YILDIZ TEKNİK ÜNİVERSİTESİ 1911

COMPUTER NETWORK AND COMMUNICATION PROTOCOLS

congestion control in packet–switching network

STUDENT NAME: BAN ISAM RASHID

PROF .DR . HASAN HÜSEYEİN BALIK

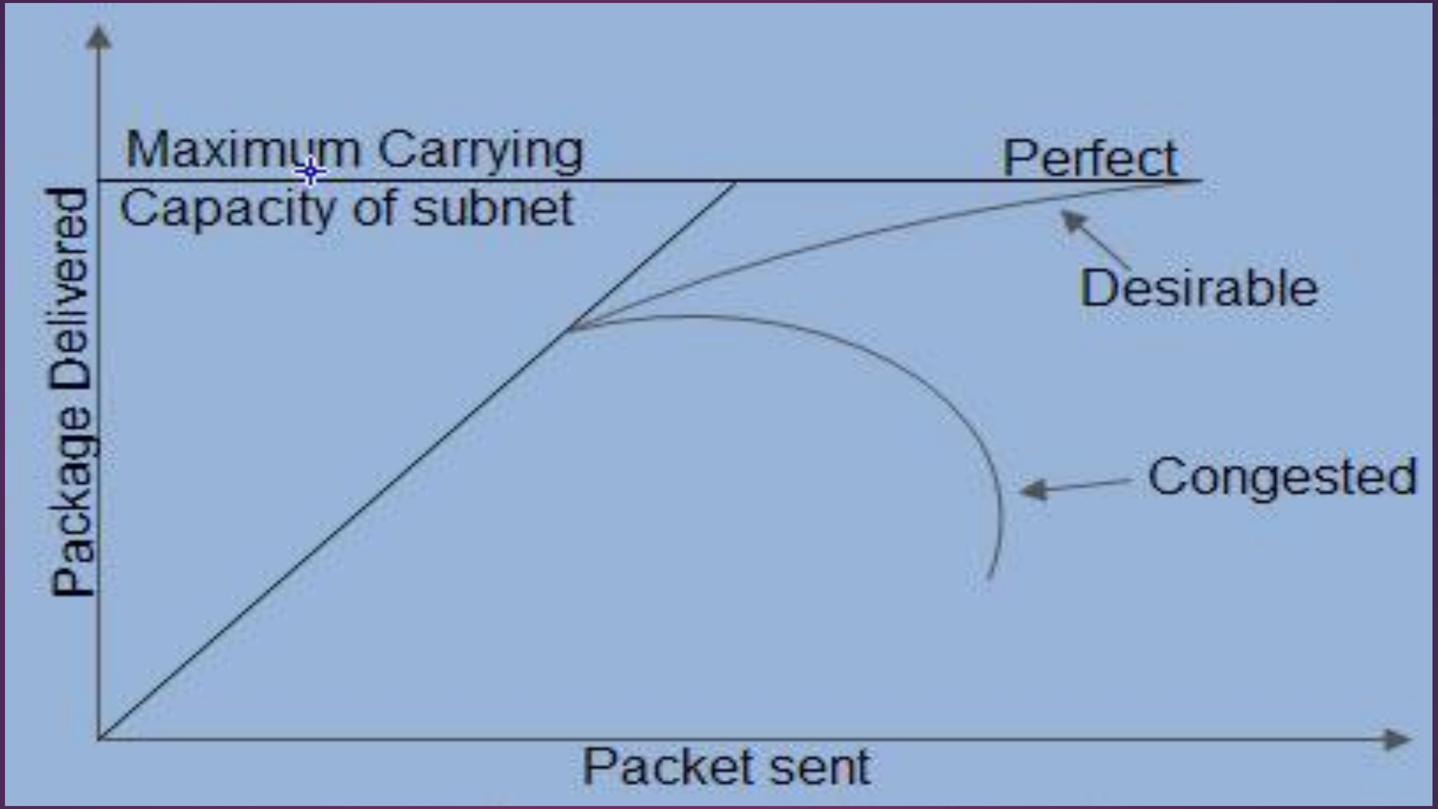
OUTLINE

- *WHAT IS CONGESTION ?*
- *CAUSING OF CONGESTION*
- *TRAFFIC SHAPPING AND TRAFFIC POLICING*
- *MECHANISMS OF CONGESTION CONTROL IN PACKET-SWITCHING NETWORK*
- *TCP ,DCCP PROTOCOL*

WHAT IS CONGESTION :

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades.

Congestion in a network occur when , the load on the network (the number of packets sent to the network) is greater than the capacity of the network.



