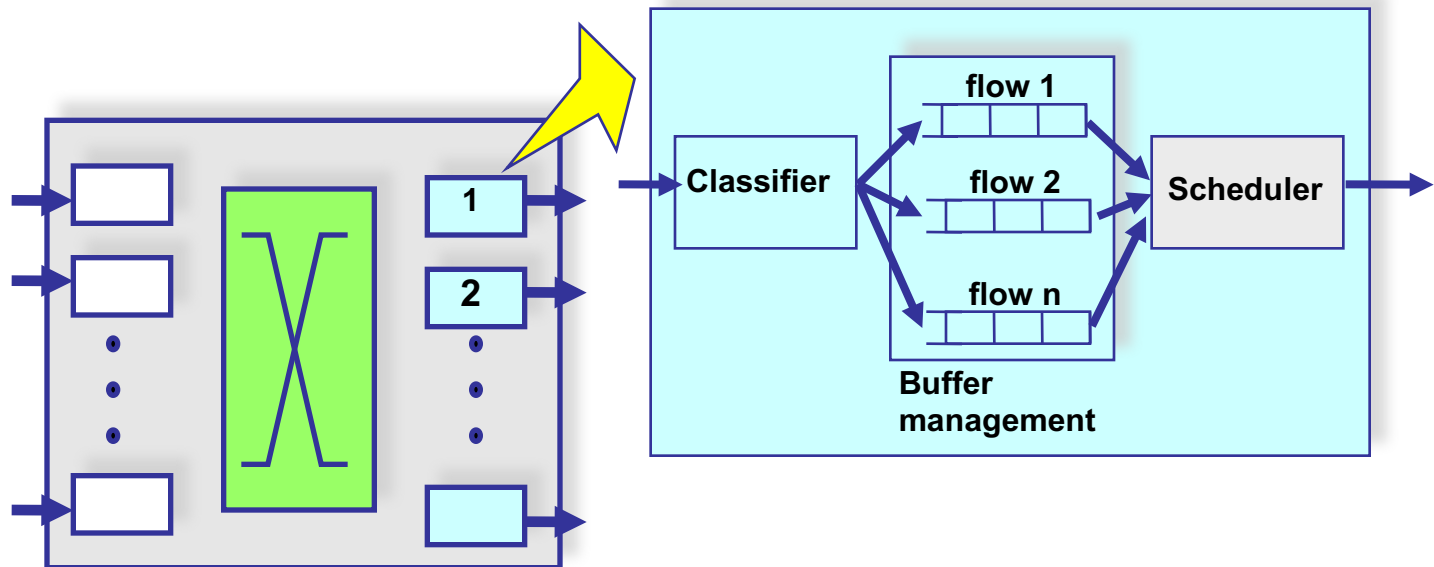
Lecture 22 Overview

- Buffer Management
 - ◆ FIFO
 - ◆ RED
- Traffic Policing/Scheduling



Key Router Challenges

- **Buffer management**: which packet to drop when?
 - ◆ We only have finite-length queues
- **Scheduling**: which packet to transmit next?





Basic Buffer Management

- FIFO + drop-tail
 - ◆ Simplest choice
 - ◆ Used widely in the Internet
- FIFO (first-in-first-out)
 - ◆ Implies single class of traffic
- Drop-tail
 - ◆ Arriving packets get dropped when queue is full regardless of flow or importance
- Important distinction:
 - ◆ FIFO: scheduling discipline
 - ◆ Drop-tail: drop policy



FIFO/Drop-Tail Problems

- Leaves responsibility of congestion control completely to the edges (e.g., TCP)
- Does not separate between different flows
- No policing: send more packets → get more service
- Synchronization: end hosts react to same events

Active Queue Management



- Design active router queue management to aid congestion control
- Why?
 - ◆ Router has unified view of queuing behavior
 - ◆ Routers see actual queue occupancy (distinguish queue delay and propagation delay)
 - ◆ Routers can decide on transient congestion, based on workload



