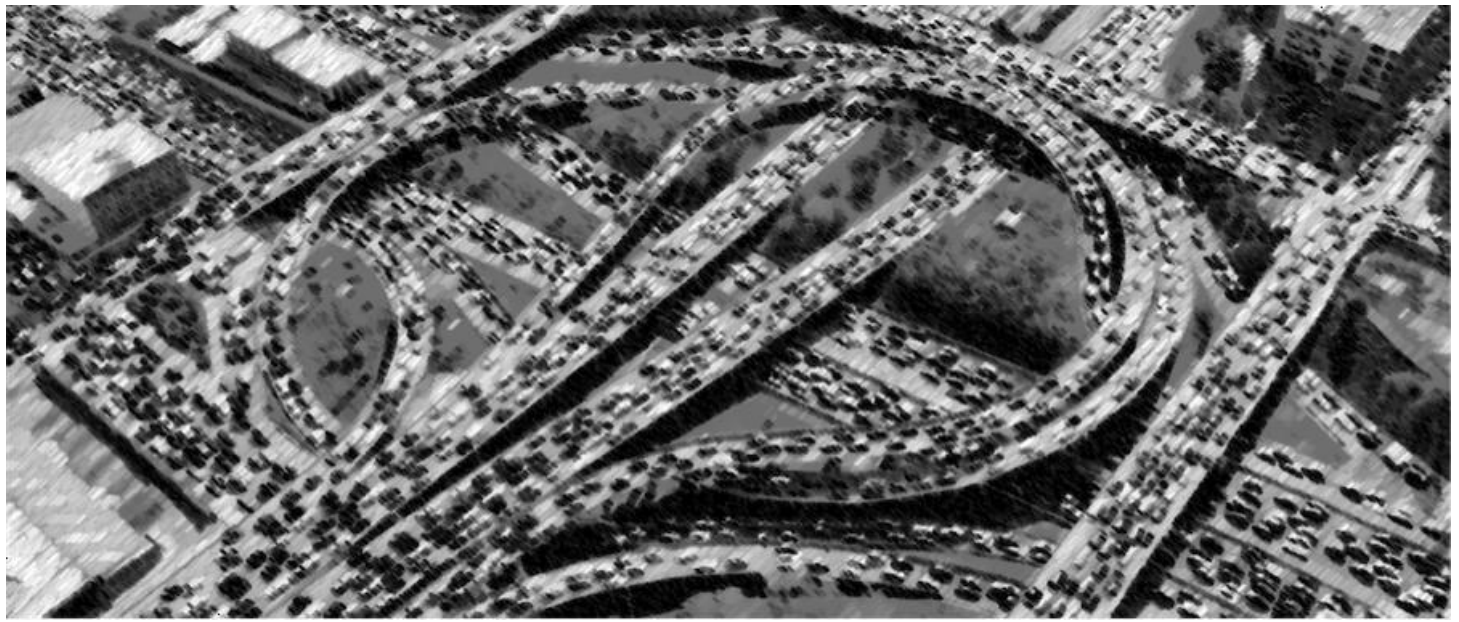
Congestion Control and QoS:
from Network Layer perspective

Computer network congestion is similar totraffic congestion in road network

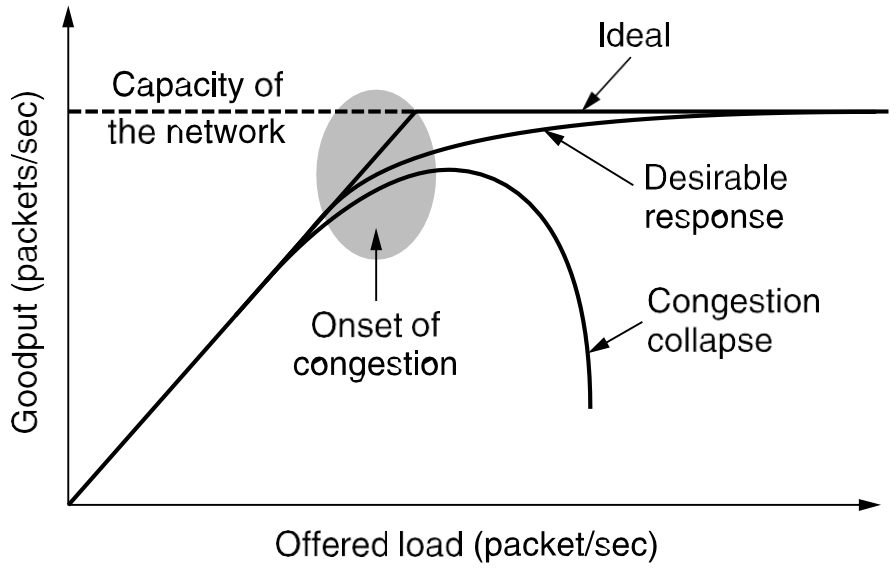


"Slow down" to the sender

Congestion control: to ensure that the network is able to carry the offered traffic. Involves all hosts and routers as it is a global issue.
Flow control: to ensure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it. Relates to the traffic between specific the sender and receiver.

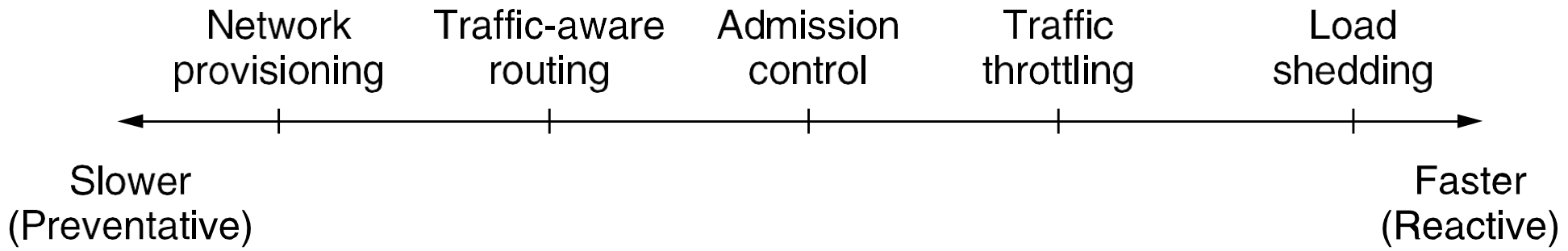
Congestion

When too much traffic is offered, congestion sets in and performance degrades sharply.



Increasing the buffer size at router is only going to worsen the situation. -- Why?

Approaches to Congestion Control

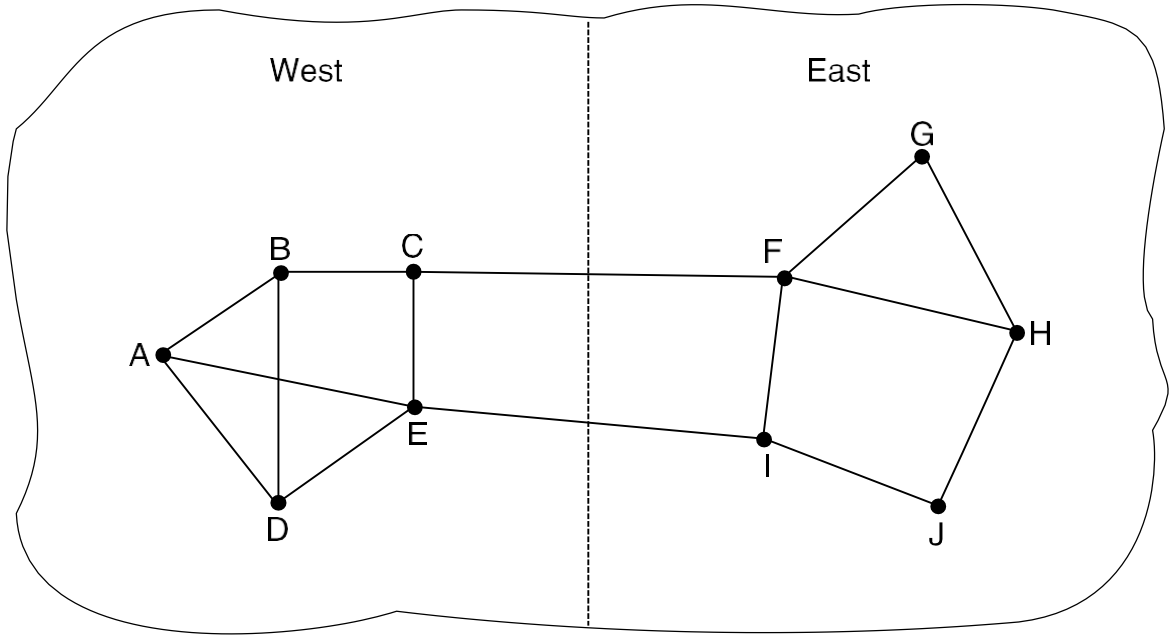


Why Congestion is managed in the Network Layer?