Figure(1) concept of congestion

Causing of Congestion:

_The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up.

_ The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

_ congestıon in subnet can occurs ıf the processor is slow

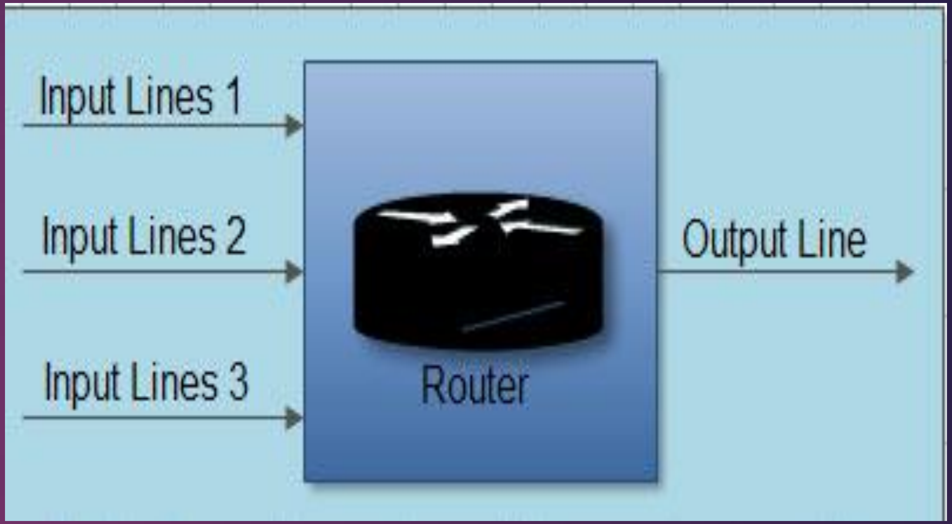
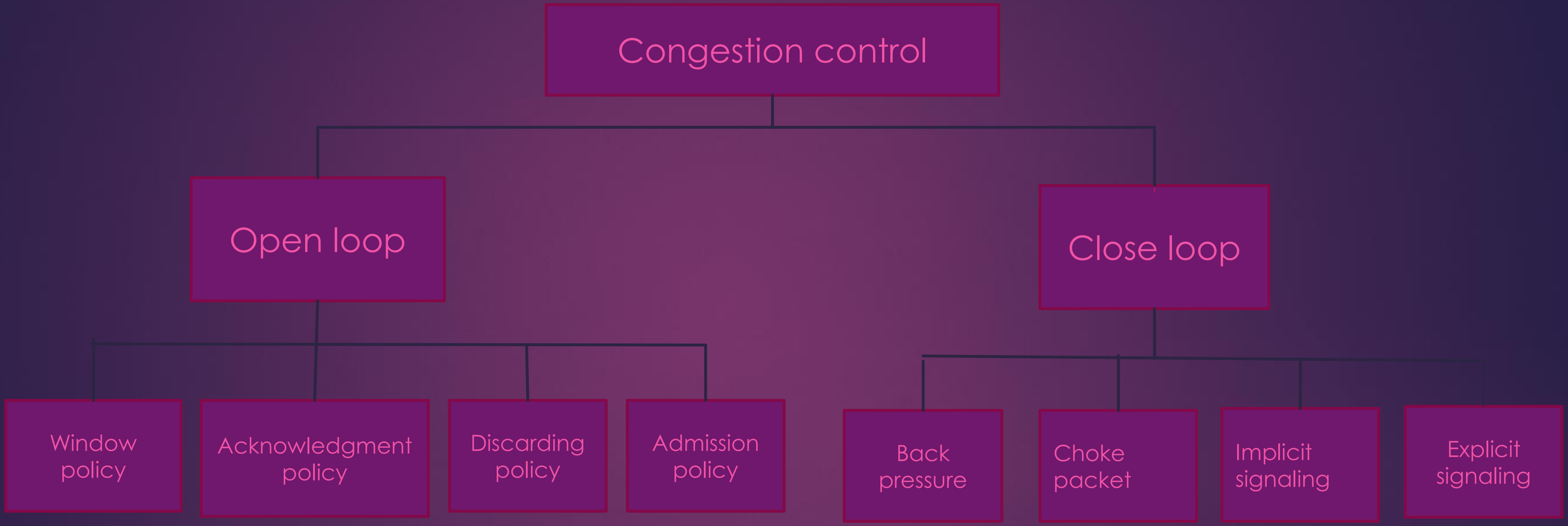


Figure (2) illustrates the congestion

THECHNIQUES OF CONGESTION CONTAL:



Congestion control

Open loop

Close loop

Window policy

Acknowledgment policy

Discarding policy

Admission policy

Back pressure

Choke packet

Implicit signaling

Explicit signaling

THECHNIQUES OF CONGESTION CONTAL: **Open loop techniques:**

in this method ,policies is used to prevent the congestion before it happens. Congestion control is handled either the source and distention .