Design Objectives

- Keep throughput high and delay low
 - ◆ High power (throughput/delay)
- Accommodate bursts
- Queue size should reflect ability to accept bursts rather than steady-state queuing
- Improve TCP performance with minimal hardware changes in router



Random Early Detection

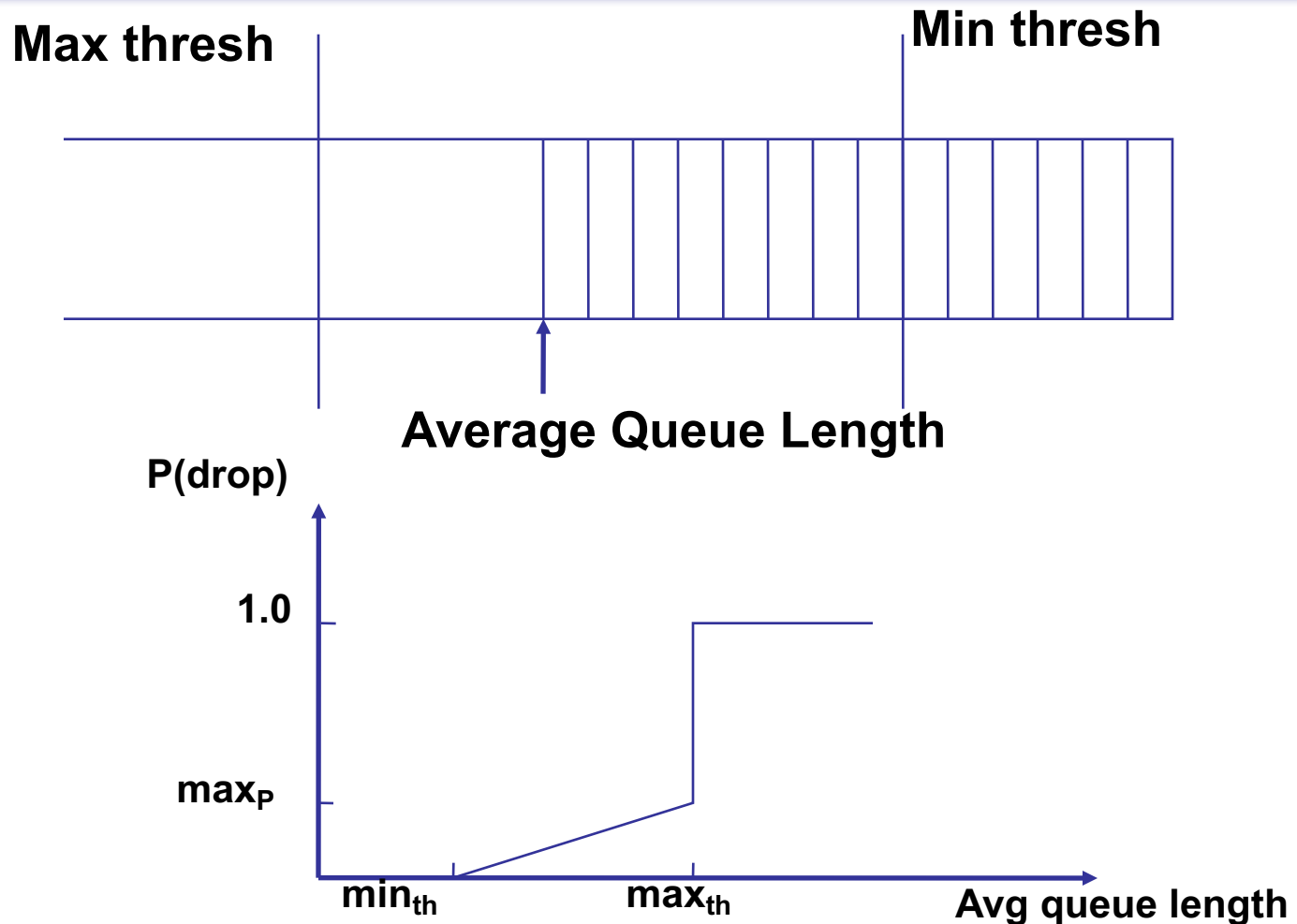
- Detect incipient congestion
- *Assume* hosts respond to lost packets
- Avoid window synchronization
 - ◆ Randomly mark packets
- Avoid bias against bursty traffic