- *Maintaining QoS requires both per-hop and end-to-end behavior.*
- *Resource reservation needs to be done on per-hop basis. Otherwise end-to-end requirement can not be guaranteed.*
- *Network layer bridges end-to-end (Transport) and Per-hop (Data-link).*

Traffic-aware Routing

- What can be considered as the path weight? –load, propagation delay, link bandwidth

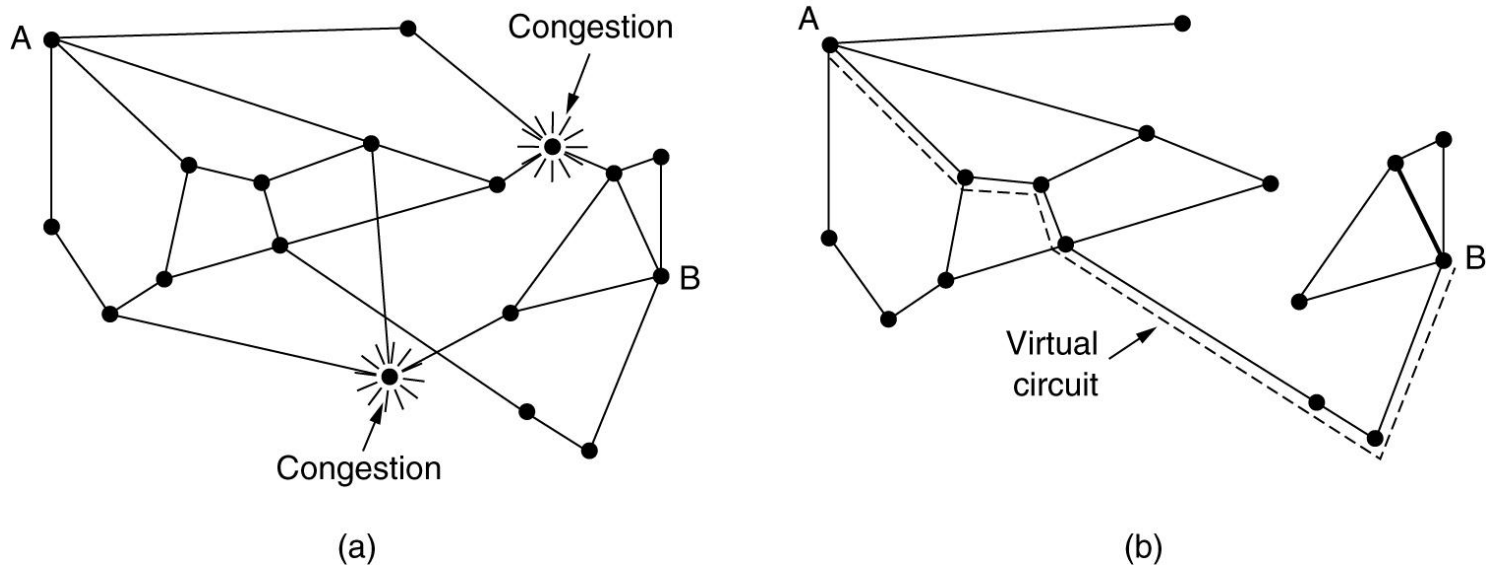


- Problem: Oscillation
- Solution approaches:
  - Multipath routing
  - Traffic engineering

Admission Control

- Widely used in virtual-circuit networks.
- Challenge: Virtual circuits in computer networks come in all shapes and sizes.
- The circuit must come with some characterization of its traffic to apply admission control.
- Admission control can also be combined with traffic-aware routing by considering routes around traffic hotspots as part of the setup procedure.

Admission Control



(a) A congested subnet. (b) A re-drawn subnet, eliminates congestion and a virtual circuit from A to B.

Traffic Throttling

1. Routers must determine when congestion is approaching, ideally before it has arrived. Continuously monitor the resources and look for
   - The utilization of the output links,
   - ***The buffering of queued packets inside the router***,
   - The number of packets that are lost due to insufficient buffering

   To maintain a good estimate of the queueing delay, d, a sample of the instantaneous queue length, s, can be made periodically and d updated according to

   $d_{new} = \alpha d_{old} + (1 - \alpha)s$

   where the constant α determines how fast the router forgets recent history

2. The routers must deliver timely feedback to the senders that are causing the congestion

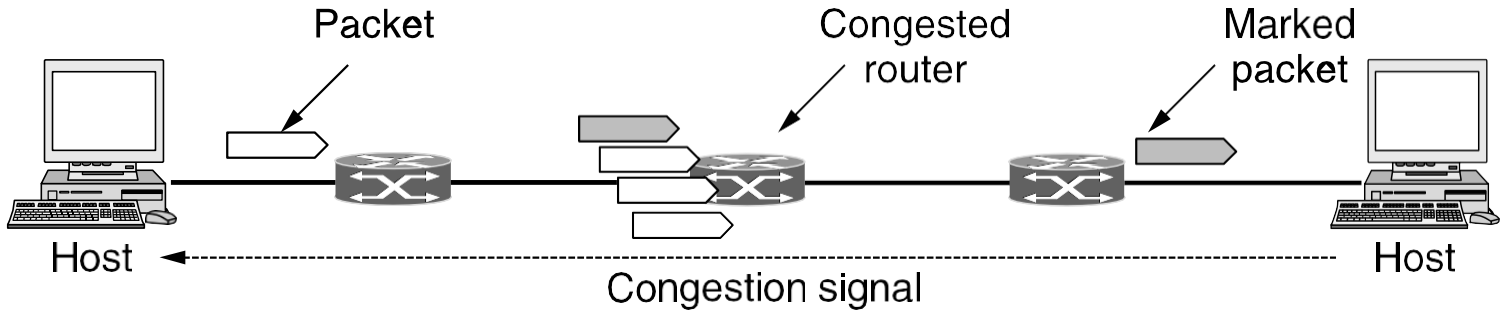
Feedback Mechanisms

Choke Packets:

- The router selects a congested packet and sends a **choke packet** back to the source host, giving it the destination found in the packet.

Explicit Congestion Notification (ECN):

- a router can tag any packet it forwards to signal that it is experiencing
- congestion→ destination note that there is a congestion and informs the hosts about it while sends back the reply→ the sender can throttle its transmission