* **The acknowledgement policy** : imposed by the receiver may also affect congestion.

- If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.
  - To implement it, several approaches can be used:
    1. A receiver may send an acknowledgement only if it has a packet to be sent.
    2. A receiver may send an acknowledgement when a timer expires.
    3. A receiver may also decide to acknowledge only *N* packets at a time.

* **Discarding Policy:** A router may discard some packets when congestion is likely to happen.

* **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 here is a possibility of future congestion.

* **Window Policy:**To implement window policy selective reject window method is used for congestion control. Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receive.

THECHNIQUES OF CONGESTION CONTAL: **close loop techniques:**

Closed loop congestion control mechanisms try to remove the congestion after it happens .

Backpressure : Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.

- The backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.
- In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.

Choke Packet :

In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

• Here, congested node does not inform its upstream node about the congestion as in backpressure method.

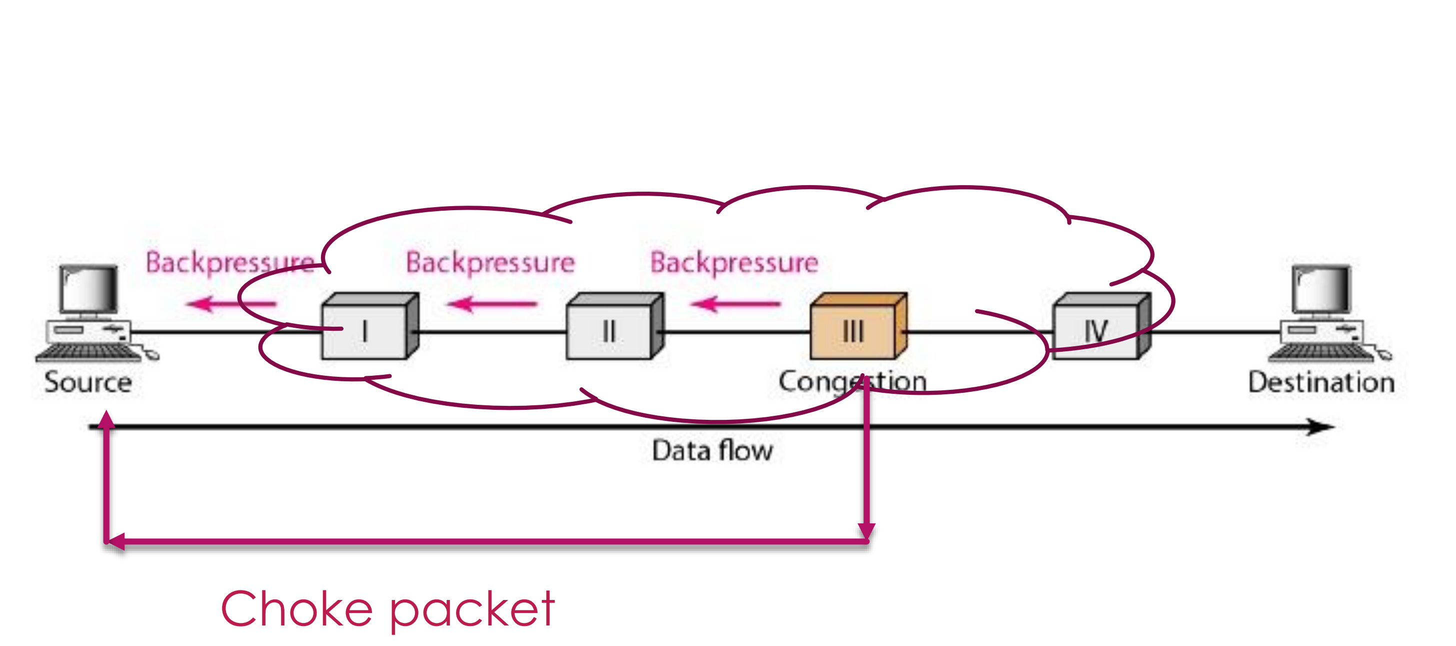


Figure (3)illustrates choke packet and backpressure

THECHNIQUES OF CONGESTION CONTAL: **close loop techniques:**

Implicit Signaling:

- In implicit signaling, there is no communication between the congested node or nodes and the source.
- The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.

