Computer Networks

Wenzhong Li
Nanjing University
Fall 2014

Chapter 6.
Congestion Control and QoS

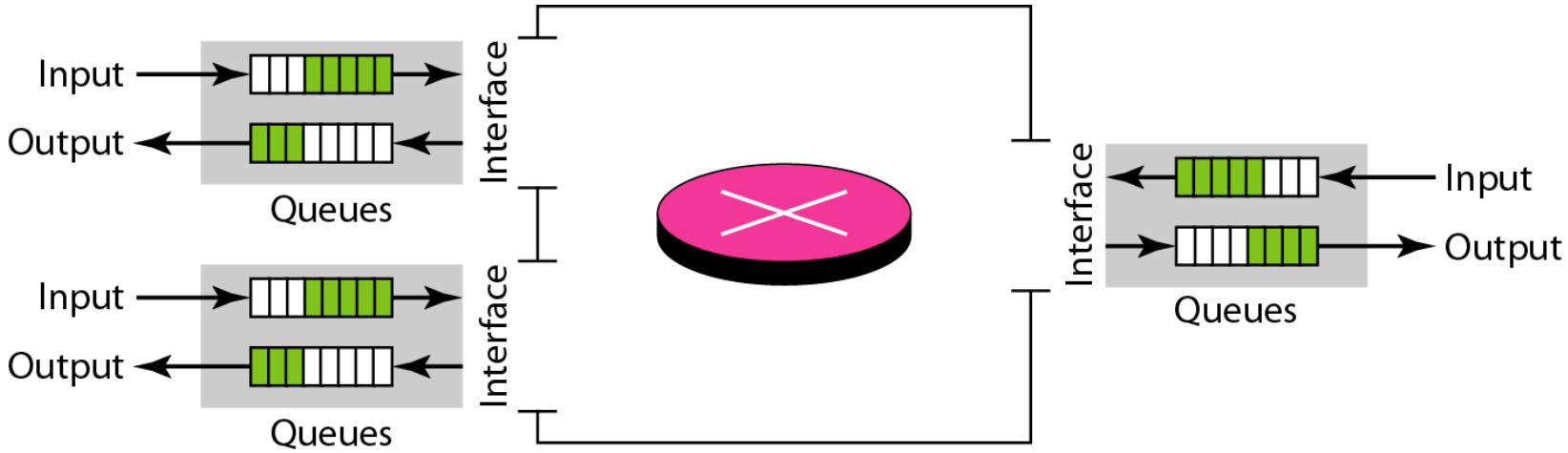
- Network Congestion
- Congestion Control in FR
- Traffic Management in ATM
- Internet QoS
- Resource Allocation and RSVP
- Differentiated Services

Network Congestion

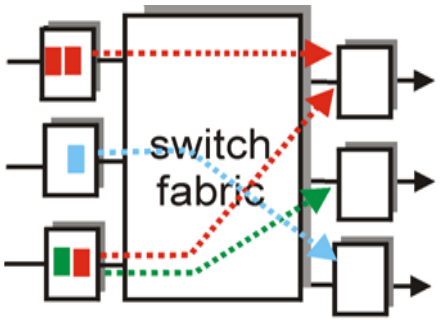
- Congestion
  - Number of packets transmitted through the network approaches the packet handling capacity of the network
- One or more switches/routers becomes overloaded
  - Generally 80% utilization is critical
- Congestion control
  - Keep number of packets below level at which performance falls off dramatically

Queues at a Switch

- Switch overloads because receiving packets faster than it can forward

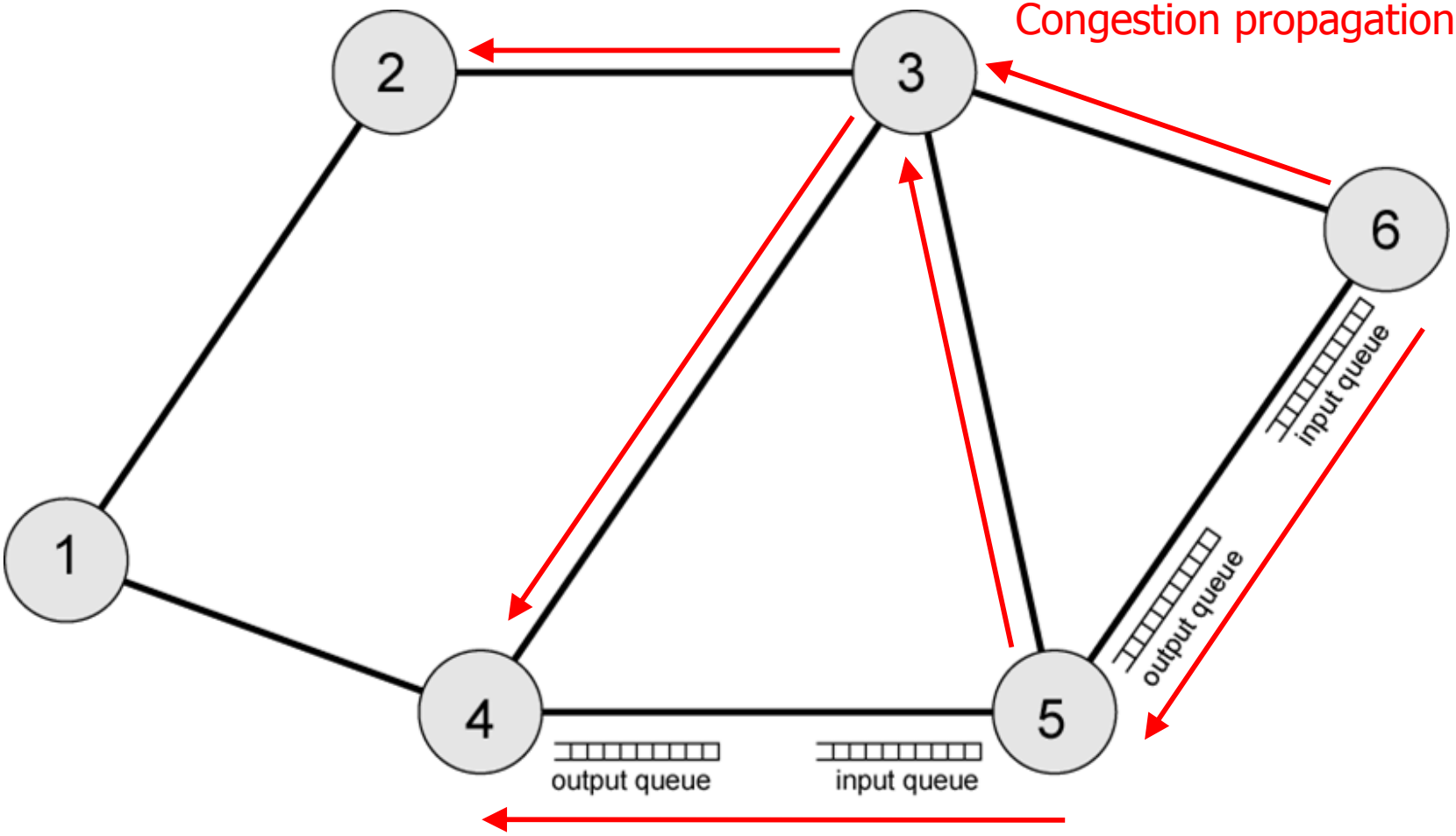


Causing Congestion



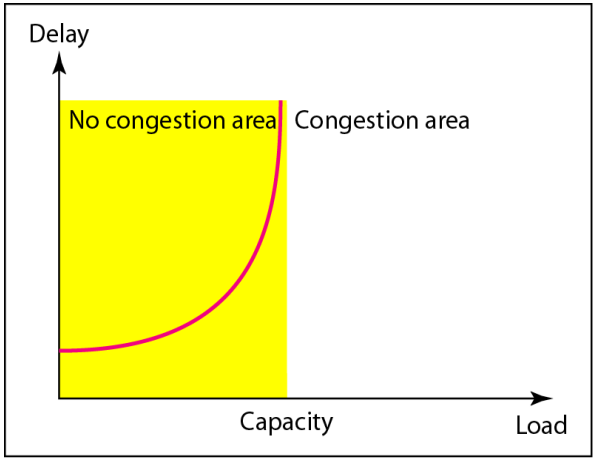
- Congestion at switch
  - Bursty traffic / poor topology
  - Packet arrival rate exceeds the outgoing link capacity
  - Packet processing rate < packet arriving rate
  - Insufficient memory to store arriving packets
- Effects caused at congested switch
  - Discard queued packets to make room for new comings
  - Prevent additional packets from entering the congested port (link-layer flow control)