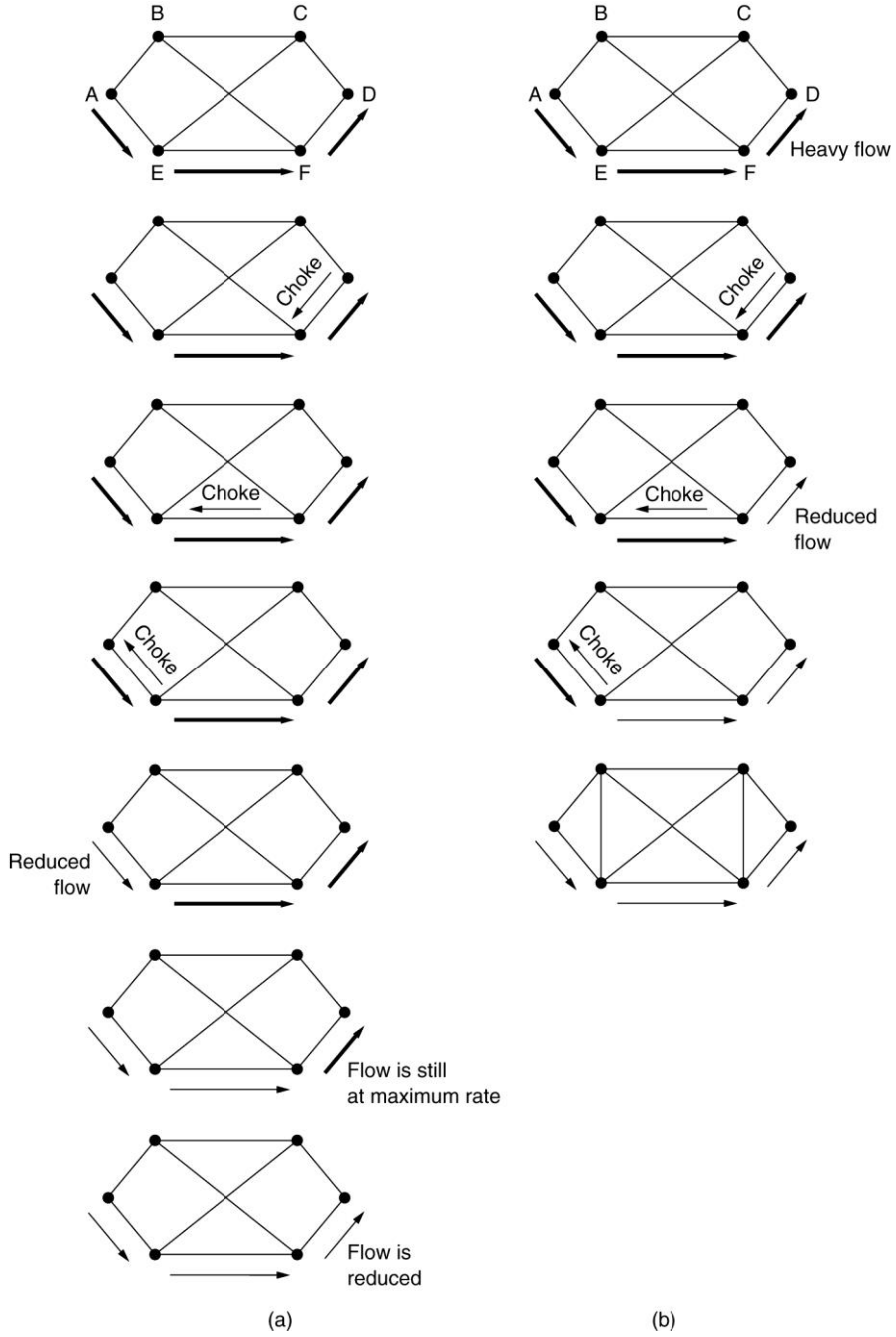
Feedback Mechanisms

Hop-by-Hop Backpressure

It takes 30 ms for a choke packet to get from NY to SF. For a 155 Mbps, 4.6 Mbps gets in the pipe.

(a) A choke packet that affects only the source.

(b) A choke packet that affects each hop it passes through



Dropping Packets

Load shedding: Wine Vs. Milk

Wine: drop new packets (keep old); good for file transfer

Milk: drop old packets (keep new); good for multimedia

Q. Which packets to discard? *Intelligent load shedding requires cooperation from senders.*

Random Early Detection (RED)

- When the average queue length exceeds a threshold, packets are picked at random from the queue and discarded → The fastest sender will see a packet drop
- The affected sender will notice the loss when there is no acknowledgement, and then the transport protocol will slow down.

Quality of Service

- Some applications often need a minimum throughput and maximum latency to work.
- QoS refers to the ability of a network to provide better service to selected network traffic.
- An easy solution to provide good QoS is by overprovisioning.
- QoS mechanisms let a network with less capacity meet application requirements just as well at a lower cost.
- With QoS mechanisms, the network can honor the performance guarantees that it makes even when traffic spikes, at the cost of turning down some requests.

The primary objective of QoS is to provide priority including **dedicated bandwidth**, **controlled jitter** and **latency** (required by some real-time and interactive traffic), and **improved loss characteristics**.

Quality of Service

- Four issues must be addressed to ensure quality of service:
  1. What applications need from the network.
  2. How to regulate the traffic that enters the network.
  3. How to reserve resources at routers to guarantee performance.
  4. Whether the network can safely accept more traffic.

Quality of Service

- A stream of packets from a source to a destination is called a ***flow.***
  - A flow can be characterized by four primary parameters:

- **Bandwidth**

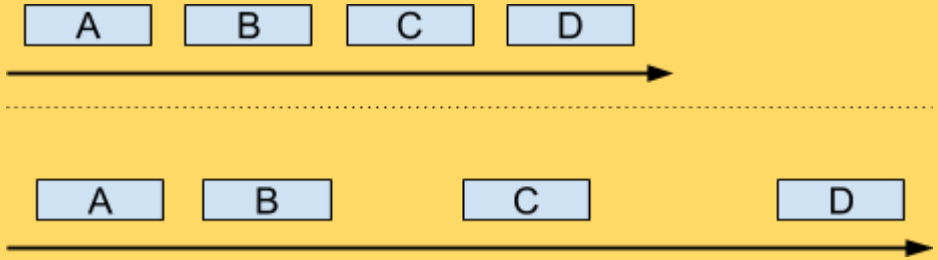
Delay

Transmission Delay

Propagation Delay

Queuing Delay

Jitter



Loss

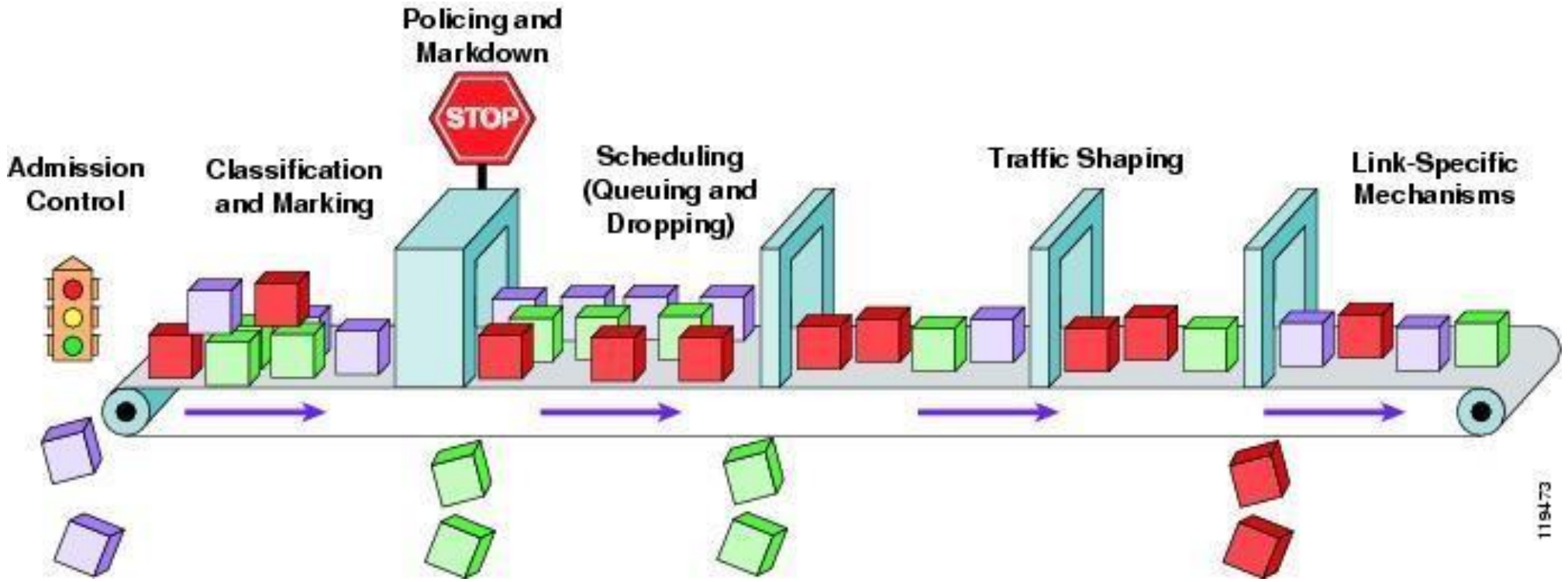
QoS Requirements

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Constant bit rate | Real-time variable bit rate | Non-real-time variable bit rate | Available bit rate

How stringent the quality-of-service requirements are.