Explicit Signaling:

- In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.
- Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .
- Explicit signaling can occur in either the forward direction or the backward direction .

TRAFFIC SHAPPING AND TRAFFIC POLICING:

Two important tools in managing network are traffic shaping and traffic policing.

* **Traffic shaping:** is aimed at smoothing out traffic flow by reducing packet clumping that leads to fluctuations in buffer occupancy.

* **Traffic policing :**discriminates between incoming packets that conform to quality of service (QoS) agreement and those that don't.

Packets that don't conform

treated in one of the following ways:

1. Give the packet lower priority compared to packets in other output queues.
2. Label the packet as nonconforming by setting the appropriate bits in a header.
3. Discard the packet.

* **Two important techniques used for traffic shaping or traffic policing are token bucket and leaky bucket .**

TRAFFIC SHAPPING AND TRAFFIC POLICING:

token bucket

* This scheme provides a concise description of the peak and average traffic load
the recipient can expect and it also provides a convenient mechanism by which the
sender can implement a traffic flow policy.

* A token bucket traffic specification consists of two parameters:

Token replenishment rate R

Bucket size B.

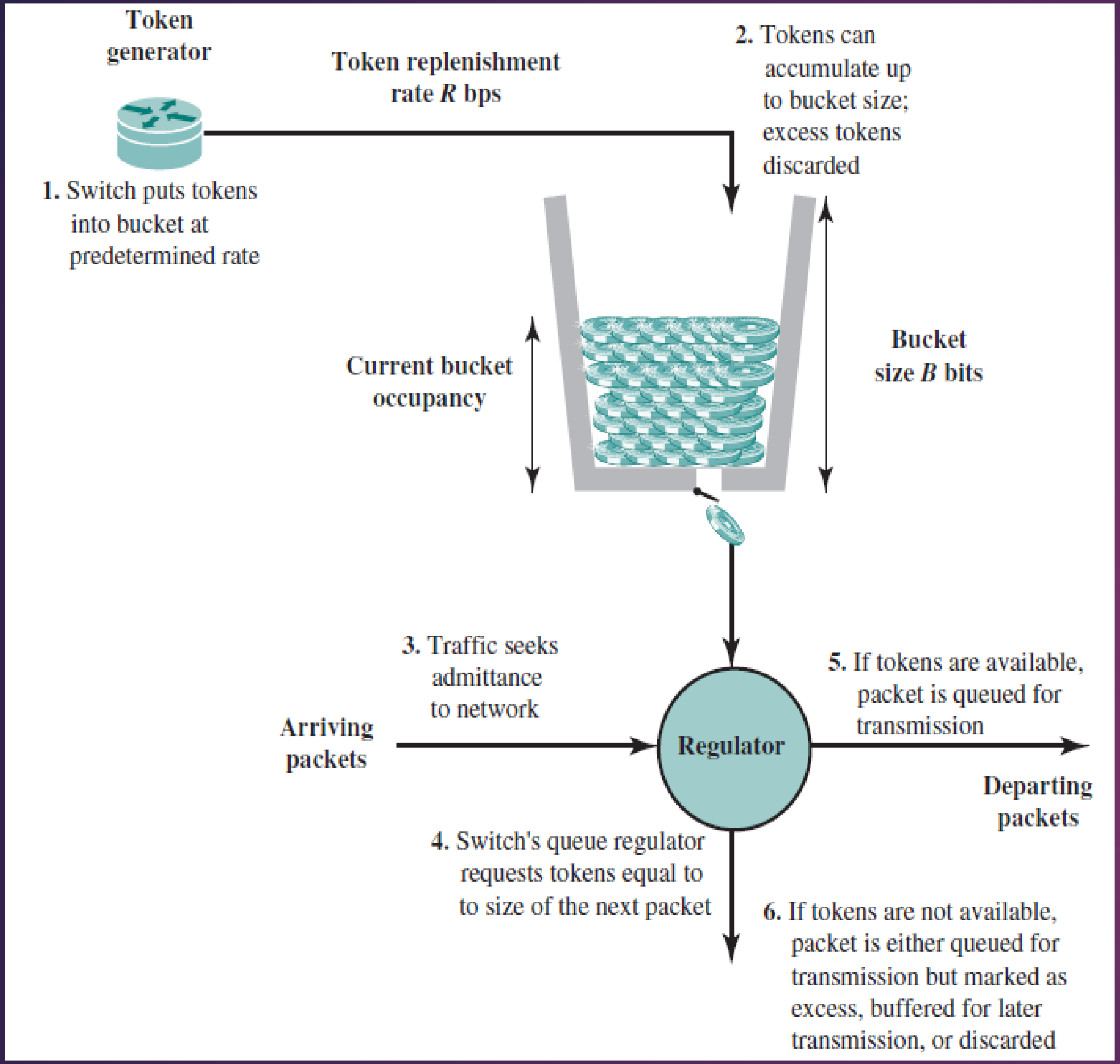
* token bucket is used in Bluetooth.