Interaction of Queues

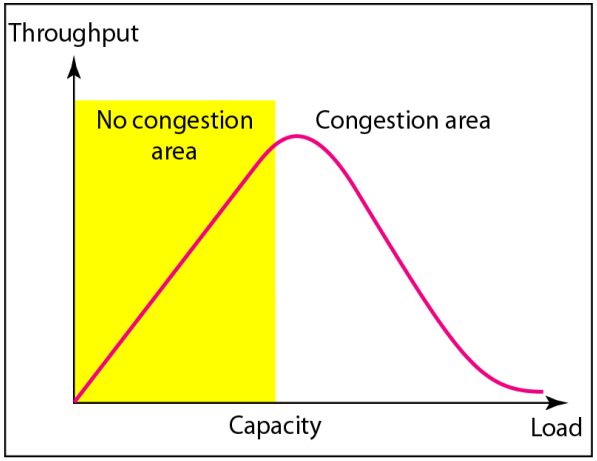


Network Utilization

- Delay and Throughput vs. Network Load



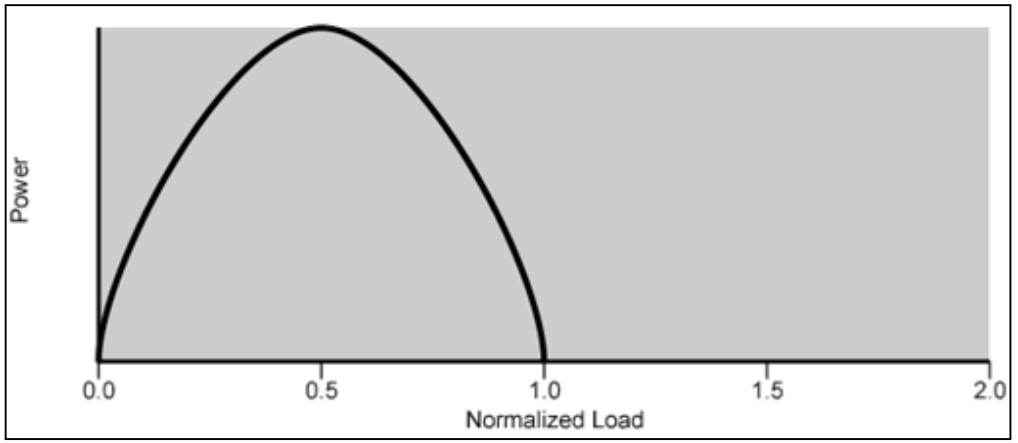
a. Delay as a function of load



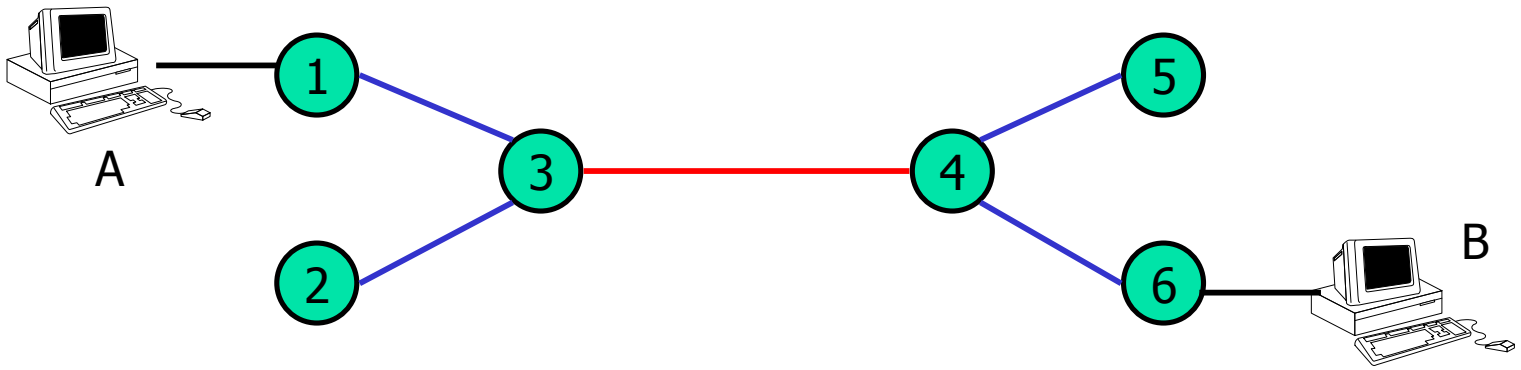
b. Throughput as a function of load

- Communication Power

$$Power = Throughput / Delay$$

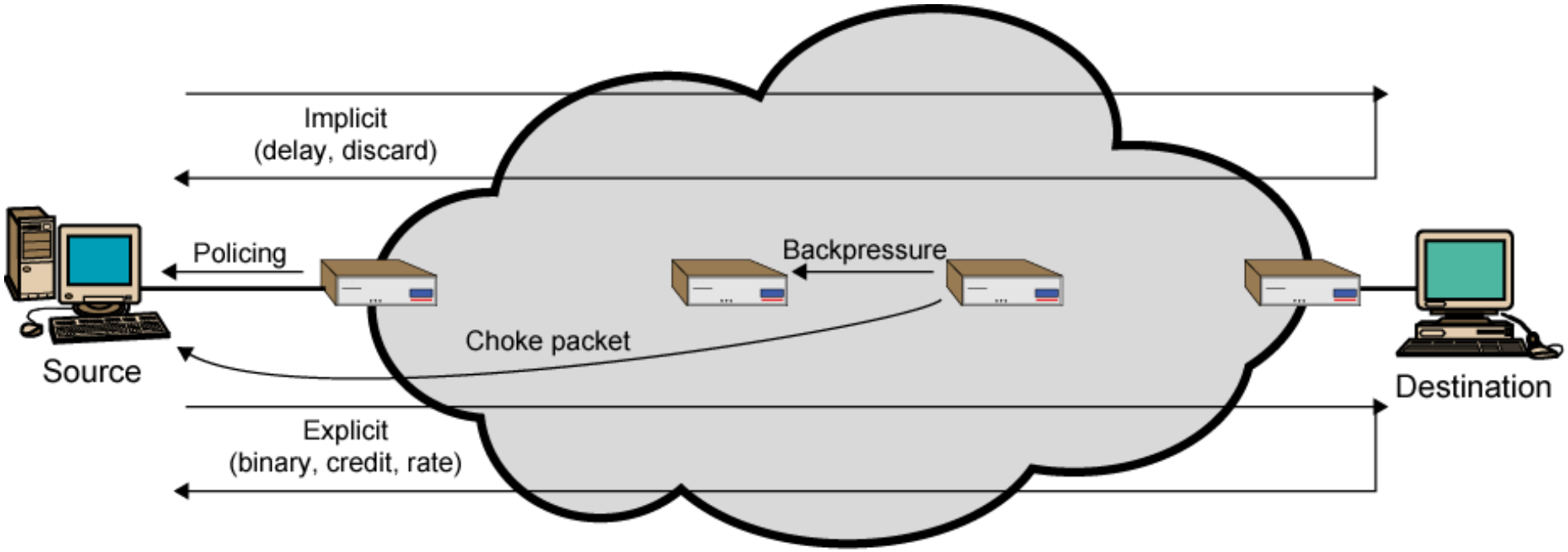


Bottleneck Effect



- Assume all the links have similar capacity, and run in full for both direction
- Then switches 3 and 4 will be in congestion

Mechanisms for Congestion Control



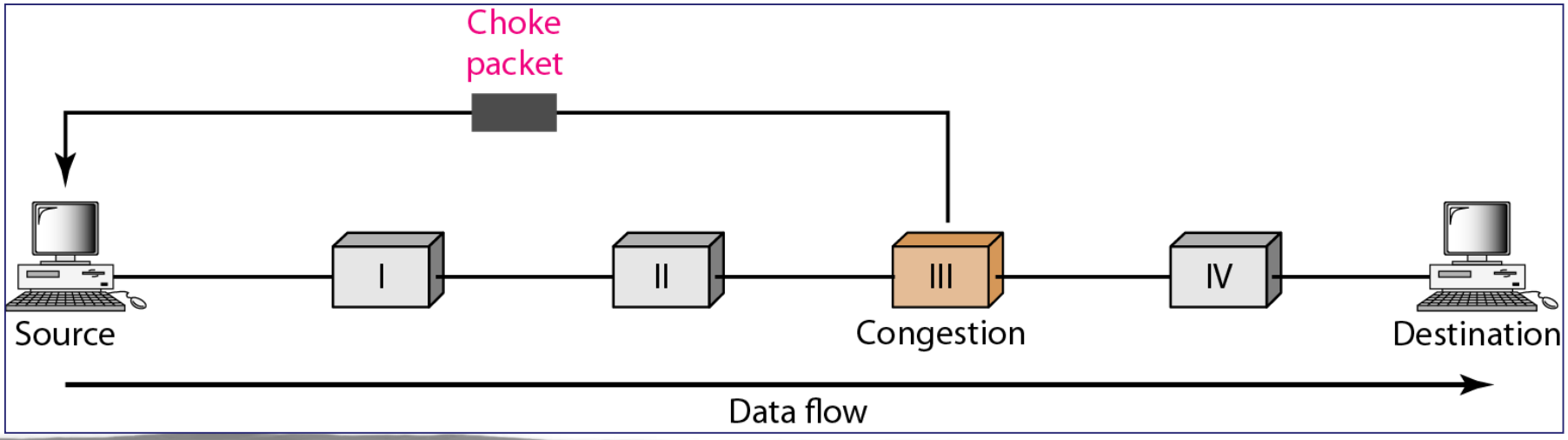
Possible Mechanisms

- Choke Packet
- Backpressure
- Warning bit
- Congestion window
- Random early discard
- Traffic shaping

