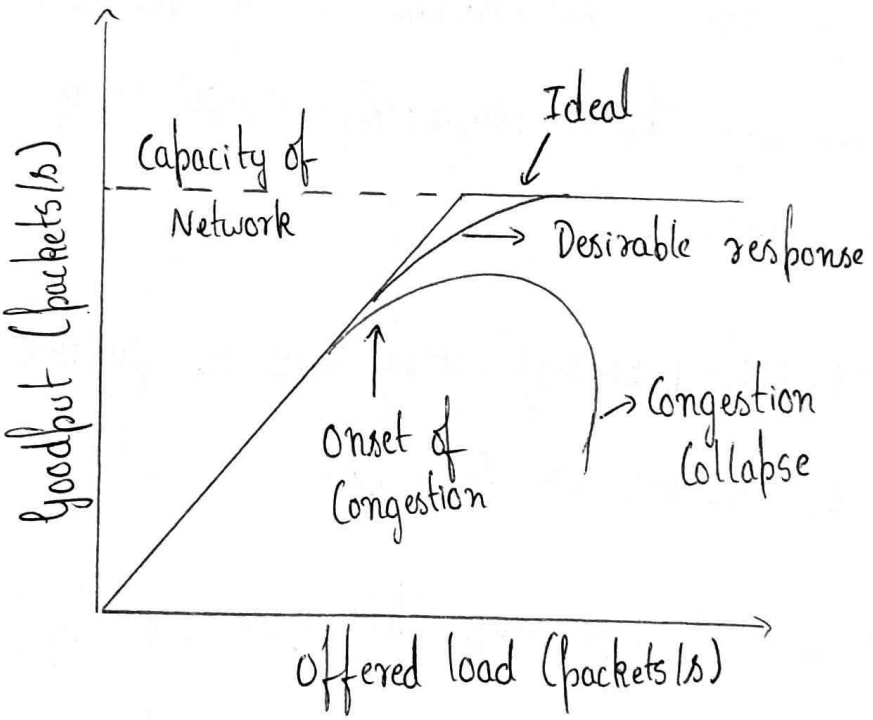
Unit-2 :- Congestion Control Algorithms

→ Congestion, the Need for Traffic Management :-

* The Network and the Transport layer share the responsibility to manage congestion.
* The most effective way is to reduce the load that the transport layer is placing on network. This requires both Transport and Network layer to work together.



* Traffic delivery in a network is proportional to the amount to traffic sent when network capacity is not exceeded.

* Congestion occurs as the offered load reaches network capacity, causing packet loss and increased latency.

* Congestion collapse can happen when increasing load leads to the reduced successful data delivery.

* It may occur due to delays inside the network rendering useless & duplicate packets.

* Goodput is a measure of rate at which useful packets are successfully delivered by network.

* Bufferbloat is the phenomena where network devices have more memory than required; which may harm network performance.

* Having excessive memory may lead to packet timeouts duplicates and congestion collapse.

* Operators can address network congestion by either shredding load & provisioning additional capacity.

⇒ Approaches to Congestion Control :-

① Network Provisioning :-

(*) The Primary way to prevent congestion is to build a sufficient capacity network for its expected load.

(*) Resources can be dynamically added to alleviate (reduce) congestion, such as activating spare routers (or) enabling back up lines

(*) Typically, heavily used routers and links are upgraded over months which is based on long term traffic needs.

② Traffic aware Routing :-

(*) To optimize network capacity, routes can be adjusted to accomodate changing traffic patterns throughout the day, such as shifting traffic away from congested paths.

(*) It involves real-time adjustments based on the conditions like road congestion, helping direct the network traffic efficiently.

(*) Splitting traffic across multiple paths can also help to distribute load and reduce congestion.

③ Admission Control:-

* It is a technique used in Virtual circuit networks that allows setting up a new circuit if and only if the network can handle the added traffic therefore preventing congestion

* When there is an anticipation of congestion, the new Virtual circuit is not setup to prevent the worsening of situation.

* The Determining of when a new circuit may add to congestion can be done using Characterization and Estimation

* Characterization is describing the traffic in terms of rate and shape which is challenging since traffic is bursty.

* Estimation is based on previous network behaviour and statistical analysis

④ Traffic Throttling:-

* When the congestion is about to happen, the network can provide feedback to sources responsible for congestion to slow down their sending rates.

* In this approach, identifying the onset of congestion is a problem. For this, routers can monitor parameters like average load, queing delay or packet loss to send feedback to sources.