RED Algorithm

- Maintain running average of queue length in router
- If $\text{avg} < \text{min}_{\text{th}}$ do nothing
 - ◆ Low queuing, send packets through
- If $\text{avg} > \text{max}_{\text{th}}$, drop packet
 - ◆ Protection from misbehaving sources
- Else drop/mark packet in a manner proportional to queue length
 - ◆ Notify sources of incipient congestion
 - ◆ Dropping vs Marking tradeoff (Explicit Congestion Notification)

RED Operation

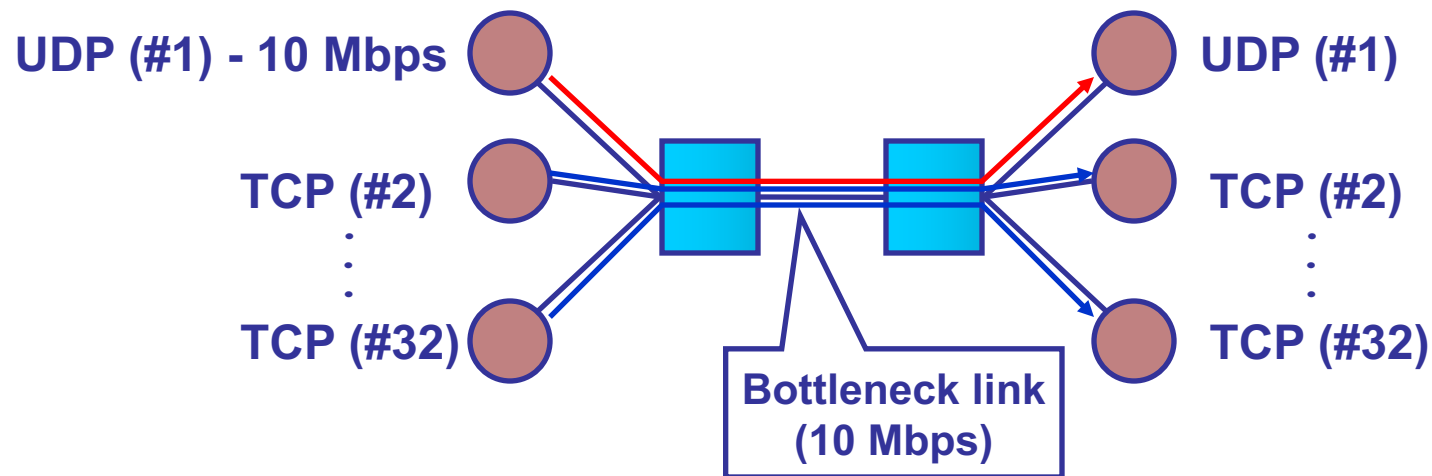


Problem:

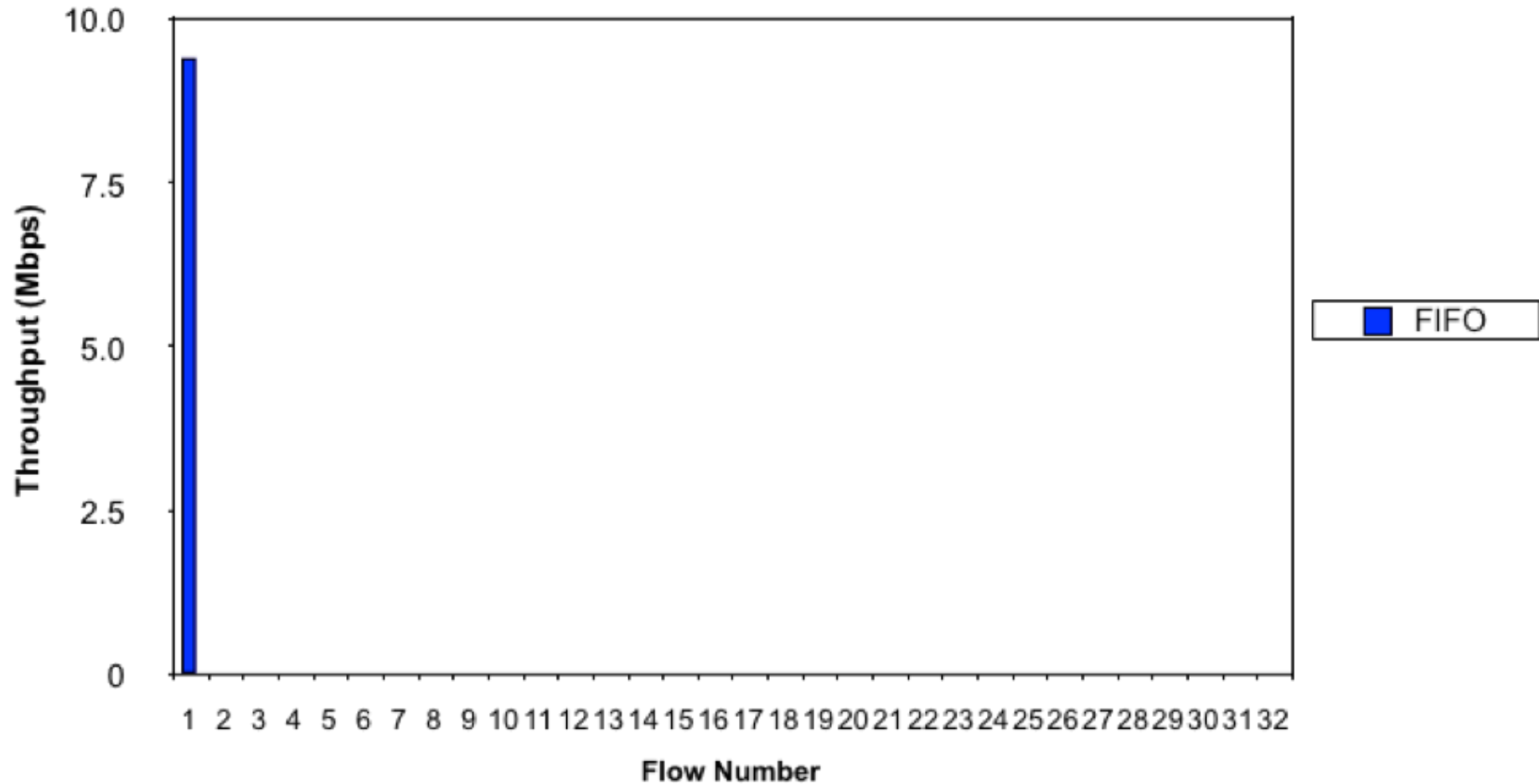
Non-responsive Senders



1 UDP (10 Mbps) and 31 TCPs sharing a 10 Mbps line