- 抑制分组
- 反压
- 警告位
- 拥塞窗口
- 随机早期丢弃
- 流量整形

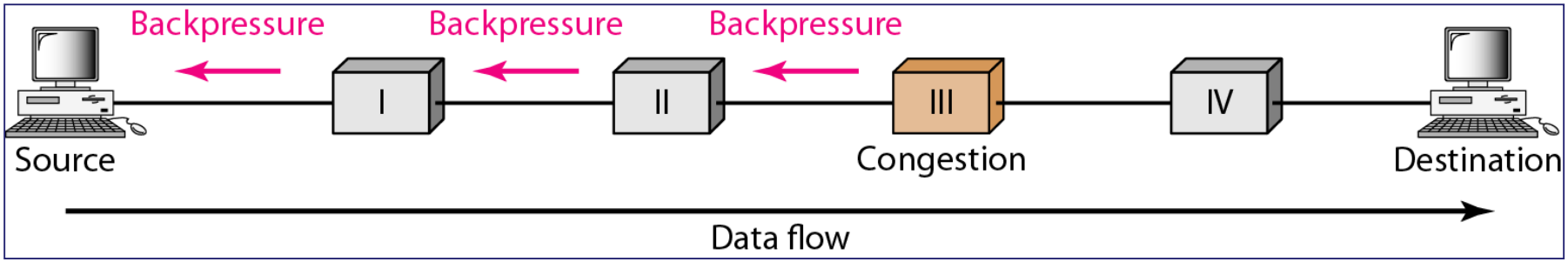
(1) Choke Packet

- Control packet
  - Generated at congested node
  - Sent to source node
- ICMP source quench
  - From router or destination, sent for every discarded packet



(2) Backpressure

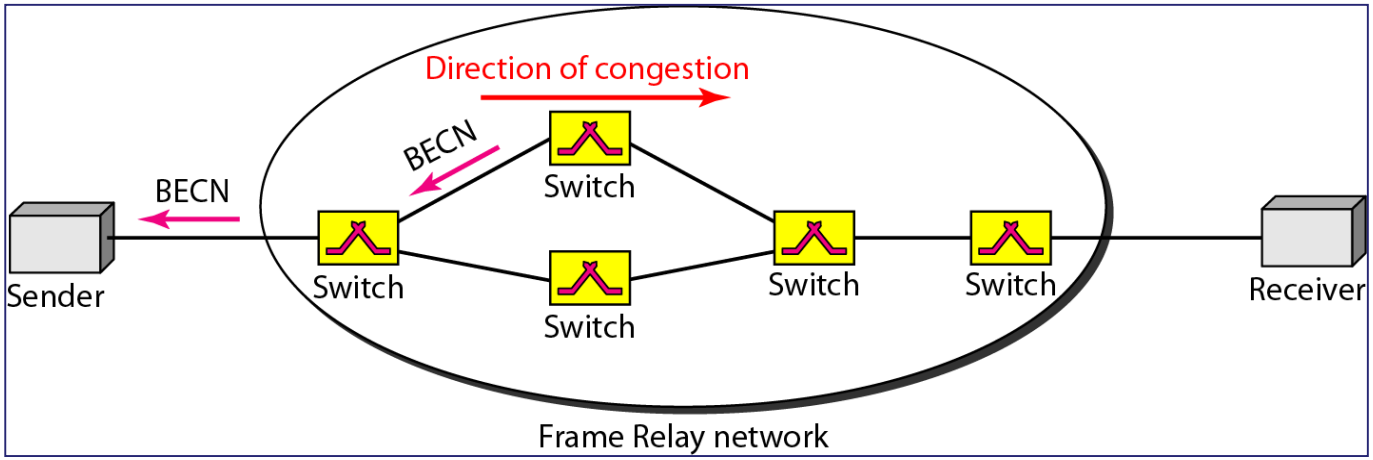
- Hop-by-Hop Choke Packets
  - Propagation time > transmission time (long distance or high speed link)
  - Choke packets from router to source are not effective
  - Require each hop to reduce its transmission

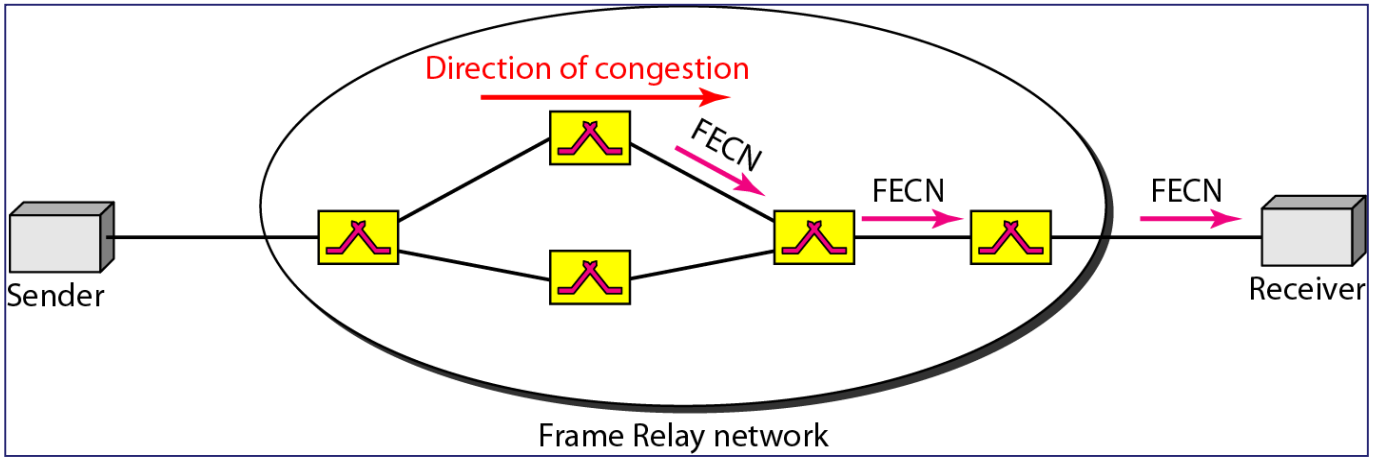


(3) Warning Bit

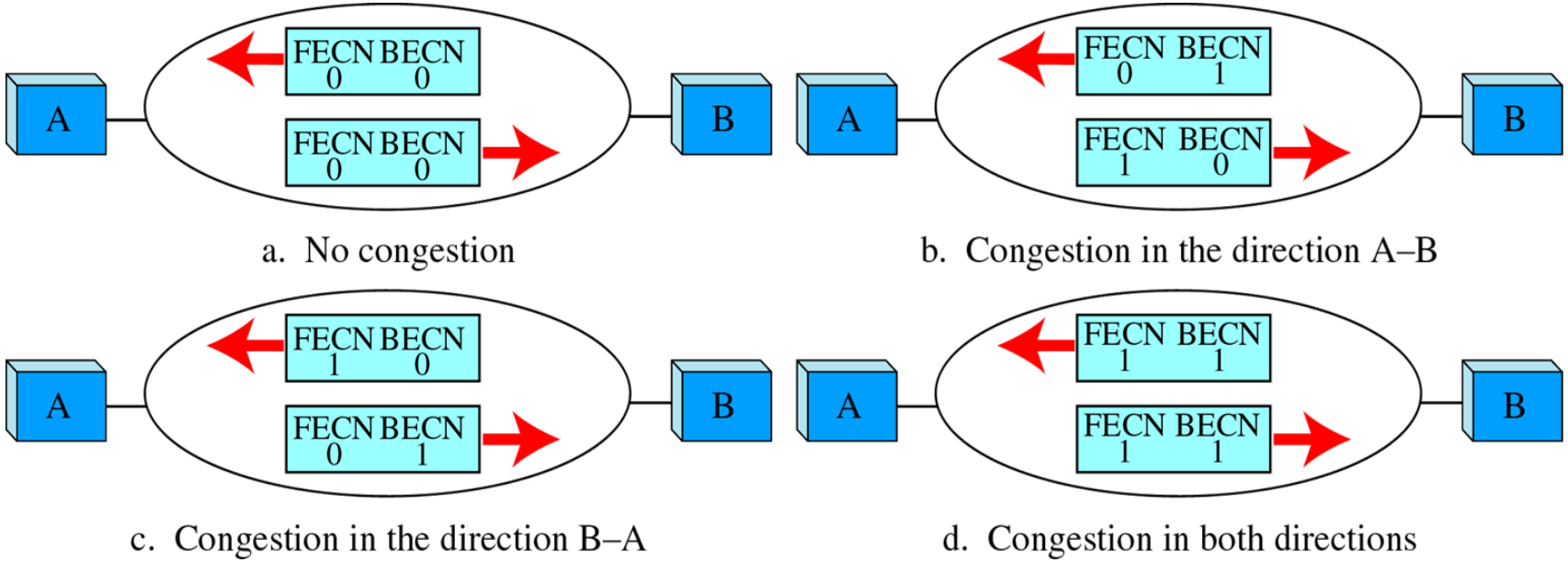
- Special bits set in the packet header by switches
  - Alerts end systems of increasing congestion
  - End systems take steps to reduce offered load
- Backwards
  - Congestion avoidance in opposite direction to congested packet
  - Assume congestion will burst up quickly
- Forwards
  - Congestion avoidance in same direction as congested packet
  - Assume congestion will cumulate slowly