Advantages:

Many traffic sources can be defined easily and accurately by a token bucket scheme.

The token bucket scheme provides a concise description of the load

The token bucket scheme provides the input parameters to policing function


Token generator
Token replenishment rate *R* bps
2. Tokens can accumulate up to bucket size; excess tokens discarded
1. Switch puts tokens into bucket at predetermined rate
Current bucket occupancy
Bucket size *B* bits
3. Traffic seeks admittance to network
Arriving packets
Regulator
5. If tokens are available, packet is queued for transmission
Departing packets
4. Switch's queue regulator requests tokens equal to to size of the next packet
6. If tokens are not available, packet is either queued for transmission but marked as excess, buffered for later transmission, or discarded

Figure(4) illustrate token bucket Algorithm

The bucket represents a counter that indicates the allowable number of bytes of data that can be sent at any time

- The bucket fills with byte tokens at the rate of R ,up to the bucket capacity

- Data arrive from the user and are assembled into packets, which are queued for transmission

- A packet may be transmitted if there are sufficient tokens to match the packet size
- If so, the packet is transmitted and
- the bucket is drained of the corresponding number of tokens
- If there are insufficient tokens available, then the packet exceeds the specification for this flow.

TRAFFIC SHAPPING AND TRAFFIC POLICING: leaky bucket

The algorithm maintains a running count of the cumulative amount of data sent in a counter *X*.

The counter is decremented at a constant rate of one unit per time unit to a minimum value of zero.

The counter is incremented by *I* for each arriving packet, where *I* is the size of the packet, subject to the restriction that the maximum counter value is *L*.

Leaky bucket is used in the asynchronous transfer mode (ATM), and in the TU-T H.261 standard for digital video coding and transmission