⑤ Load Shredding :-

* Load Shredding is the strategy employed by routers where they drop the packets which they cannot handle due to congestion.
* The critical decision is to decide which packets to drop, and it may vary according to the application
* For File transfers, old packets are preffered over new ones because dropping older packets may lead to less data buffering.
* In contrast, in real-time media like audio or video newer packets are more valuable than older ones, as delay can render old packets useless.
* File transfer Policy is called Wine (Old wine better than new)
* Media Policy is called Milk (New Milk better than old)

⑥ Random Early Detection :- (RED)

- ⊛ Load Shredding can be implemented by discarding the packets earlier before buffer space is fully exhausted.
- ⊛ Hosts on internet can typically detect congestion through packet loss rather than explicit notification from routers.
- ⊛ Routers can exploit this by dropping packets early, giving senders time to react before the congestion becomes severe.
- ⊛ The Random Early Detection algorithm helps routers decide when to start discarding the packets.
- ⊛ Randomly dropping packets make it more likely that senders will experience the loss @ drops faster.
- ⊛ RED Routers generally perform better than other routers that only drop packets when the buffer is full.

⑦ Choke Packets :-

* The most direct way to notify a sender of congestion is to send a choke packet directly back to the source host. This packet contains destination information from congested packets.

* To avoid adding more load to network, the choke packets are sent at a low rate.

* When a source recieves a choke packet, it is required to reduce traffic sent to specified destination.

* Multiple choke packets can be sent to the same host and destination, but the host should ignore additional choke packets.

* The main issue in this approach is that delay is caused at router while generating choke packets and some bandwidth is consumed by these packets affecting the network.

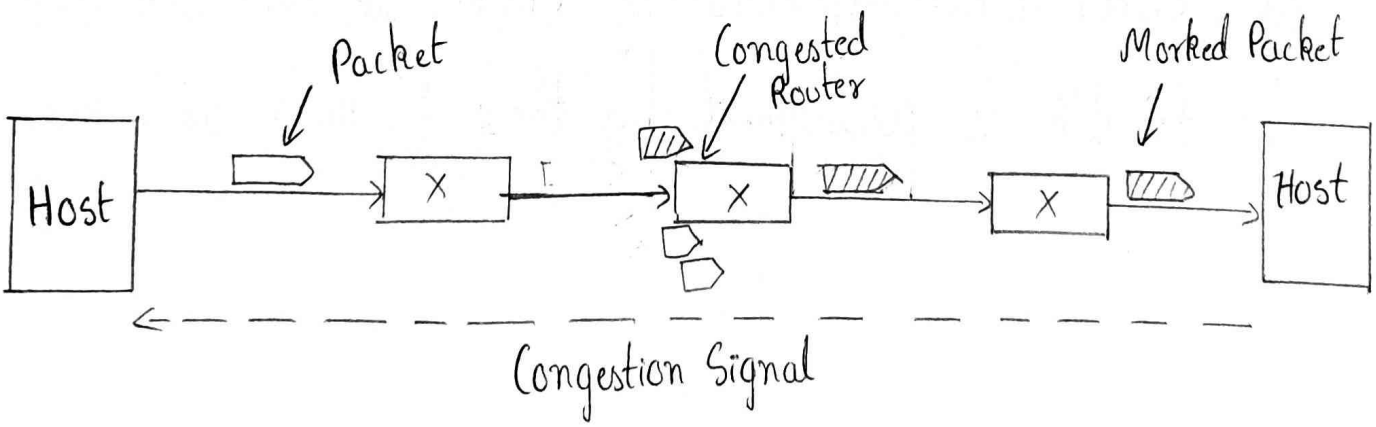
(8) Explicit Congestion Notification :- (ECN)

(*) Instead of generating additional packets to warn of congestion, routers can tag the packets by setting a bit in packet's header to indicate congestion.

(*) When this packet reaches destination, the destination can inform sender by sending an ECN with its reply packet.

(*) Two bits in Packet header are used to record if the packet experienced congestion.

(*) The packet starts from source unmarked, the routers mark these packets if they are passed through congested router. The destination echoes any congestion if marked by adding ECN in the reply packet. The sender on recieving ECN must throttle its transmission.



⑨ Hop by Hop BackPressure :-

* During Congestion, signals may take time to propogate especially over a large distance, many new packets will be transmitted before signal takes effect.

* To prevent this, make the choke packet take effect at every hop it passes through by signalling that hop to reduce transmission until the congestion is cleared providing immediate relief to congestion point.

* So, this approach prevents loss of packets at the congested router by reducing traffic into it.