BECN and FECN in FR



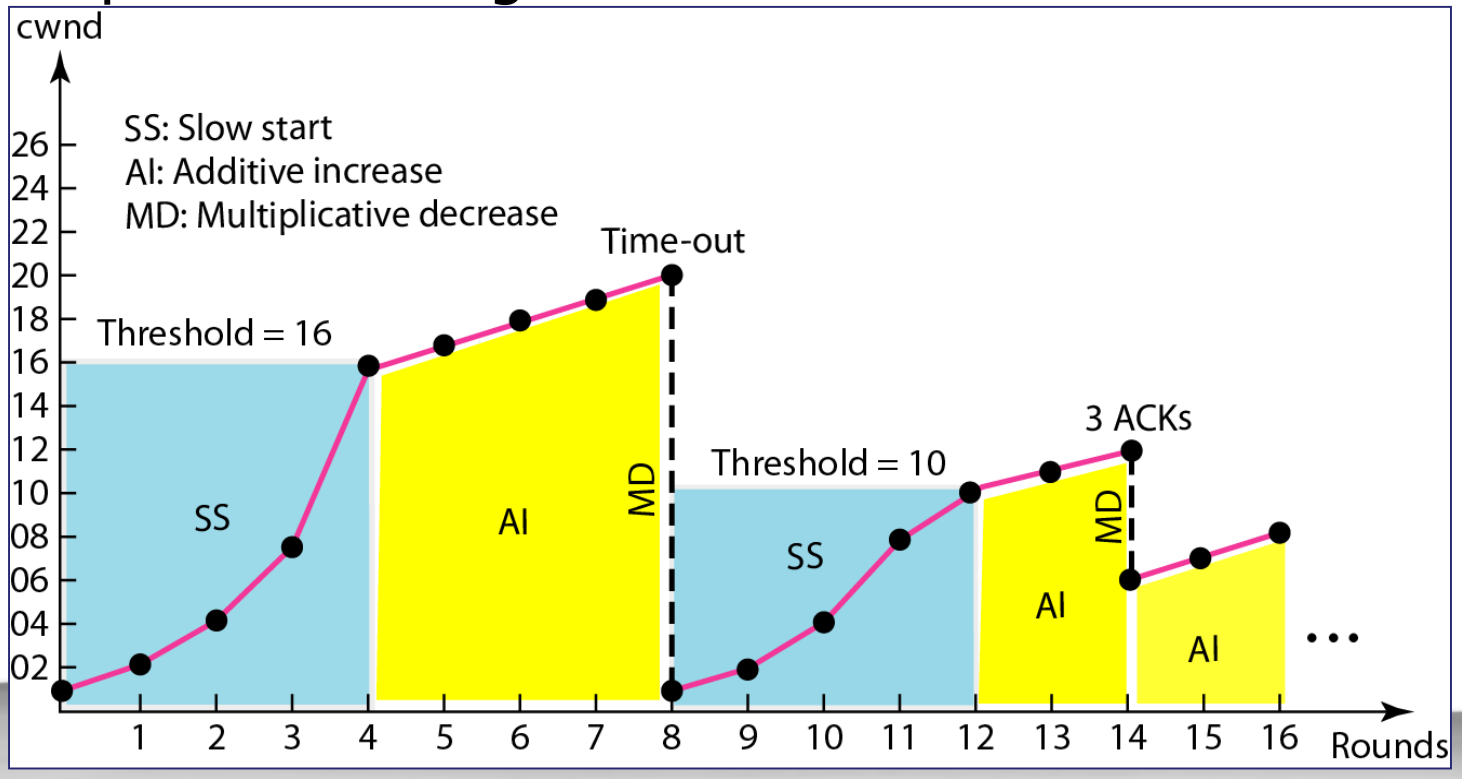


Four Cases of Congestion



(4) Congestion Window

- Control congestion at hosts
  - Packet timeout as a signal of network congestion
  - Dynamic send window management (as in TCP) to hold the packet sending



(5) Random Early Discard

- Control congestion at routers (switches)
  - Combined with congestion window at hosts
- Internet (TCP) global synchronization problem
  - Traffic burst fills queues so packets lost, TCP connections enter slow start
  - Traffic drops so network under utilized, connections leave slow start at same time causing burst again
- Handle the problem – RED
  - Router randomly discards packets before buffer becomes completely full