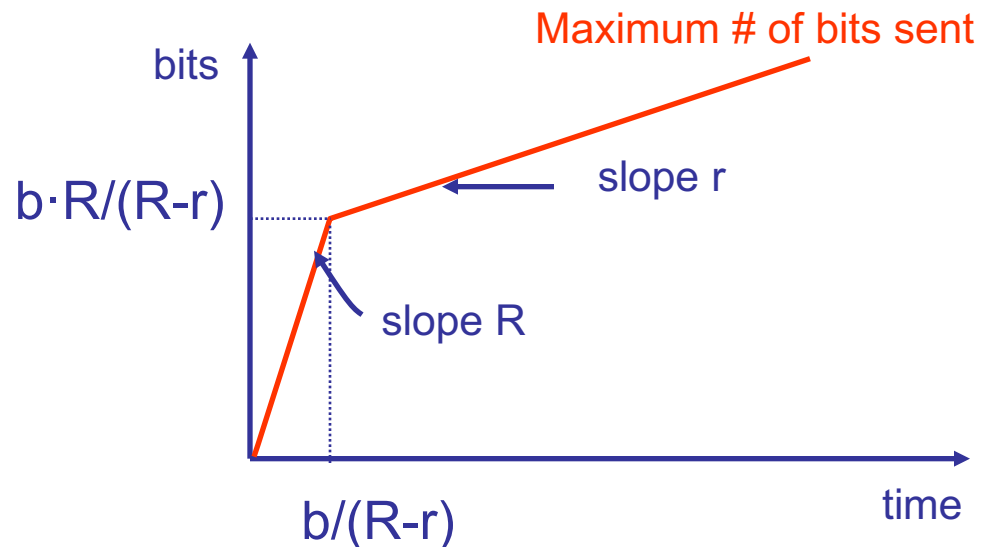
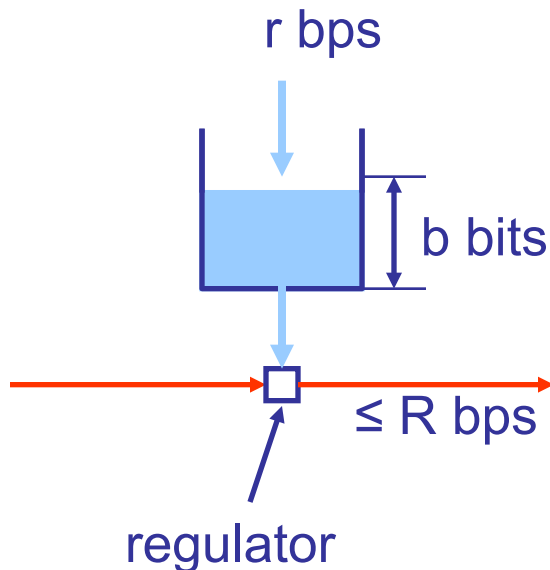
UDP vs. TCP