Basic QoS Architecture



https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html

Traffic Shaping

- Before the network can make QoS guarantees, it must know what traffic is being guaranteed.
- Traffic shaping is a technique for regulating the average rate and burstiness of a flow of data that enters the network.

The goal is to allow applications to transmit a wide variety of traffic that suits their needs, including some bursts, yet have a simple and useful way to describe the possible traffic patterns to the network.

- When a flow is set up, the user and the network (i.e., the customer and the provider) agree on a certain traffic pattern (i.e., shape) for that flow.
- In effect, the customer says to the provider “My transmission pattern will look like this; can you handle it?”
- Sometimes this agreement is called an SLA (Service Level Agreement)

Traffic Shaping

- Traffic shaping reduces congestion and thus helps the network live up to its promise.
- How the provider can tell if the customer is following the agreement and what to do if the customer is not?
- Packets in excess of the agreed pattern might be dropped by the network, or they might be marked as having lower priority.
- Monitoring a traffic flow is called traffic policing.

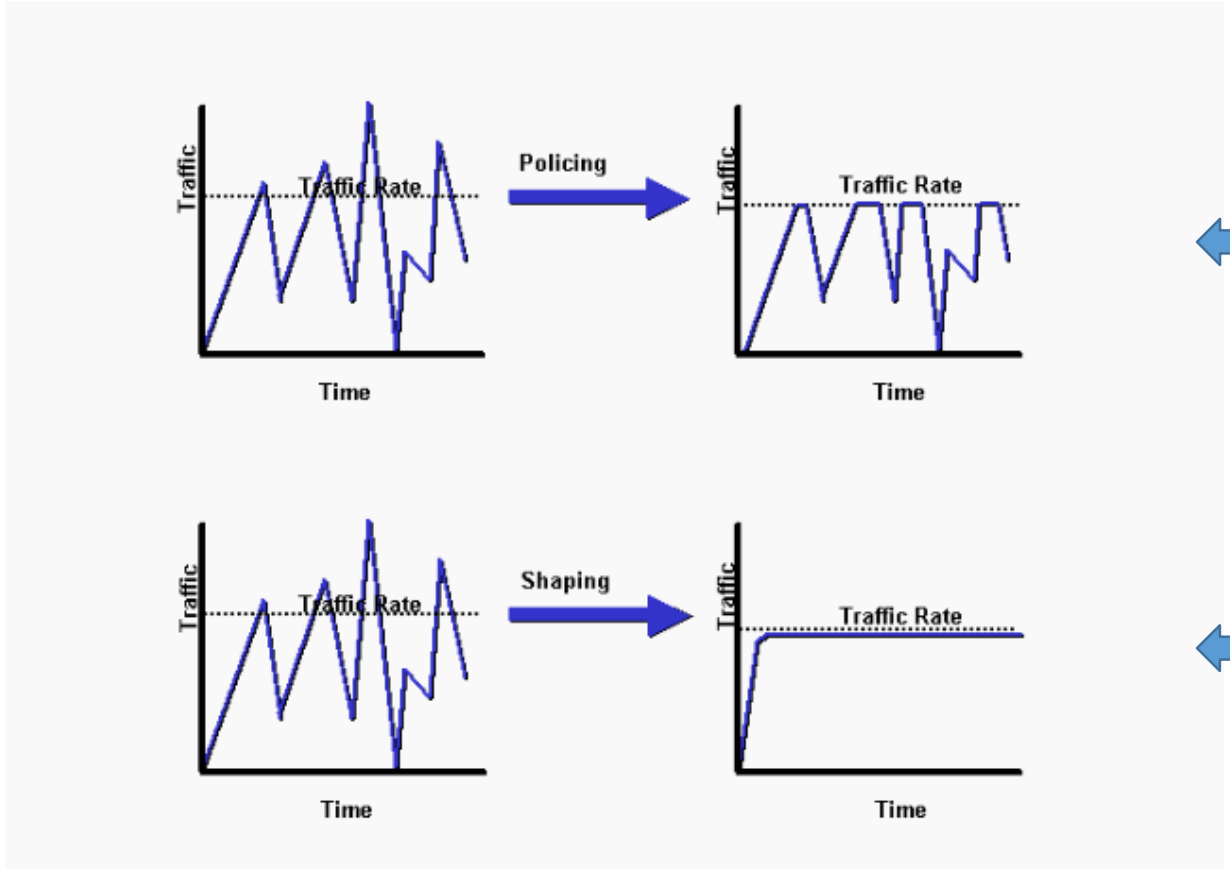
Traffic Shaping vs Traffic Policing

- **Traffic Shaping:** smooths out the traffic at the server side, rather than client side in order to regulate the average rate (and burstiness) of data transmission

- **Service level Agreement:** ‘My transmission pattern will look like this; can you handle it?”

- **Traffic Policing:** monitoring a traffic flow.