The RED Algorithm

- Compute average queue length

$$avgLen = (1-\omega)\times avgLen + \omega \times sampleLen$$

Calculate average queue size *avgLen*

if *avgLen* < TH_{min}

queue packet

else if $TH_{min} \le$ *avgLen* < TH_{max}

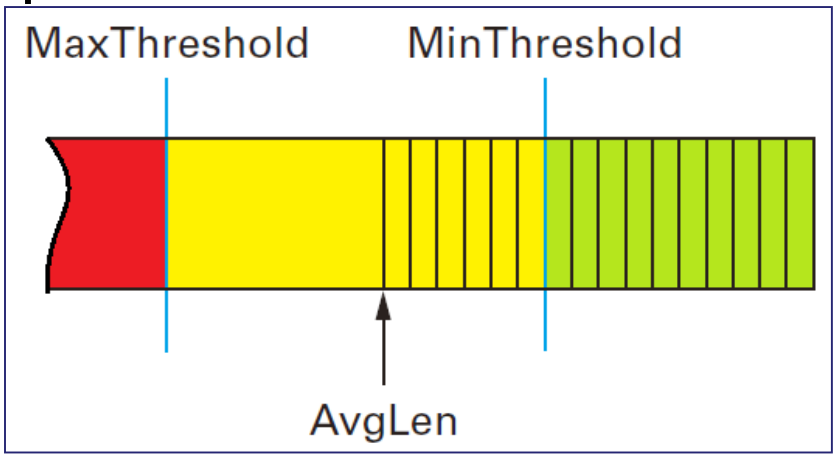
calculate probability p

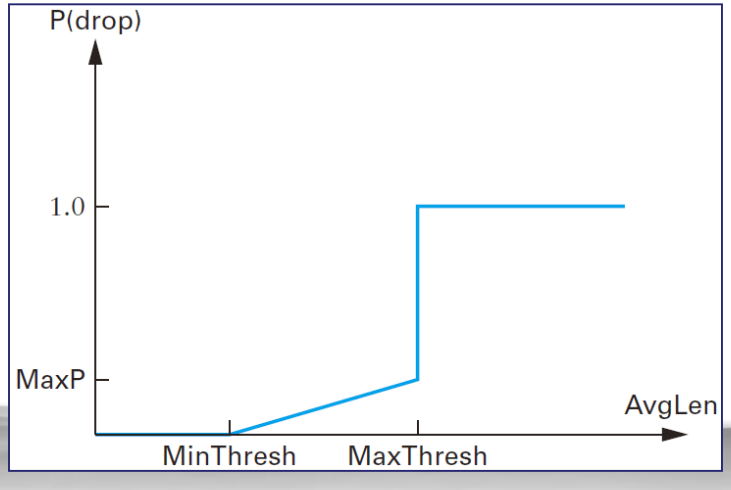
with probability p discard packet

else with probability 1-p queue packet

else if *avg* ≥ TH_{max}

discard packet



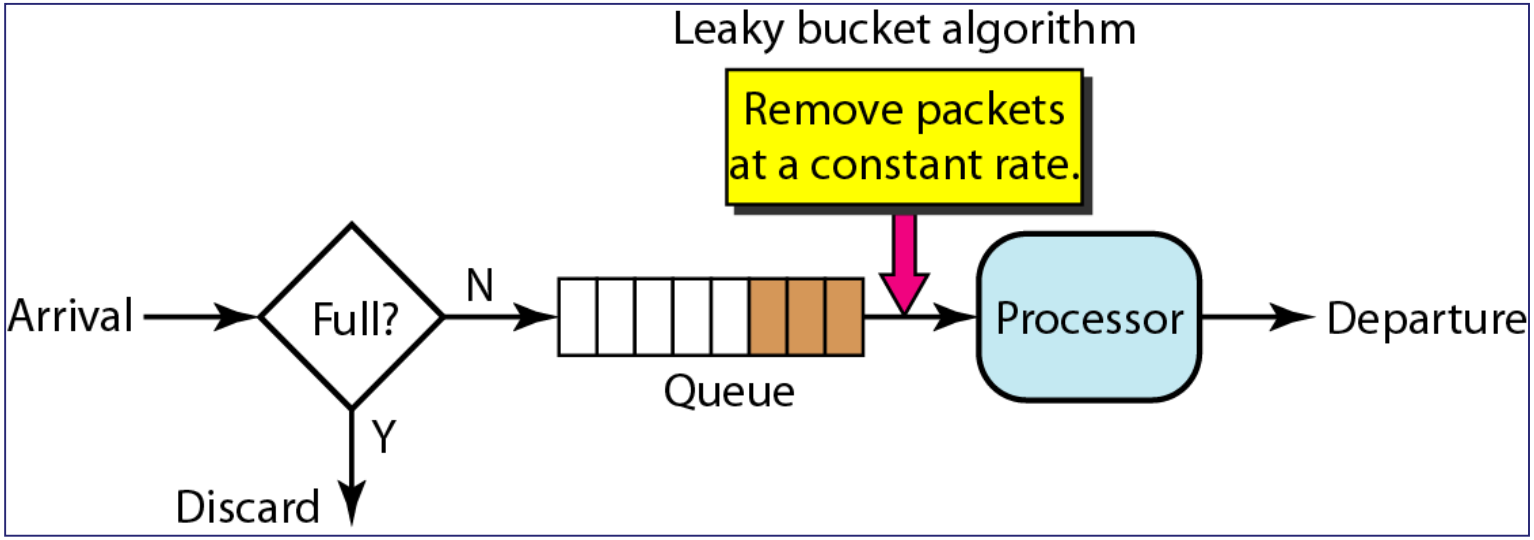


(6) Traffic Shaping

- Shape the traffic (packet flow) before it enters the network
  - Control the rate at which packets are sent
  - At connection set-up, host and end switch negotiate a traffic pattern (shape)
- Two traffic shaping algorithms
  - Leaky Bucket
  - Token Bucket

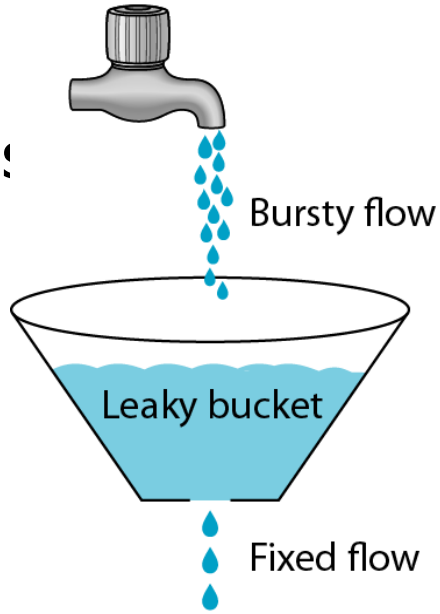
Leaky Bucket

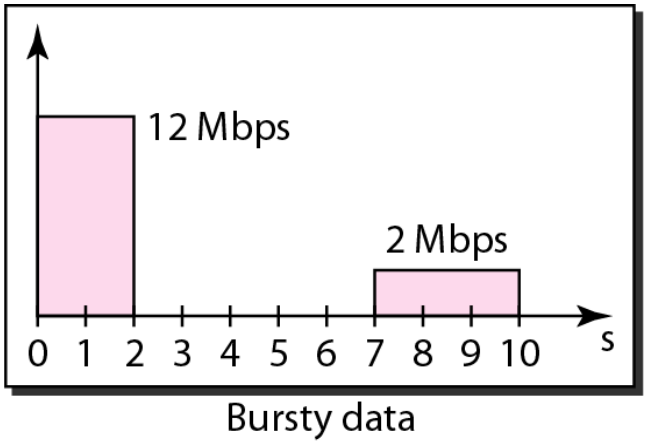
- Shape bursty traffic into fixed-rate traffic by averaging the data rate
- May drop the packets if the bucket is full



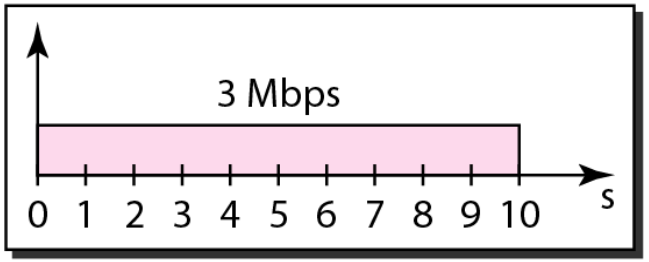
Leaky Bucket

- Do nothing when input is idle
- Packet output rate is fixed





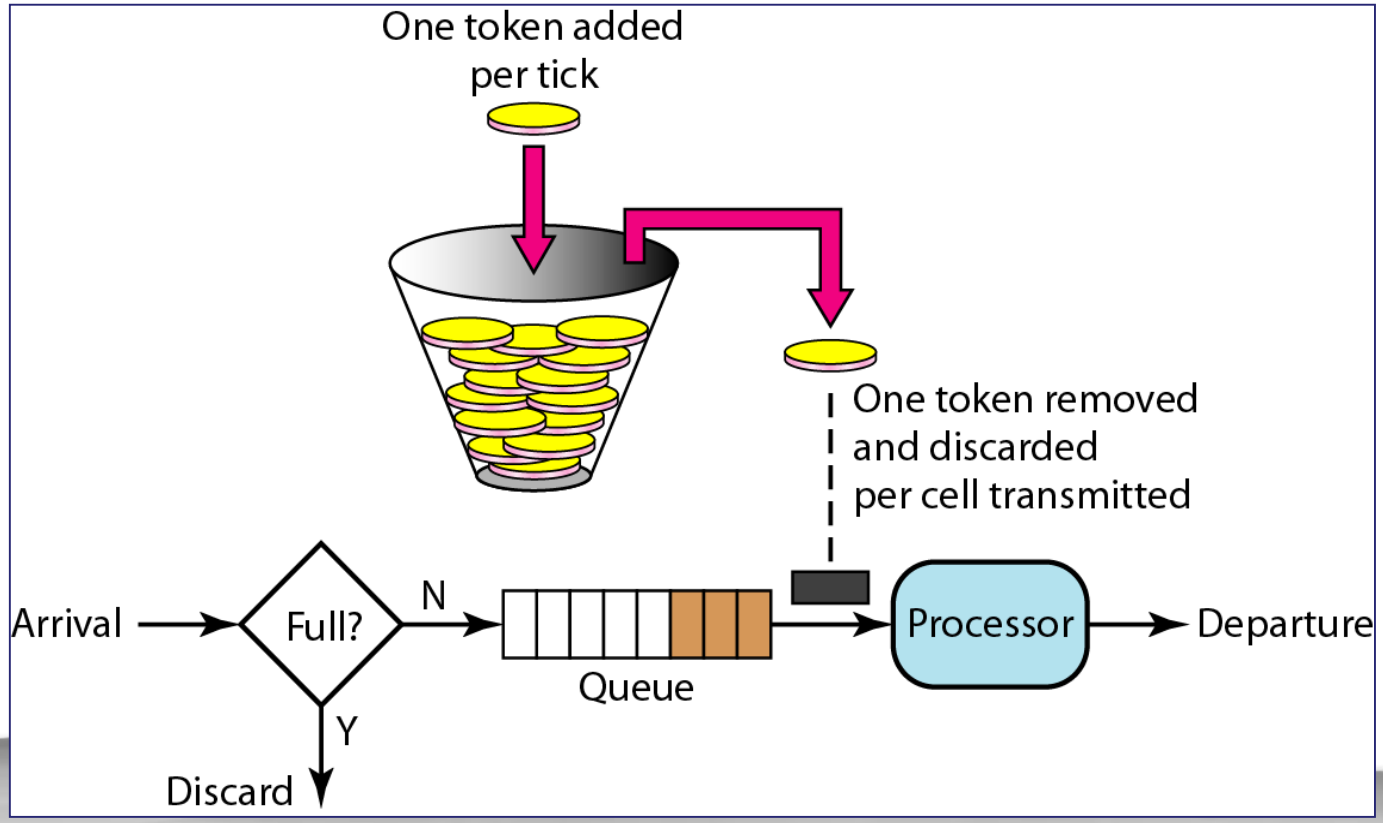
Bursty data



Fixed-rate data

Token Bucket

- Use token to control the output traffic, allowing vary output rate
- Token generation rate is fixed, may drop token (not packet) when bucket full