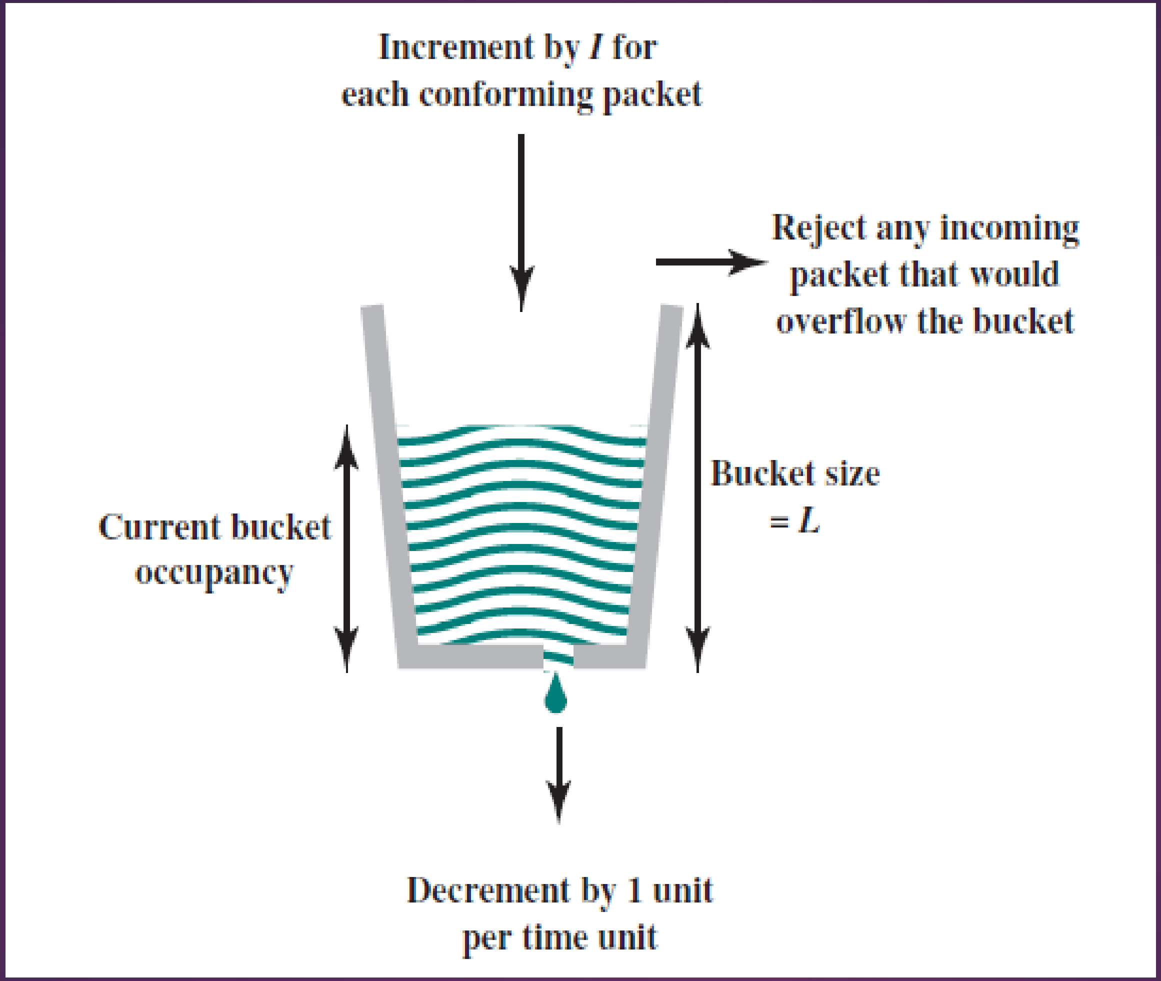
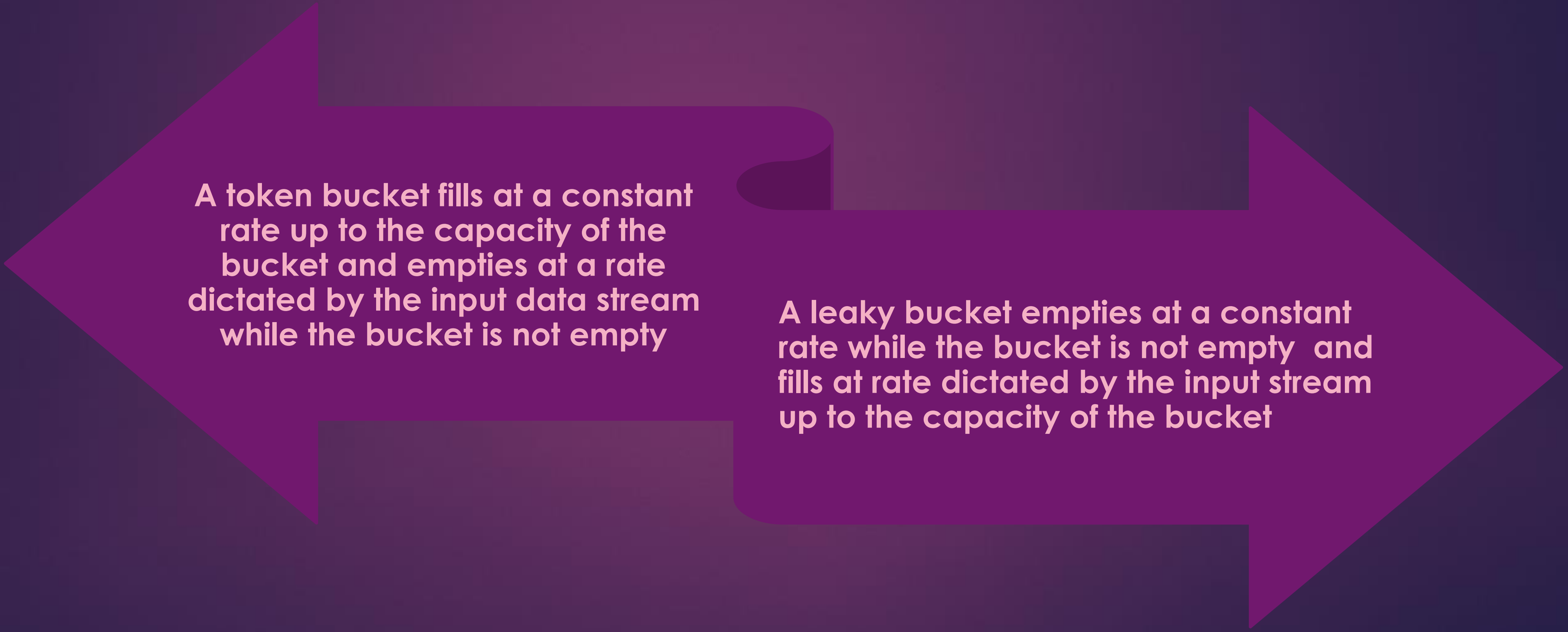