⑩ Traffic Shaping :-

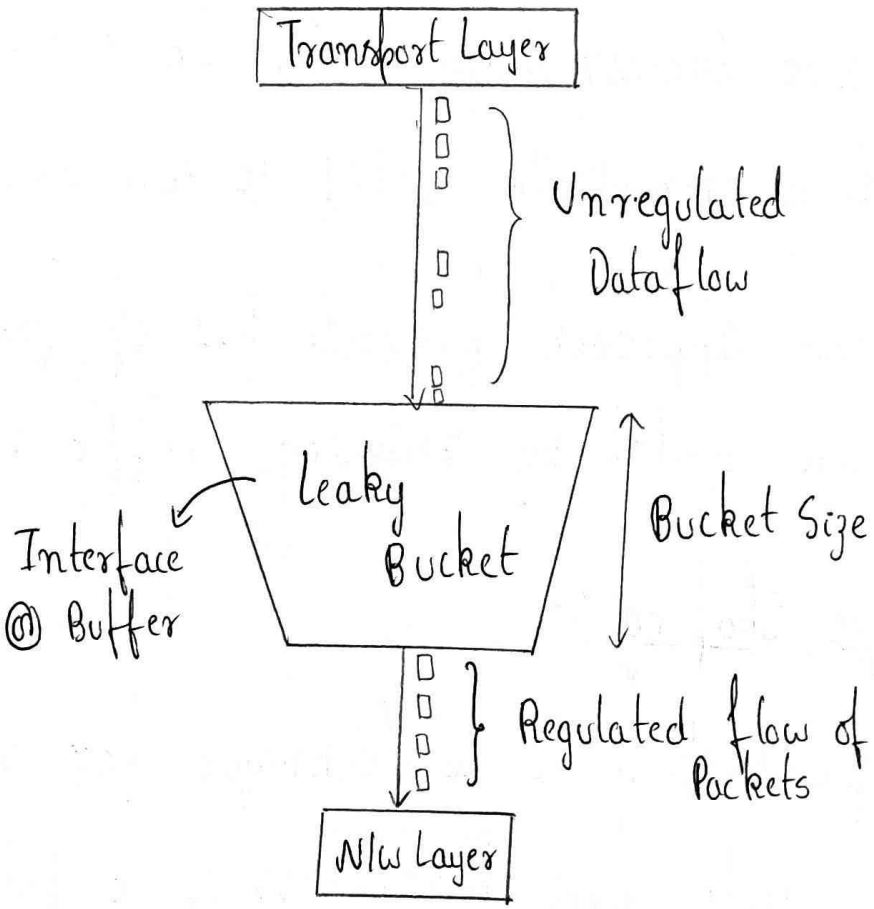
* Traffic shaping is a technique for regulating the average rate and burstiness of a flow of data that enters the network.

* Traffic Shaping reduces congestion and thus helps the network.

a) Leaky Bucket Algorithm :-

* The input rate of the packets may varg but the output rate remains constant.

* This algorithm smooths out bursty traffic and helps in maintaining uniform rate of data transmission inside the network.

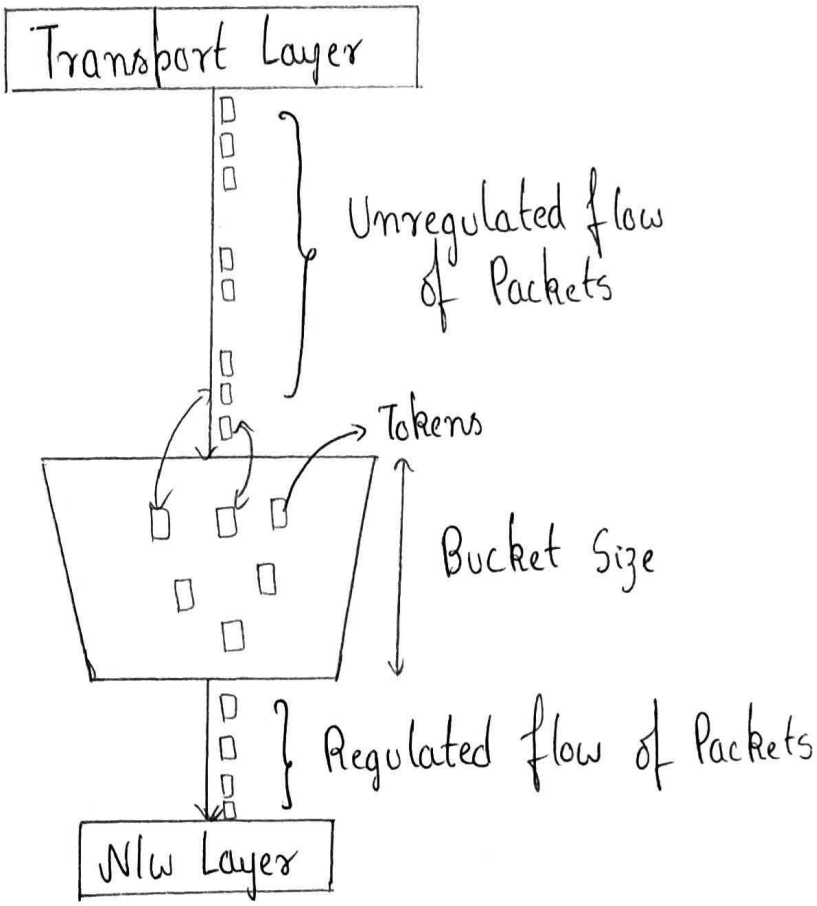


* To send a packet into the network, there must be space in bucket to accomodate it. If the bucket is full, then the packet is either queued (or) discarded.

b) Token Bucket Algorithm :-

* Similar to leaky bucket but tokens are generated in the bucket, when the packet arrives if sufficient tokens are present then they are exchanged but if not then the Transport layer fragments the Packets and then transmit them.