Token Bucket Basics

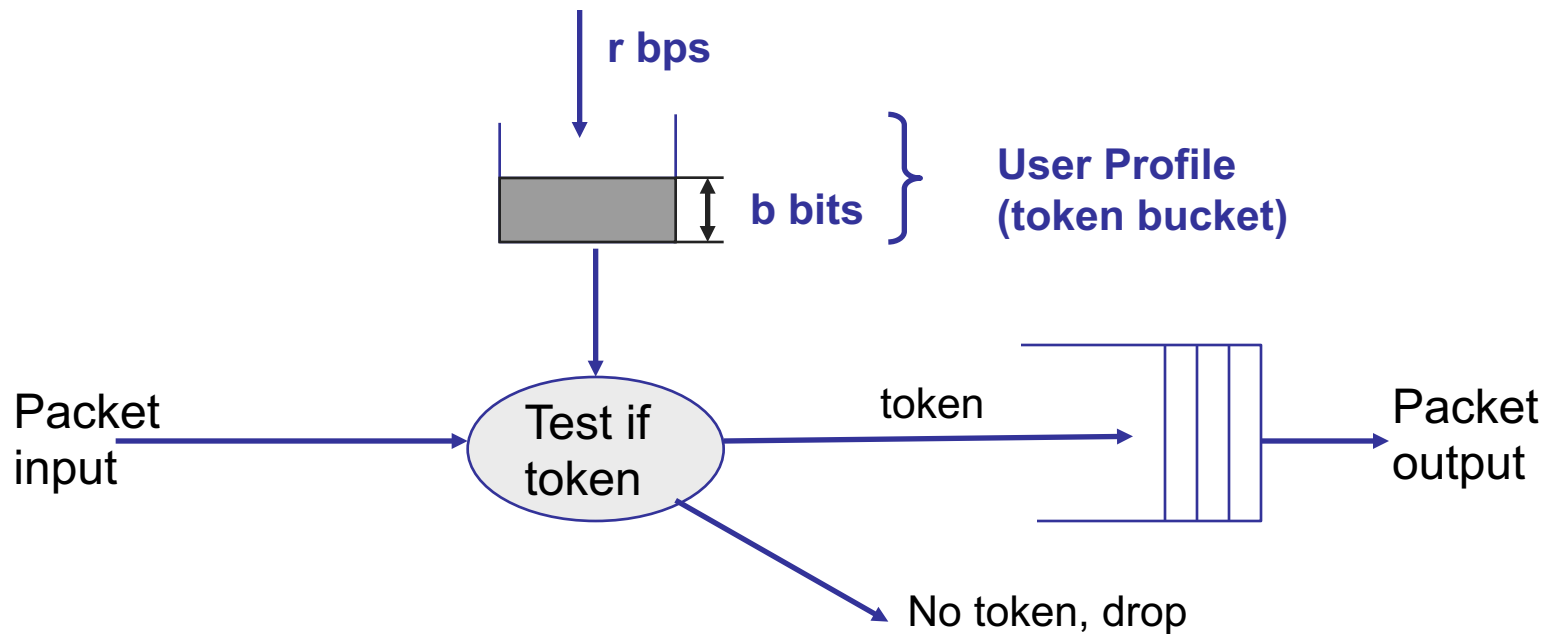
- Parameters
 - r – average rate, i.e., rate at which tokens fill the bucket
 - b – bucket depth (limits size of burst)
 - R – maximum link capacity or peak rate (optional parameter)
- A bit can be transmitted only when a token is available





Traffic Policing

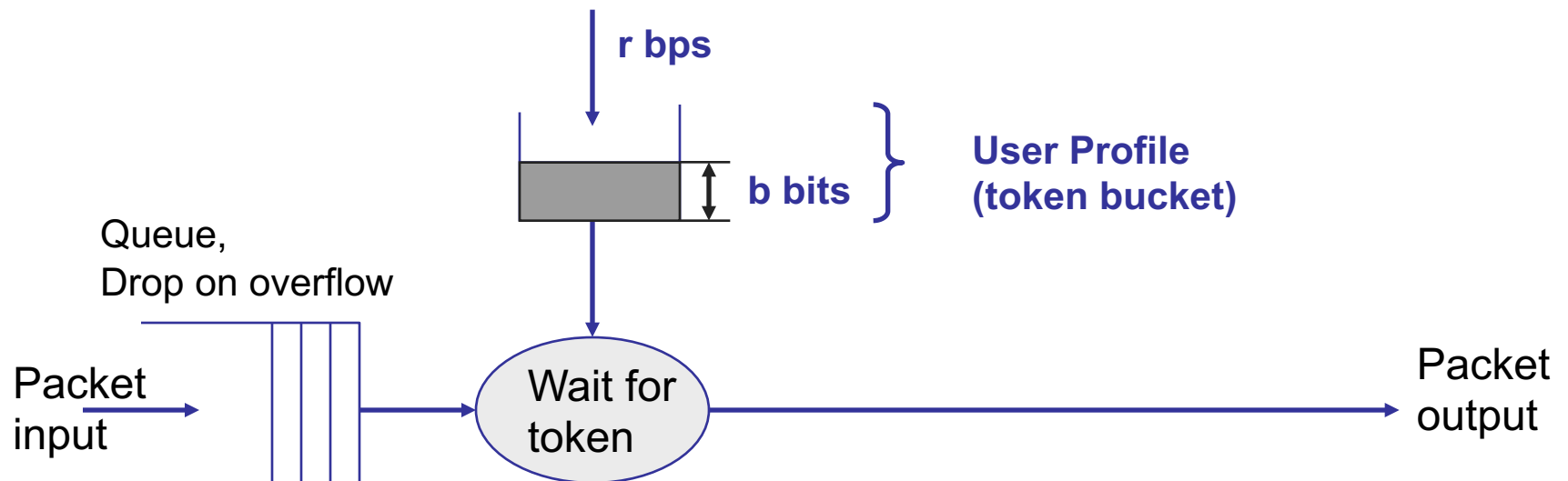
- Drop packets that don't meet **user profile**
- Output limited to average of r bps and bursts of b