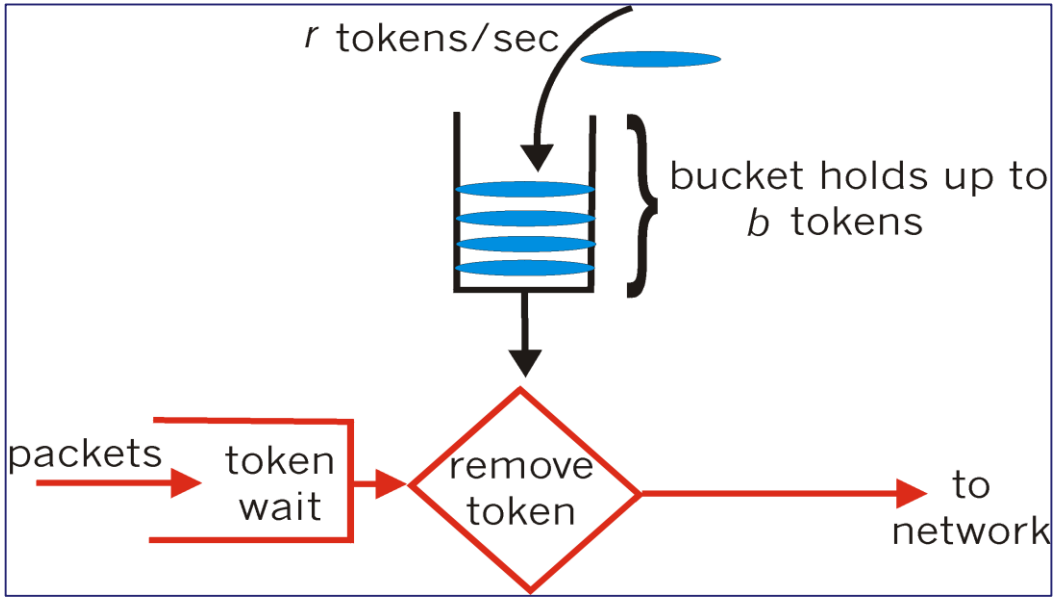


Token Bucket

- Token bucket is more powerful in traffic shaping

3 metrics defined

- Average traffic rate
- Burst traffic rate
- Maximum burst size



Summary

- Mechanisms for Network Congestion Control
  - Choke packet
  - Backpressure
  - Warning bit
  - Congestion window
  - Random early discard
  - Traffic shaping

Appendix

Congestion Control in FR & ATM

Congestion Control in FR

- Explicit signaling use warning bits in packet
  - Backward/Forward explicit congestion notification
- Traffic Rate Management
  - Define Committed information rate (CIR)
  - Congestion avoidance
  - Discard strategy

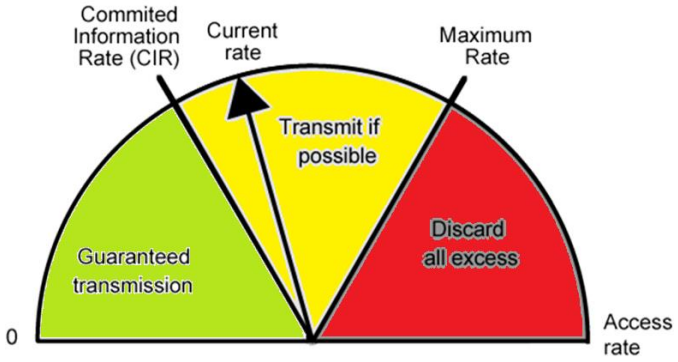
Committed information Rate

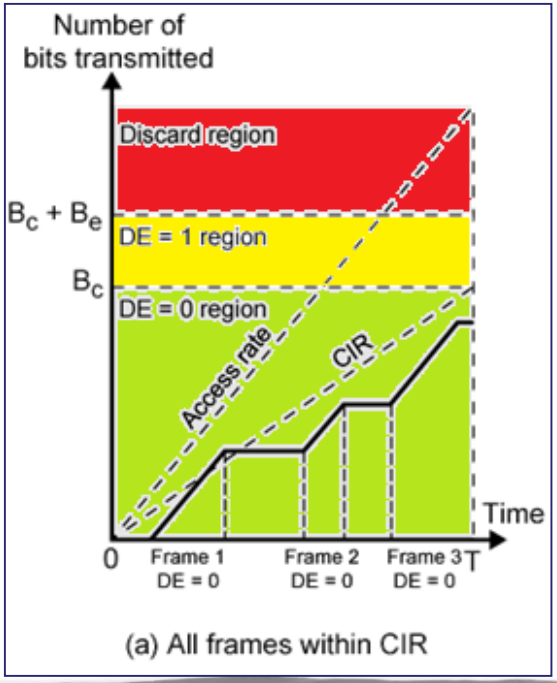
- Average bandwidth (throughput) guaranteed for a virtual circuit
  - Aggregate CIR should not exceed line speed
  - Data in excess of CIR liable to discard, i.e. not guaranteed
- 2 metrics in *CIR*
  - Committed burst size (B_c in duration T)
  - Excess burst size (B_e in duration T)

$$CIR = B_C / T$$

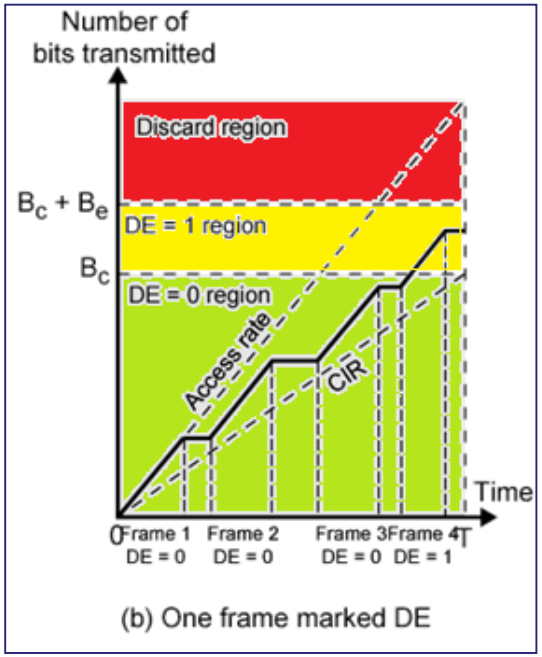
- Discard strategy
  - Data between B_c+B_e are permitted but not guaranteed
  - Data above B_c+B_e are discarded