Traffic Policing vs. Traffic Shaping

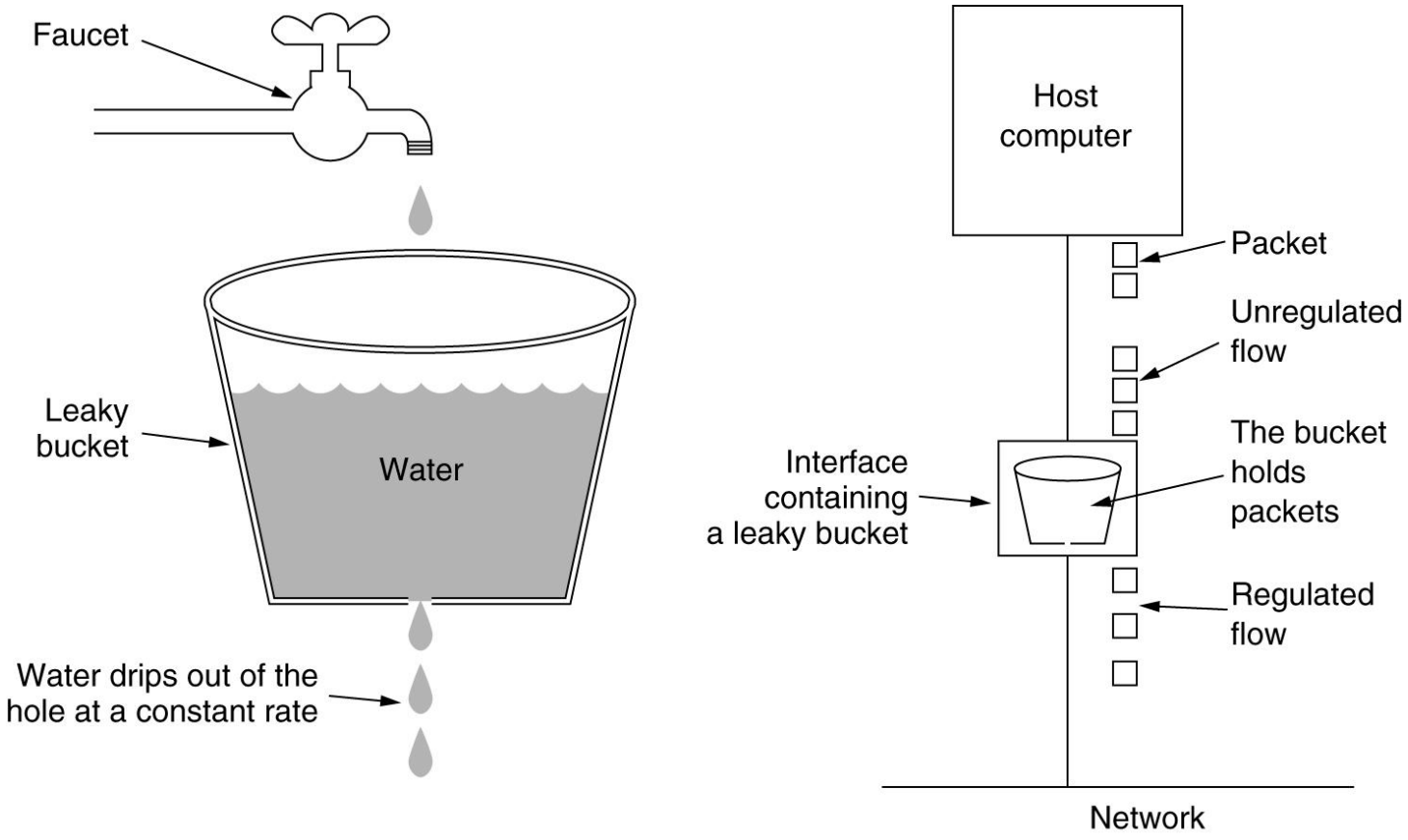


Applied to the inbound traffic

Applied to the outbound traffic

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

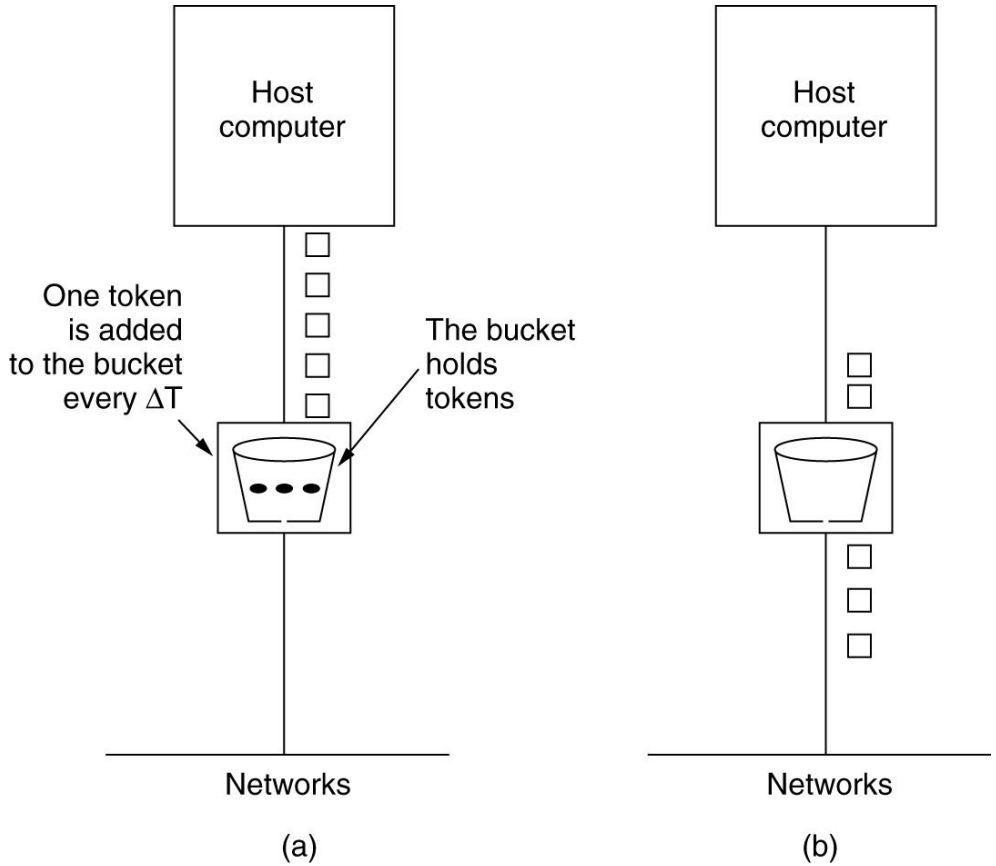
Traffic Shaping: The Leaky Bucket Algorithm(1986)



(a) A leaky bucket with water. (b) a leaky bucket with packets.

- ✓ Enforces a rigid output pattern at the avg rate
- ✓ Does not consider the traffic burstiness

Traffic Shaping: Token Bucket Algorithm



- ✓ Allows the idle host to save up the permission to send large bursts later, upto size of the bucket n.
- ✓ It always throws away the tokens when the bucket fills up but never discards packets.

Token bucket allows some burstiness (up to the number of token the bucket can hold)

Packet Scheduling

- To provide a performance guarantee, we must reserve sufficient resources along the route that the packets take through the network.
- Similar to virtual circuits, we can, assign a specific route to a flow and then ***reserve resources*** along that route.
- Algorithms that allocate router resources among the packets of a flow and between competing flows are called packet scheduling algorithms.
- Three kinds of resources can be reserved:
  - **Bandwidth:** not to oversubscribe any output line
  - **Buffer space:** some buffers can be reserved for a specific flow at the router
  - **CPU cycles:** to ensure timely processing of each packet at the router

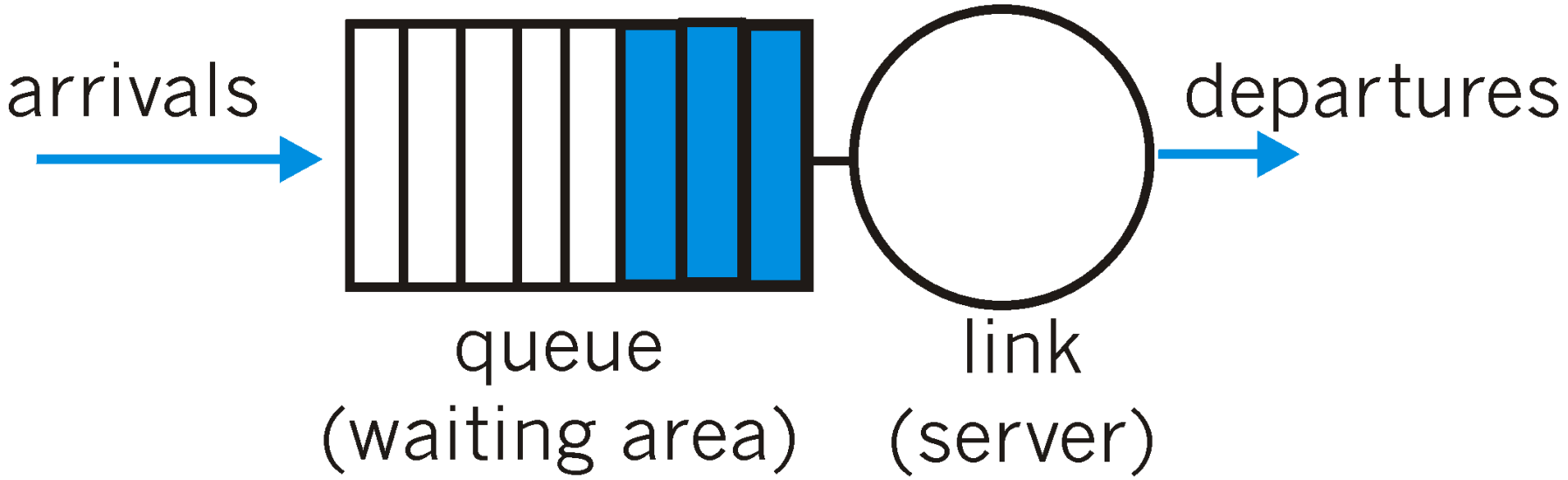
Packet Scheduling

- Packet scheduling algorithms allocate bandwidth and other router resources by determining which of the buffered packets to send on the output line next.

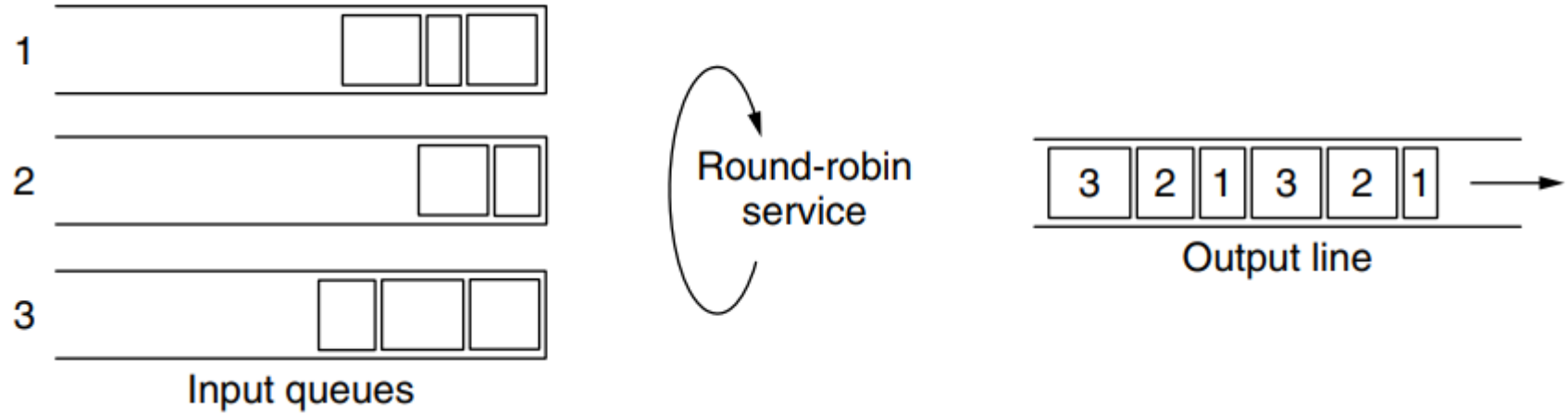
- Each router buffers packets in a queue for each output line until they can be sent, and they are sent in the same order that they arrived.