Traffic Shaping

- Shape packets according to user profile
- Output limited to average of r bps and bursts of b

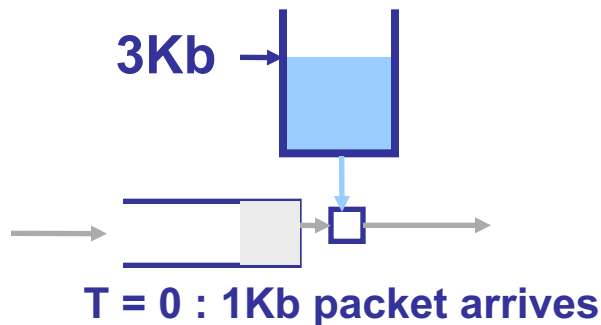




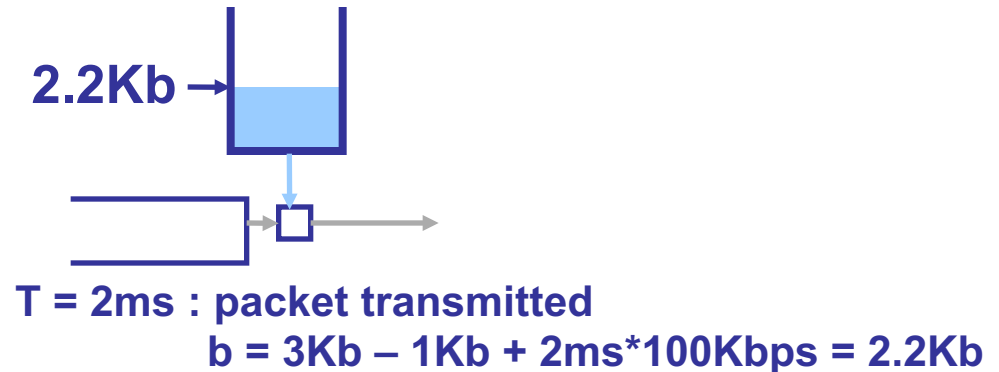
Shaping Example

- $r = 100 \text{ Kbps}$; $b = 3 \text{ Kb}$; $R = 500 \text{ Kbps}$

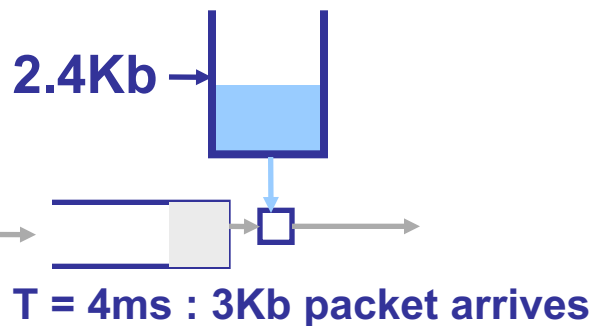
(a)



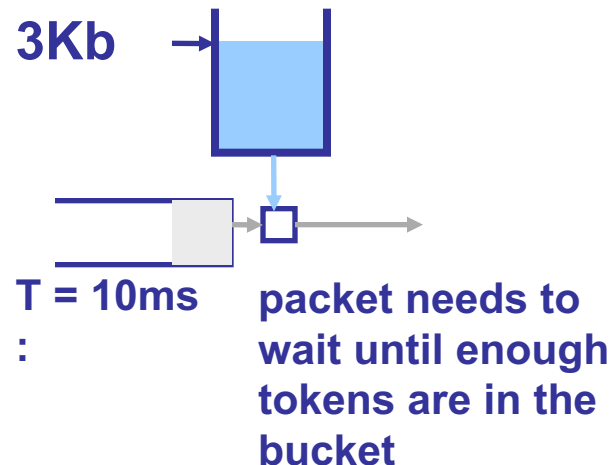
(b)