Increment by *I* for each conforming packet
Reject any incoming packet that would overflow the bucket
Bucket size = *L*
Current bucket occupancy
Decrement by 1 unit per time unit

Figure (5) illustrate leaky bucket Algorithm

TRAFFIC SHAPPING AND TRAFFIC POLICING:

- The difference between leaky bucket and token bucket



A token bucket fills at a constant rate up to the capacity of the bucket and empties at a rate dictated by the input data stream while the bucket is not empty

A leaky bucket empties at a constant rate while the bucket is not empty and fills at rate dictated by the input stream up to the capacity of the bucket

MECHANISMS OF CONGESTION CONTROL IN PACKET– SWITCHING NETWORK

1- Send a control packet from a congested node to some or all source nodes. This choke packet will have the effect of stopping or slowing the rate of transmission from sources

2- Rely on routing information. Routing algorithms, such as ARPANET's, provide link delay information to other nodes, which influences routing decisions.

3- Make use of an end-to-end probe packet. Such a packet could be time stamped to measure the delay between two particular endpoints

4- Allow packet-switching nodes to add congestion information to packets as they go by.

TCP , DATAGRAM CONGESTION CONTROL PROTOCOL (DCCP) PROTOCOL

TCP: designed to enable a destination to restrict the flow of segment from source to avoid buffer overflow at the destination

- the same flow mechanism is used to provide congestion control over the internet between source and destination

In multi media operation such as streaming audio or video ,reliable connection protocol is not appropriate .

- For TCP is difficult to see how many unreliable connectionless transport protocol such as UDP

DCCP is the developed protocol form a UDP

- DCCP include mechanism for detecting congestion by determining round-trip and packet drop rate
- DCCP run in the top of Ip and consists of ten packet types

TCP , DATAGRAM CONGESTION CONTROL PROTOCOL (DCCP) PROTOCOL

DCCP : packet types

- DCCP-Request: Sent by the client to initiate a connection
- DCCP-Response: Sent by the server in response to a DCCP-Request
- DCCP-Data: Used to transmit application data.
- DCCP-Ack: Used to transmit pure acknowledgments. That is, this packet is sent by one end of the connection to acknowledge an incoming data packet when there is no data packet available to send back.
- DCCP-Data Ack : Used to transmit application data with piggybacked acknowledgment information.
- DCCP-Close Req : Sent by the server to request that the client close the connection.
- DCCP-Close: Used by the client or the server to close the connection.
- DCCP-Reset: Used to terminate the connection, either normally or abnormally.
- DCCP-Sync, DCCP-Sync Ack: Used to resynchronize sequence numbers after large bursts of loss.