Packet Scheduling

- If a router handling multiple flows uses first-come first-served method to process packets, there is possibility of some flows being starved.

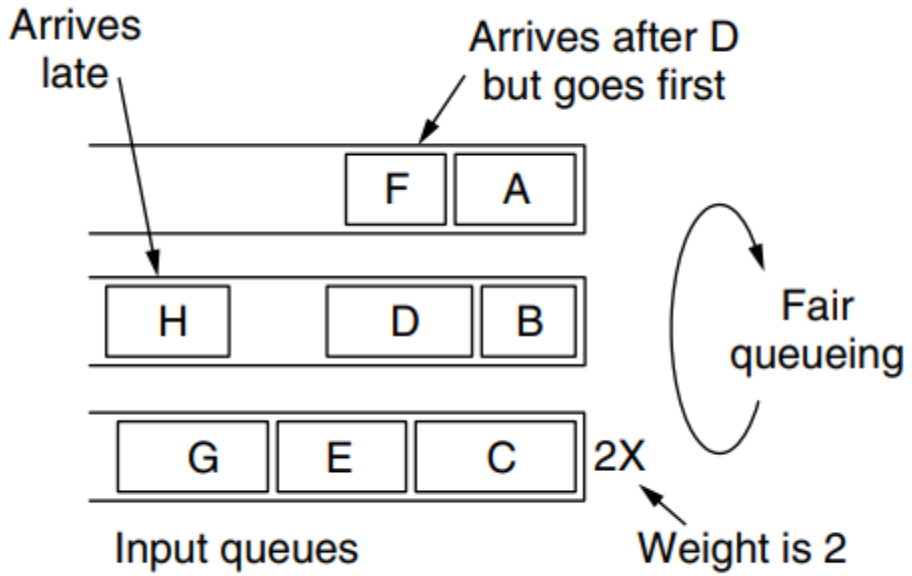


Round Robin fair queueing



Flaw: it gives more bandwidth to hosts that use large packets than to hosts that use small packets.

Weighted Fair Scheduling



(a)

Packet	Arrival time	Length	Finish time	Output order
A	0	8	8	1
B	5	6	11	3
C	5	10	10	2
D	8	9	20	7
E	8	8	14	4
F	10	6	16	5
G	11	10	19	6
H	20	8	28	8

(b)

(a) Weighted Fair Queueing. (b) Finishing times for the packets

Admission Control

- QoS guarantees are established through the process of admission control.
- The user offers a flow with an accompanying QoS requirement to the network.
- The network then decides whether to accept or reject the flow based on its capacity and the commitments it has made to other flows.
- If it accepts, the network reserves capacity in advance at routers to guarantee QoS when traffic is sent on the new flow.

Admission Control

- The reservations must be made at all of the routers along the route that the packets take through the network.
- Any routers on the path without reservations might become congested, and a single congested router can break the QoS guarantee.
- Many routing algorithms find the single best path between each source and each destination and send all traffic over the best path.
- This may cause some flows to be rejected if there is not enough spare capacity along the best path.
- QoS guarantees for new flows may still be accommodated by choosing a different route for the flow that has excess capacity.
- This is called QoS routing.

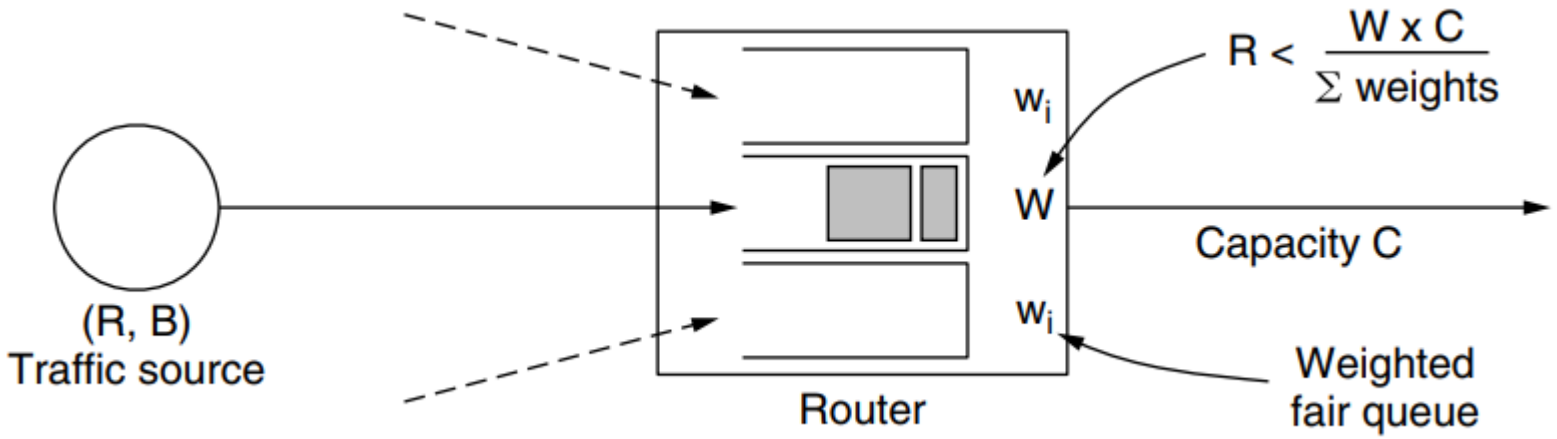
Admission Control

Parameter	Unit
Token bucket rate	Bytes/sec
Token bucket size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

An example flow-specification

Relating flow specifications to Router Resources:

One method of relating flow specifications to router resources that correspond to bandwidth and delay performance guarantees is given by Parekh and Gallagher (1993, 1994).



Bandwidth and delay guarantees with token buckets and WFQ

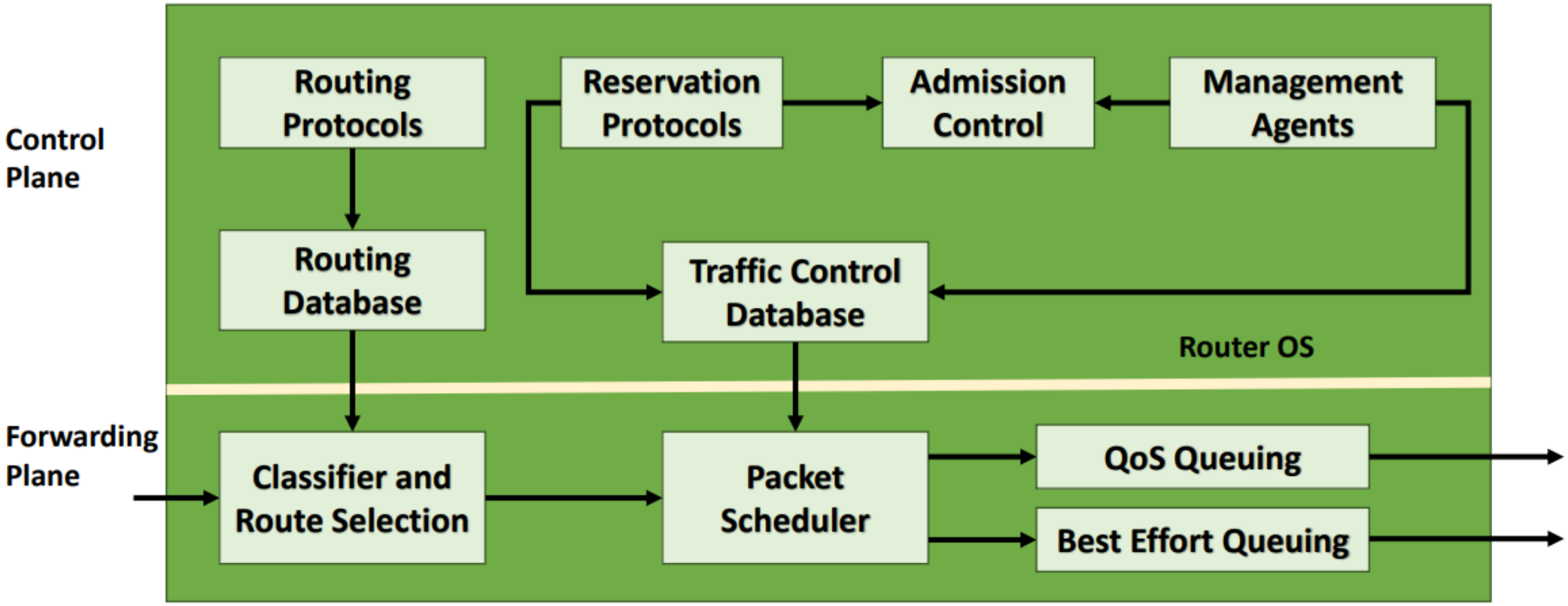
Relating flow specifications to Router Resources:

- It is based on traffic sources shaped by (R, B) token buckets and WFQ at routers.
- Each flow is given a WFQ weight W large enough to drain its token bucket rate R.

- For example, if the flow has a rate of 1 Mbps and the router and output link have a capacity of 1 Gbps, the weight for the flow must be greater than 1/1000th of the total of the weights for all of the flows at that router for the output link.

- This guarantees the flow a minimum bandwidth. If it cannot be given a large enough rate, the flow cannot be admitted.

Internet Service Architecture in a Router



Integrated Service (IntServ)

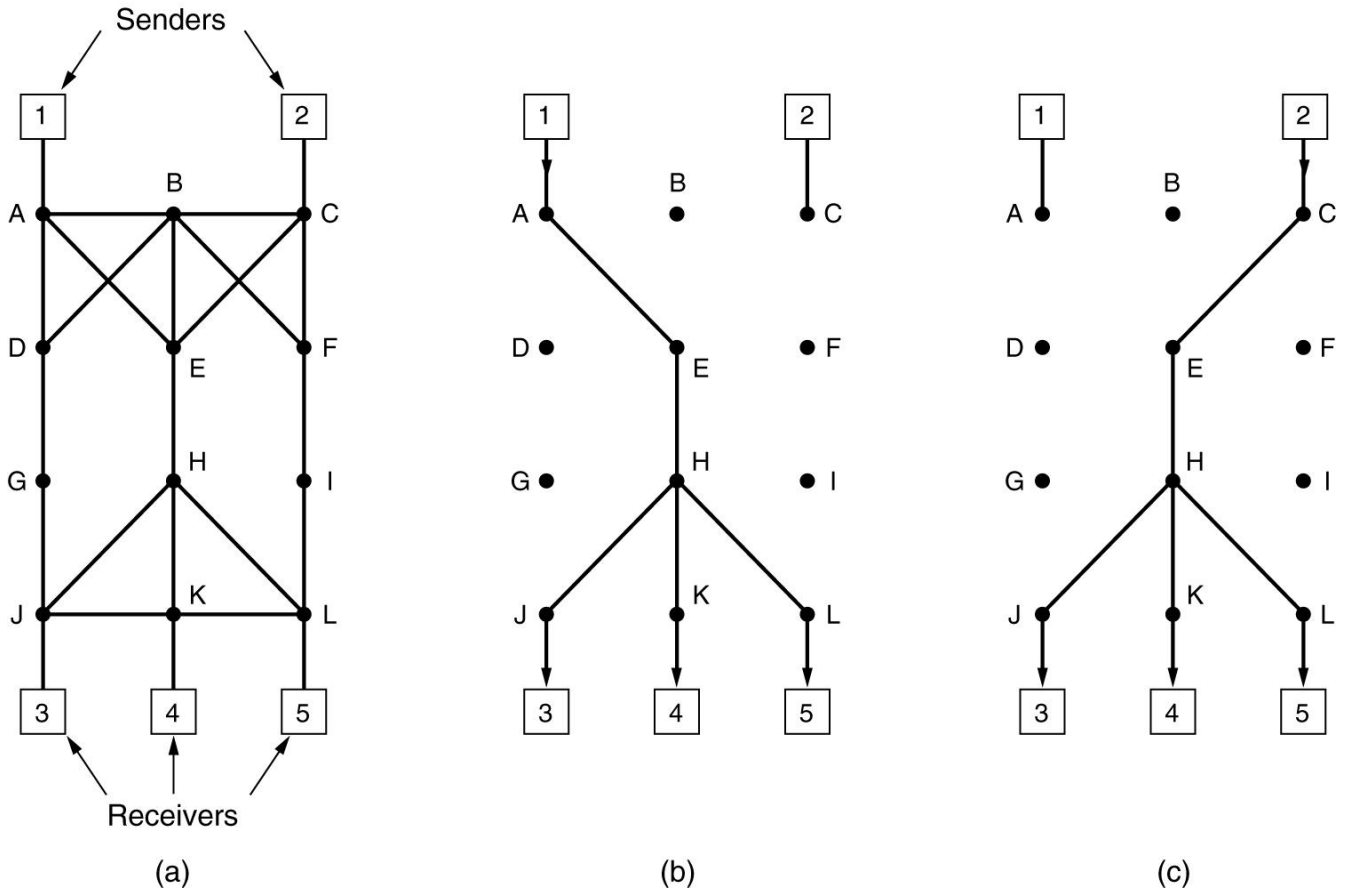
- A ***flow-based*** approach to QoS using resource reservation.
- Set of protocols aimed at ***streaming multimedia*** and standardized by the IETF. Allows both unicast and multicast transmissions.

- ***Resource reSerVation Protocol (RSVP)*** is used to reserve the resources at intermediate routers between sender and receivers.

- RSVP allows:
  - Multiple senders to transmit to multiple groups of receivers
  - Permits individual users to switch channels freely
  - Optimises bandwidth utilization while simultaneously eliminating congestion.