Operations of CIR

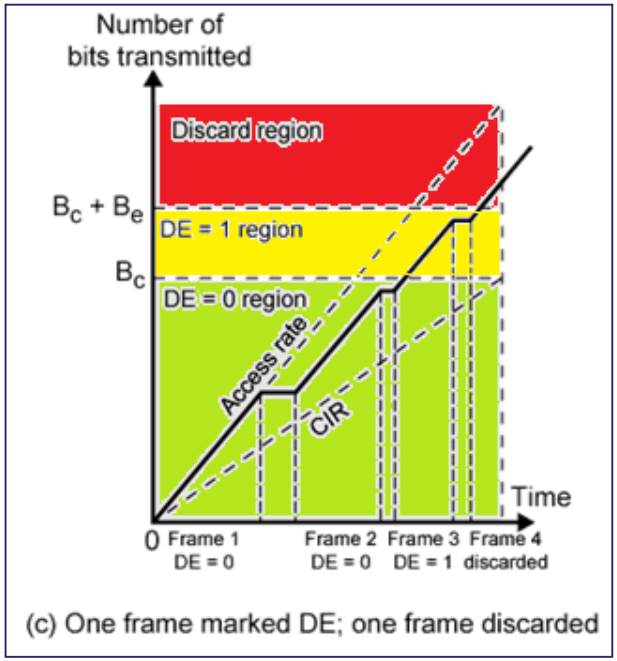




(a) All frames within CIR



(b) One frame marked DE

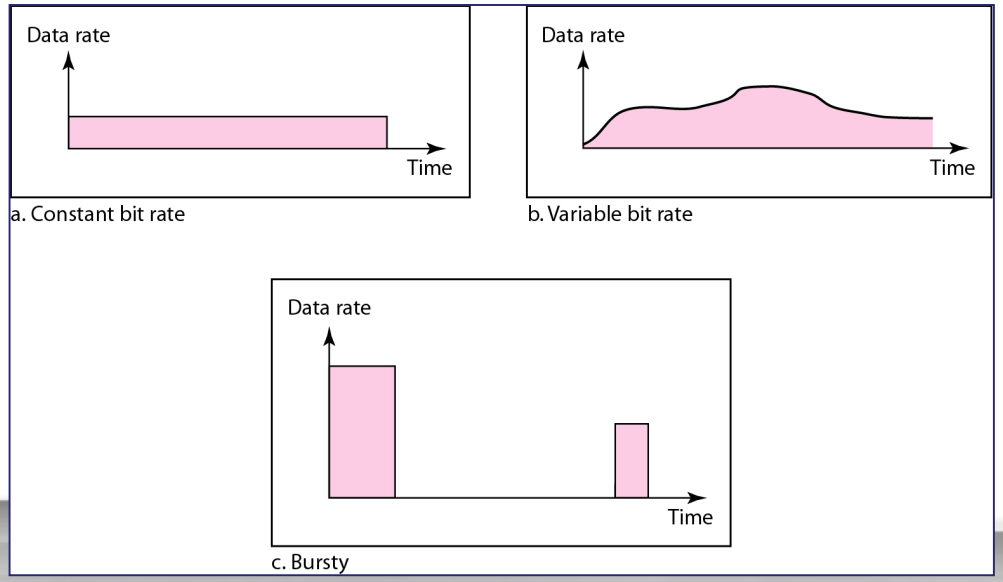


(c) One frame marked DE; one frame discarded

Traffic Management in ATM

- ATM Peculiarities
  - Wide range of application demands, from several kbps to hundreds of Mbps
  - Different traffic patterns, from real-time traffic to bursty traffic
  - Different network QOS, from lost sensitive to delay sensitive
  - Real-time traffic not amenable to flow control (not draw back)

Traffic Patterns



Latency/Speed Effects

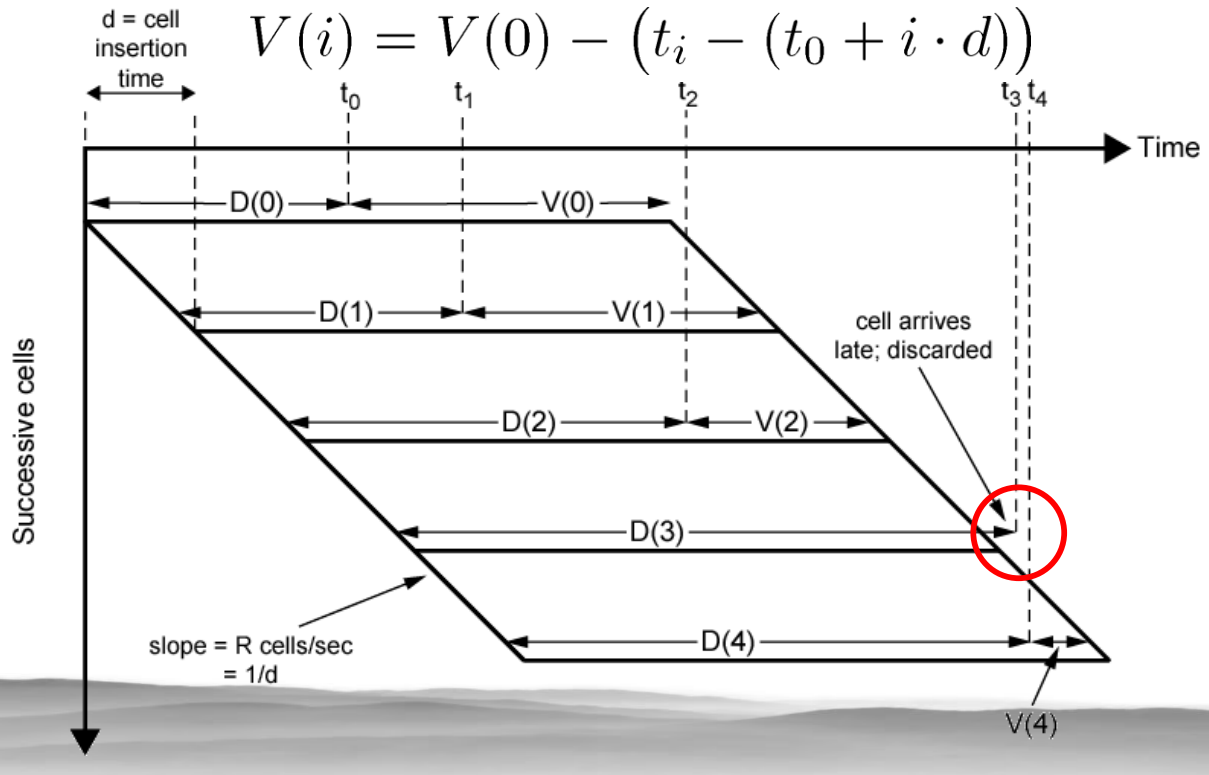
- ATM transmission rate is 150Mbps
  - Time to insert a cell $53\times 8 / (150\times 10^6) \approx 2.8\times 10^{-6} s$
  - Time to traverse network: $\approx 50\times 10^{-3}$ seconds
- If using choking packet or timeout mechanism
  - By the time source knows a cell is dropped, number of wasted bits will be:

$$N = \frac{50 \times 10^{-3}}{2.8 \times 10^{-6}} = 1.8 \times 10^4 \text{ cell} = 7.6 \text{ Mbits}$$

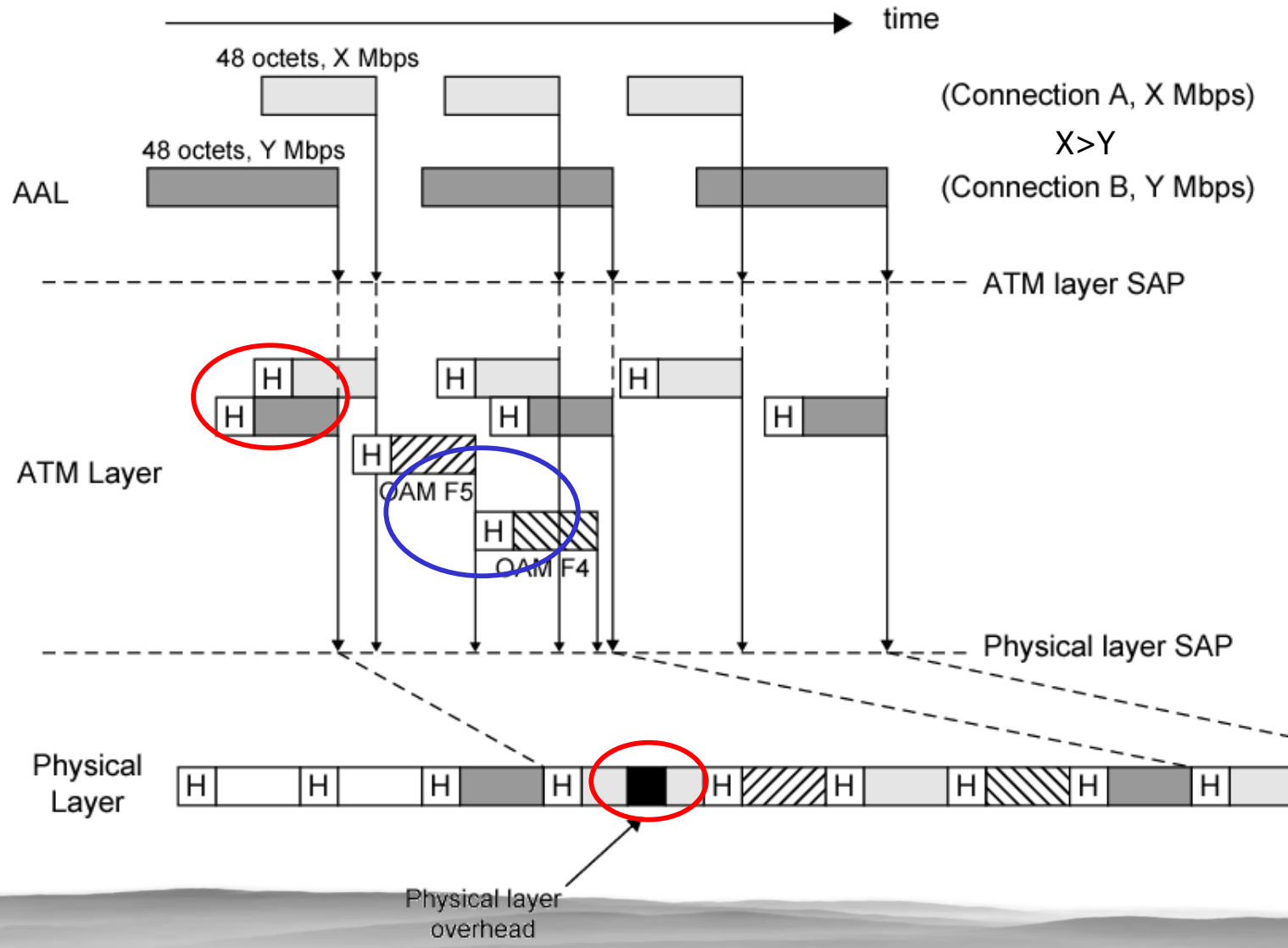
Real-Time Traffic

- For ATM voice/video, data is a real-time stream of cells
  - There will always be some variation in transit
  - Cell delivery delay is needed to maintain constant bit rate at app