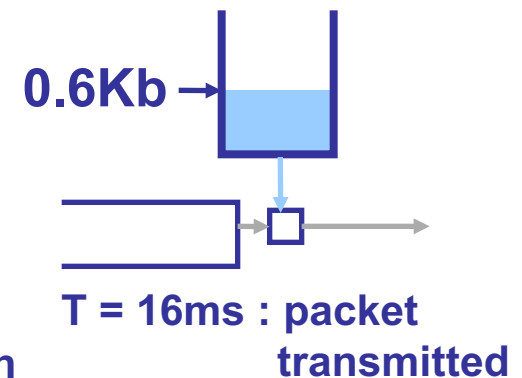
(c)



(d)



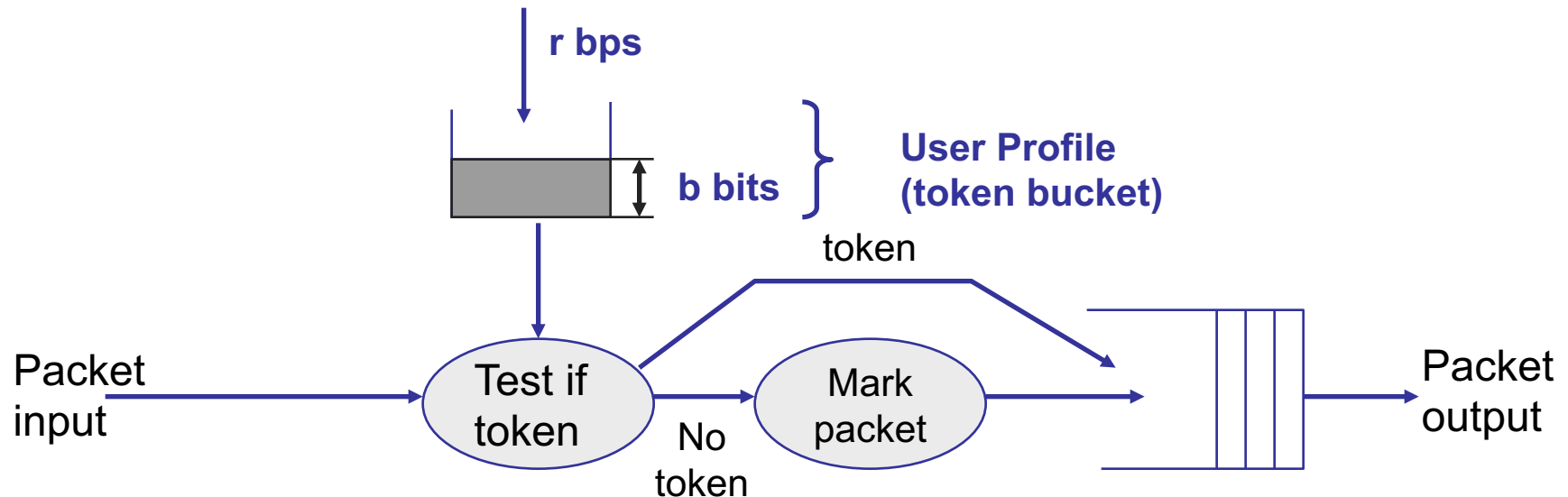
(e)



Using Token buckets for Buffer Management



- Mark packets that exceed user profile
- During congestion, drop marked packets first





For next time...

- HW #4 will be up later today (due on last day of class)
- No class rest of week (enjoy the break)
- Read Ch. 6.5 in P&D; finish Proj #2