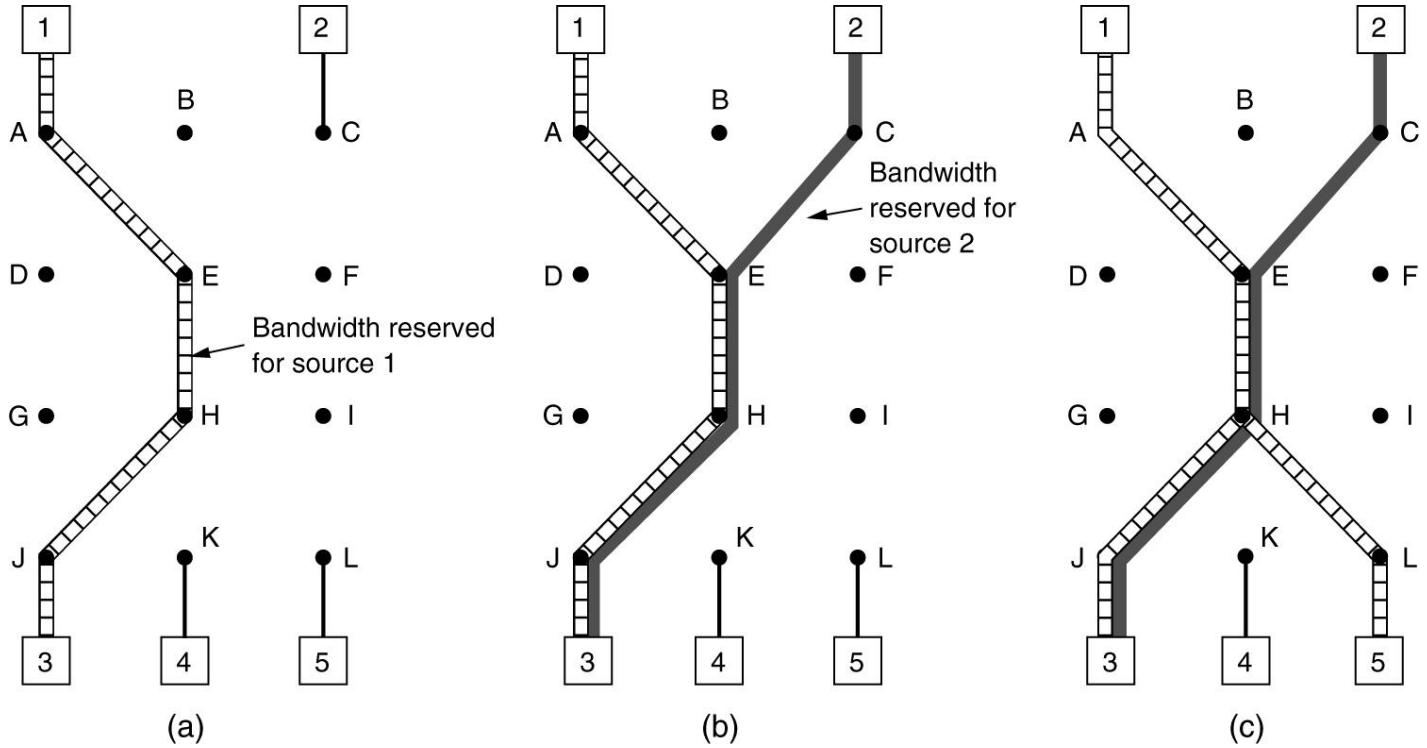
RSVP-The ReSerVation Protocol

- Bandwidth reservation is done with reverse path forwarding along the spanning tree.



(a)A network, (b) The multicast spanning tree for host 1. (c) The multicast spanning tree for host 2.

RSVP-The ReSerVation Protocol (2)



(a) Host 3 requests a channel to host 1. (b) Host 3 then requests a second channel, to host 2. (c) Host 5 requests a channel to host 1.

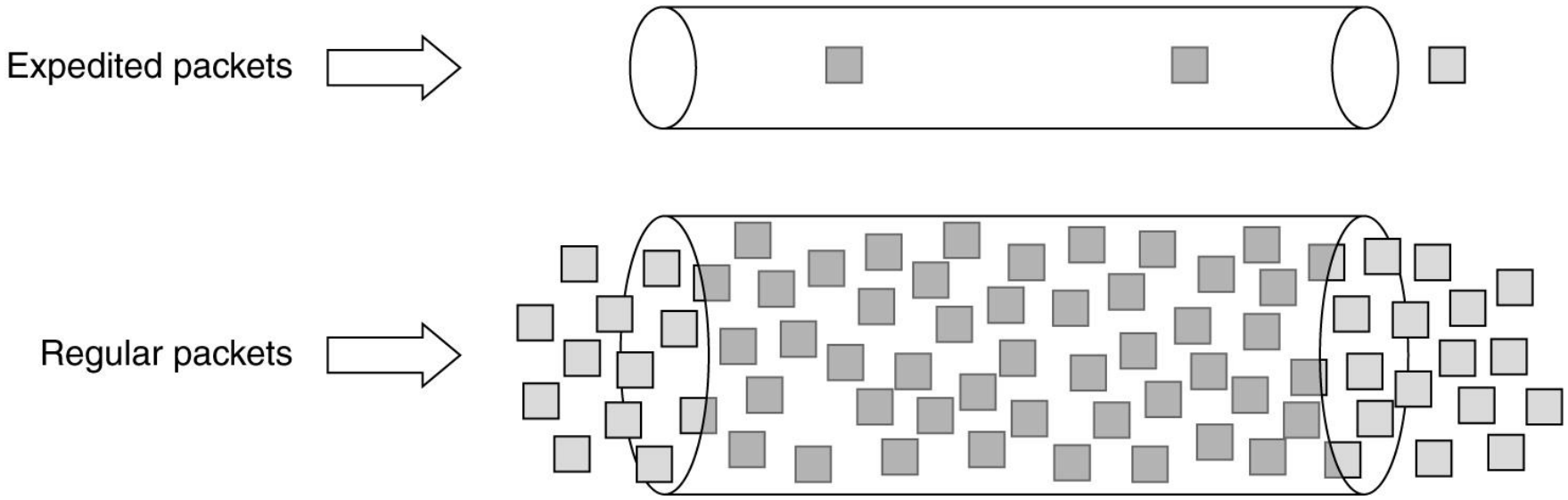
ALighter Approach to Ensure Required QoS

- IntServ is very powerful but has some severe drawbacks:
  - There is a setup phase, this incases delay in starting data flow.
  - Routers need to maintain ***per-flow state***. This approach is ***flow-based*** and not very scalable.
  - Complex router-to-router exchange of flow information.
- A simpler and approach was then designed by the IETF called, Differentiated Services (DiffServ).
- DiffServ takes a ***class-based*** (as opposed to IntSev flow-based) approach to ensure QoS

Differentiated Service (DiffServ)

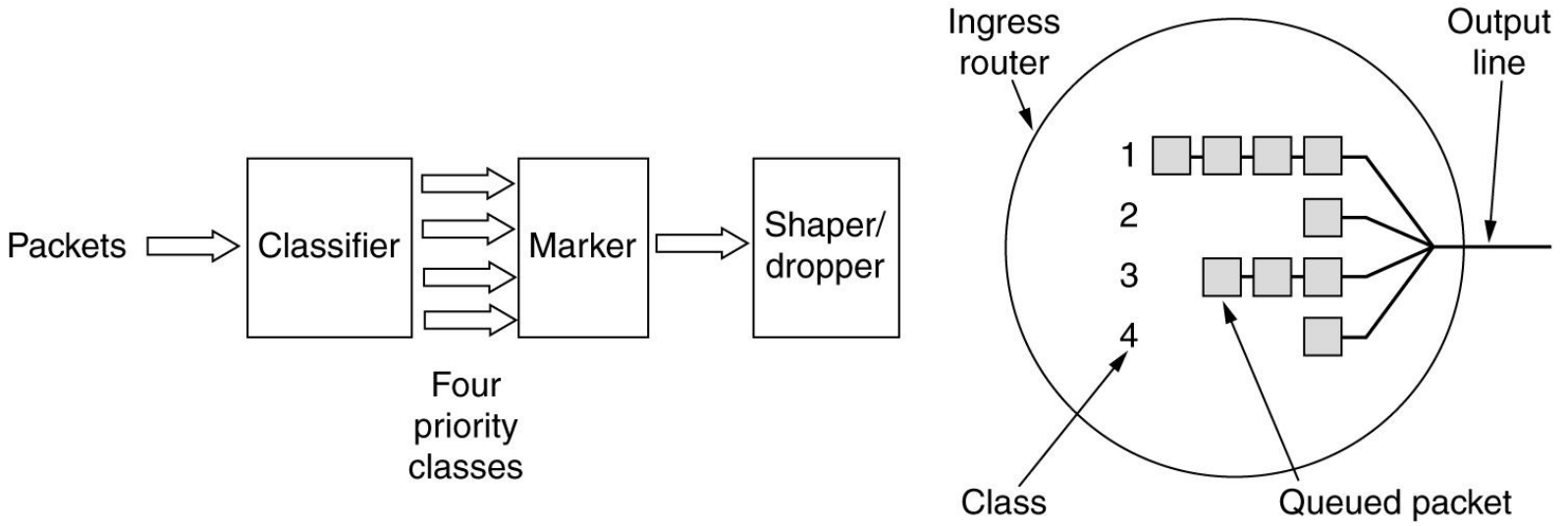
- Introduces ***services classes*** with corresponding ***forwarding rules***.
- Network operator can “sell” services. Every incoming packet carries a ***Type of Service*** field***.*** Depending on the service class of a packet, it may receive preferential treatment. The number of classes are decided by the network operator.
- Idea similar to overnight, two-day and surface delivery in courier services.
- Two simple classes are: Regular and Expedited.

Expedited Forwarding



Expedited packets experience a traffic-free network, e.g., if 10% of the traffic is expedited and 90% regular, 20% bandwidth is dedicated to expedited traffic.

Assured Forwarding



A possible implementation of the data flow for assured forwarding. There are 4 priority classes and 3 discard probabilities: low, medium, high.