TCP , DATAGRAM CONGESTION CONTROL PROTOCOL (DCCP) PROTOCOL

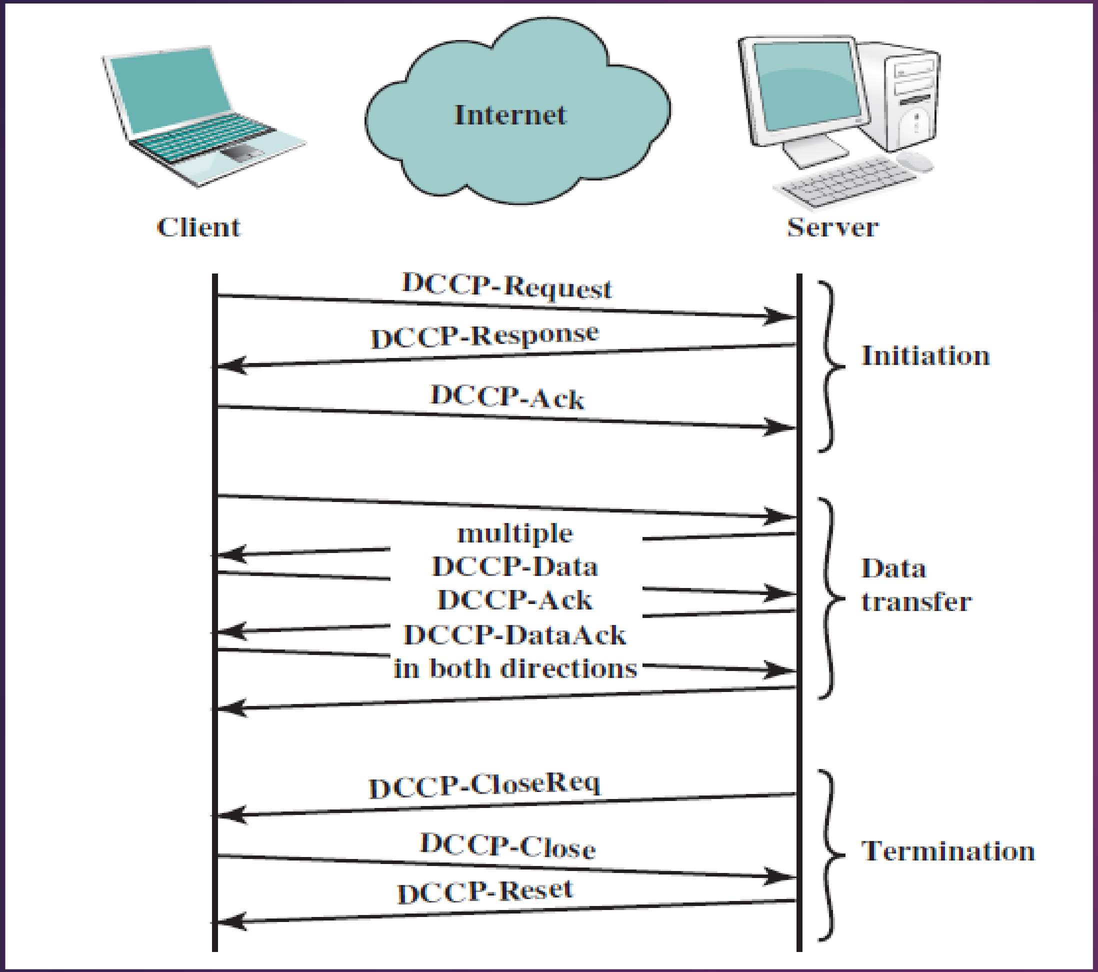
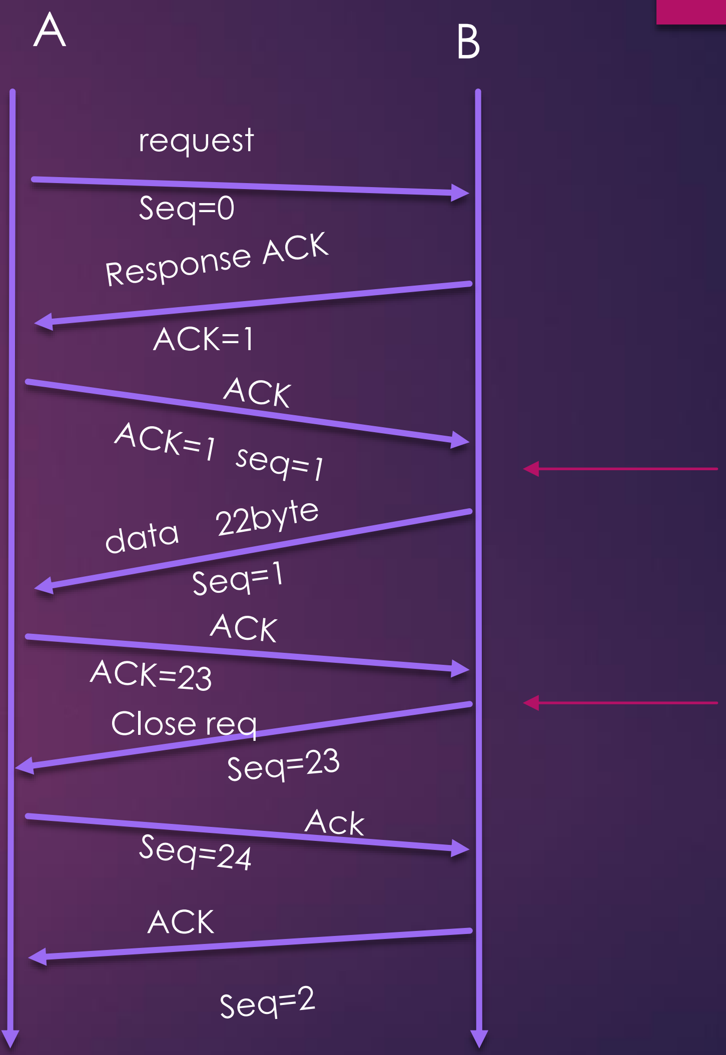


Figure (6)DCCP packet exchange



ÖNEMLİ

Bu projeler lisansüstü öğrencilerinin hazırladığı çalışmalar olup tüm sorumluluk hazırlayan öğrencilere aittir. Öğrenciler hazırladığı projeye göre not almışlardır.