$$V(i) = V(0) - \left(t_i - (t_0 + i \cdot d)\right)$$



Cell Delay Variation

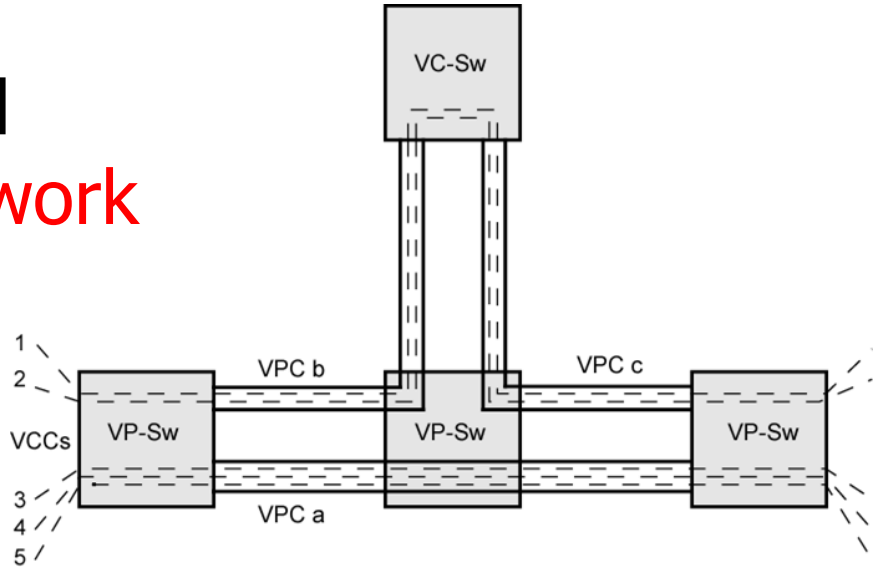


ATM Traffic Control Functions

- Resource management using virtual paths
- Connection admission control
- Usage parameter control
  - Traffic shaping using Token Bucket
- Selective cell discard
- Cell scheduling

Resource Management Using Virtual Paths

- Separate traffic flow according to traffic characteristics
  - User to User, User to Network, Network to Network
  - Cell loss ratio, Cell transfer delay, Cell delay variation
- VCs within a VP should experience similar network performance



VPC = Virtual path connection
VCC = Virtual channel connection
VP-Sw = Virtual path switching function
VC-Sw = Virtual channel switching function

Connection Admission Control

- First line of defense
  - User specifies traffic characteristics for new connection (VC or VP) by selecting a traffic contract
  - Network accepts connection only if it can meet the demand
- Traffic contract
  - Peak cell rate: max cell per second
  - Cell delay variation tolerance: millisecond diff tolerated
  - Sustainable cell rate: average cell per second
  - Maximum burst size: max number of cells in PCR

Usage Parameter Control

- Traffic policing
  - Monitor connection to ensure traffic conforms to contract
  - Based on traffic contracts
- Combined with cell tagging
  - CLP: Cell Loss Priority
  - Variable bit rate connections
  - Constant bit rate connections

Parameter Control in VBR

- Apply token bucket
  - Cells that exceed *PCR* are discarded
  - Cells that below *SCR* is ok
  - Cells that exceed *SCR+MBS* are either discarded or tagged with *CLP=1*
  - Cells that exceed *SCR* (<*MBS*) may be tagged with *CLP=1*
- Suppose *PCR* set to 20Mbps, *MBS* set to 100 cells
  - Then time for burst will be

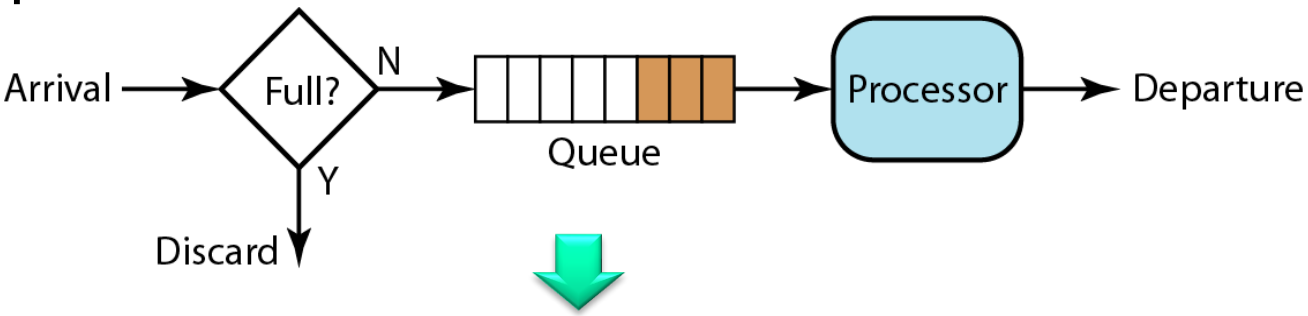
$$(100cells \times 424bits/cell) \Big/ 20 \times 10^6 bits/second = 2.12ms$$

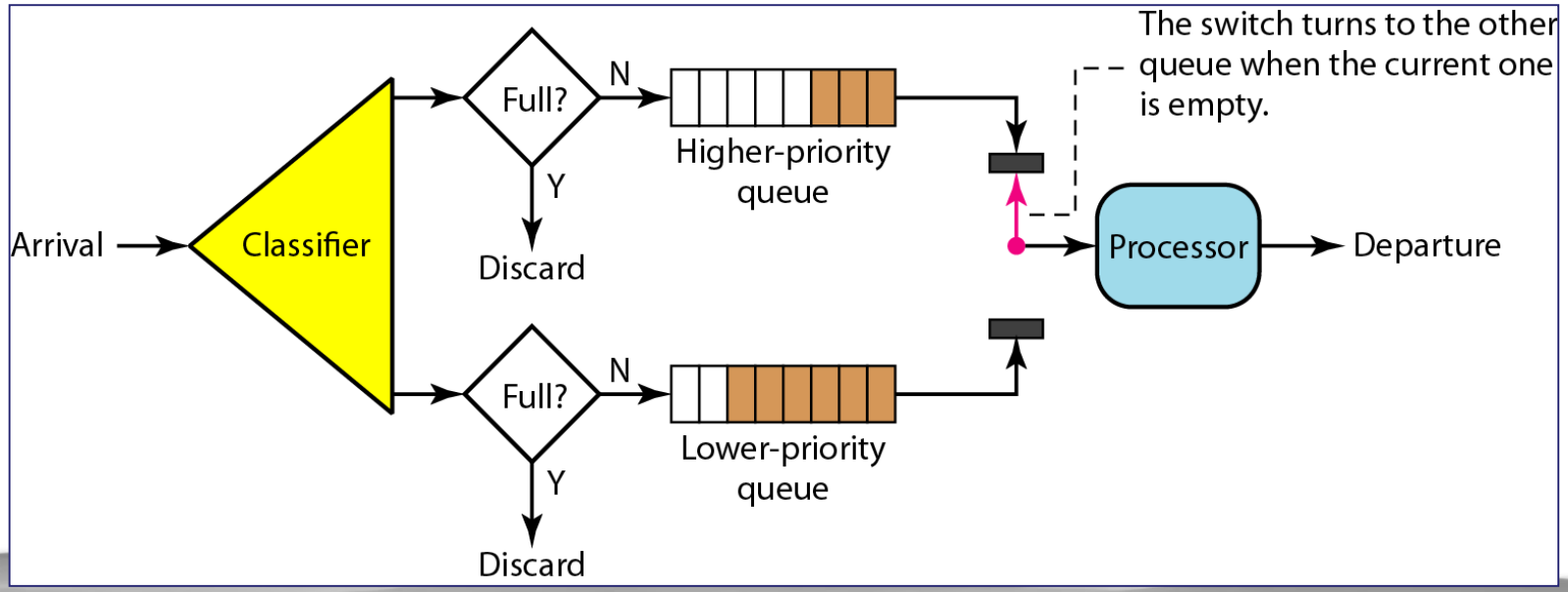
Parameter Control in CBR

- Much like leaky bucket
  - Compute cell inter-arrival time d = 1/PCR
  - (d – CDVT) will be the tolerance limit
- Tagging policy
  - Cells that exceed tolerance limit are discarded
  - Cells that below PCR is ok
  - Cells that exceed PCR but blow tolerance limit are either tagged or discarded

Cell Scheduling

- On each switch, instead of FIFO queue, priority queuing is applied for each cell





More Advanced Scheduling

- Weighted fair queuing, scheduling based on VP or VC