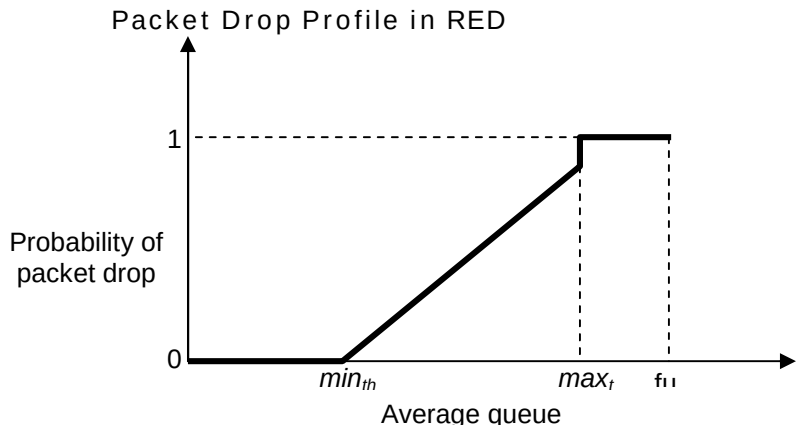
BUFFER MANAGEMENT : RANDOM EARLY DETECTION (RED)

- An approach to preventing unfair buffer hogging by detecting congestion when a buffer begins to reach certain level and it notifies the source to reduce the rate at which they send packets.
- Packets produced by TCP will reduce input rate in response to network congestion
- RED is a buffer management technique that attempts to provide equal access to FIFO system by randomly dropping arriving packets before the buffer overflows.
- A dropped packet provides feedback information to the source and informs the source to reduce its transmission rate.
- Early drop: discard packets before buffers are full
- Random drop causes some sources to reduce rate before others, causing gradual reduction in aggregate input rate.
- Min_{th} and Max_{th} are the two thresholds defined
- RED algorithm uses average queue length, when average queue length is below Min_{th} , RED does not drop any arriving packets.
- When average queue length is between Min_{th} and Max_{th}, RED drops an arriving packet with an increasing probability as the average queue length increases.
- Packet drop probability increases linearly with queue length
- RED improves performance of cooperating TCP sources.
- RED increases loss probability of misbehaving sources

Algorithm:

- Maintain running average of queue length
- If Qavg < minthreshold, do nothing
- If Qavg > maxthreshold, drop packet
- If in between, drop packet according to probability
- Flows that send more packets are more likely to have packets dropped



Traffic Management at the Flow Level

- Management of individual traffic flows & resource allocation to ensure delivery of QoS(e.g. Delay, jitter, loss)
- Traffic management at flow level operates on the order of milliseconds to seconds.
- It is concerned with managing the individual traffic flow to ensure the QoS (e.g. delay, jitter, loss) requested by user is satisfied.
- The purpose of Traffic Management at the Flow Level is to control the flows of traffic and maintain performance even in presence of traffic overload.
- The process of managing the traffic flow in order to control congestion is called congestion control.
- Congestion occurs when a surge of traffic overloads network resources

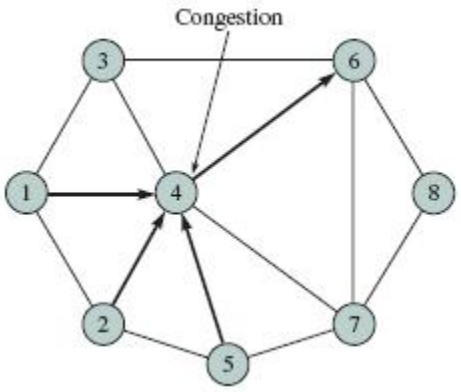


FIGURE 7.50 A congested switch

Approaches to Congestion Control:

- Preventive Approaches: Scheduling & Reservations
- Reactive Approaches: Detect & Throttle/Discard

Ideal effect of congestion control:
Resources used efficiently up to capacity available

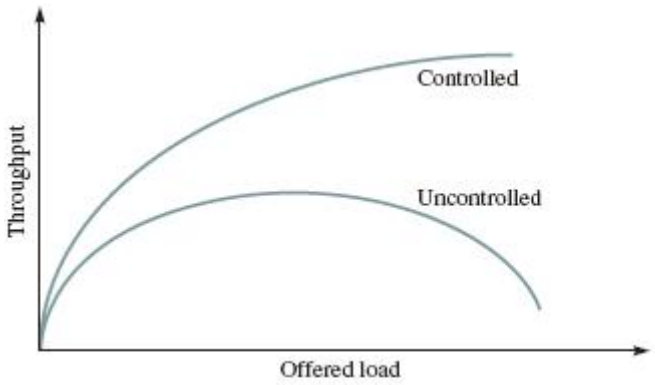


FIGURE 7.51 Throughput drops when congestion occurs

Open-loop control and closed-loop control are the two logical approaches of congestion control.

Open-Loop Control

- It prevents congestion from occurring.
- It does not depend on feedback information to react to congestion.
- Network performance is guaranteed to all traffic flows that have been admitted into the network
- It depends on three Key Mechanisms and they are:-
  - Admission Control
  - Policing
  - Traffic Shaping

Admission Control

- It is a network function that computes the resource (bandwidth and buffers) requirements of new flow and determines whether the resources along the path to be followed are available or not available.
- Before sending packet the source must obtain permission from admission control.
- Admission control decides whether to accept the flow or not.
- Flow is accepted, if the QoS of new flow does not violate QoS of existing flows
- QoS can be expressed in terms of maximum delay, loss probability, delay variance, or other performance measures.
- QoS requirements:
  - Peak, Avg., Min Bit rate
  - Maximum burst size
  - Delay, Loss requirement
- Network computes resources needed
  - "Effective" bandwidth
- If flow accepted, network allocates resources to ensure QoS delivered as long as source conforms to contract

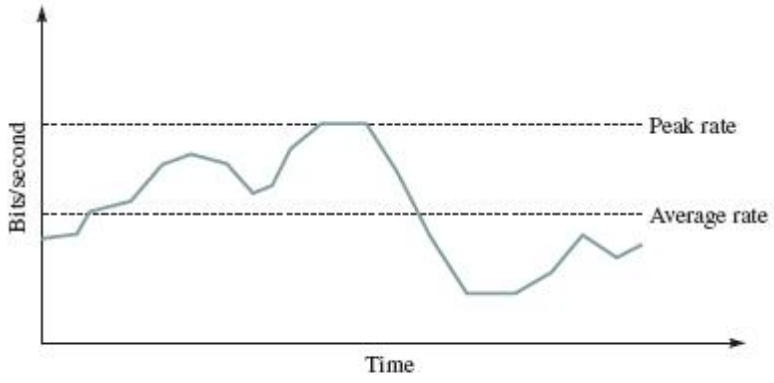


FIGURE 7.52 Example of a traffic flow

Source : http://elearningatria.files.wordpress.com/2013/10/unit2.pdf