* The output rate is constant based on the analysis of capacity of the network layer on regular intervals.



* Both Transport and Network layer are supposed to be in constant communication for this algorithm.

⇒ Quality of Service :-

* The stream of packets from source to destination is called "Flow".

* Four primary parameters characterize the needs of each flow :-
  - (i) Bandwidth
  - (ii) Delay
  - (iii) Jitter
  - (iv) Loss

* These parameters ~~are~~ collectively determine the Quality of Service required by the flow.

* Different applications have different varying network needs.

* Network requirements are less demanding when application can improve on service provided by the Network.

* Applications differ in bandwidth needs, with file sharing and video requiring more bandwidth than email @ video.

* Delay sensitivity varies with applications :
  - -> Telephone have strict requirements
  - -> File transfer application are not delay-sensitive.

* Jitter is the variation in packet arrival times which is very crucial.

* Applications like video and audio are extremely sensitive to jitter, while others, such as file transfer are not.

* Some application like file transfer have more strict requirements on loss than audio and video.

* Retransmission of lost packets are considered wasteful in certain cases.

* The network may support different categories of QoS to accomodate various applications. such as:-

  - Bit rate (Ex:- Telephone)
  - Real-time variable bit rate (Ex:- Compressed video conferencing)
  - Non-real-time variable bit rate (Ex:- On demand video)
  - Available Bit rate (Ex:- File transfer)

=> Overprovisioning :-

* It involves building a network with ample capacity to handle any traffic without significant loss.
* It ensures low latency and optimal performance.
* The main disadvantage is its high cost since it effecitively solves network issues by heavily investing in infrastructure.
* It relies on expected traffic patters, so a sudden changes can disrupts its effectiveness.
* The Qaulity of Service (QoS) mechanisms offer an alternative to overprovisioning, allowing a network with less capacity to meet application requirement at a lower cost.
* These mechanisms enable networks to maintain performance gauranteas even during traffic spikes.
* No single technique can address all QoS issues so multiple techniques developed already are combined in practical QoS solutions.

* Four Key issues in ensuring QoS:-

(i) Identifying applications' network requirements

(ii) Regulating incoming traffic

(iii) Reserving resources at routers to gaurantee performance

(iv) Assessing the network capacity to handle additional traffic

* Two versions of QoS for internet:-

(i) Integrated Services

(ii) Differentiated Services.

⇒ Packet Scheduling Algorithms:-

* Regulating the flow @ shape of ordered traffic is crucial for providing performance guarantees in a network.

* To gaurantee this performance, sufficient resources need to be allocated along the path @ route taken by the packets through the network.

(*) The algorithms that allocate router resources among packets for a flow and competing flows are called Packet Scheduling algorithms.

-> The types of resources that need to be reserved :-

(i) Bandwidth :-

Ensuring that the outgoing line's capacity is not overloaded and bandwidth is reserved as needed.

(ii) Buffer Spaces :-

Reserving buffers to absorb bursts of traffic and prevent loss of packets.

(iii) CPU Cycles :-

Managing CPU time, as the router can only process a certain number of packets per second.

(*) The Packet Scheduling algorithms allocate bandwidth and other resources by determining which of buffered packets to send on output line next.

① First in First Out (FIFO):-

* It is the most straightforward scheduler used in routers.
* Packets are buffered in a queue for each output line and are sent in order they have arrived.

* Tail Drop:-

  In FIFO, when the queue is full, newly arriving packets are usually dropped. This is called Tail drop, since it involves dropping of newly arrived packets placed at end of queue.

* Alternative to Tail drop is Random Early Detection (RED) which randomly picks a newly arriving packet to drop when average queue length becomes very large.

* FIFO is not good when there are multiple flows, one flow can easily affect the performance of other flows.
* If the first flow is aggressive and sends a large burst of packets, they will lodge in the queue. The aggressive sender can hog most of the capacity of router making other flows starve.

② Fair Queueing :-

* To overcome the issue in FIFO of starvation, this algorithm is implemented.

* Routers have seperate queues for each flow for a given output line. When, the ~~flow~~ line becomes idle, the router scans the queues in round robin and takes the first packet on the next queue.

* This ensures that all flows get to send packets at same rate.

* The major flaw in this is it favours hosts using large packets over those using small packets by giving them more bandwidth.

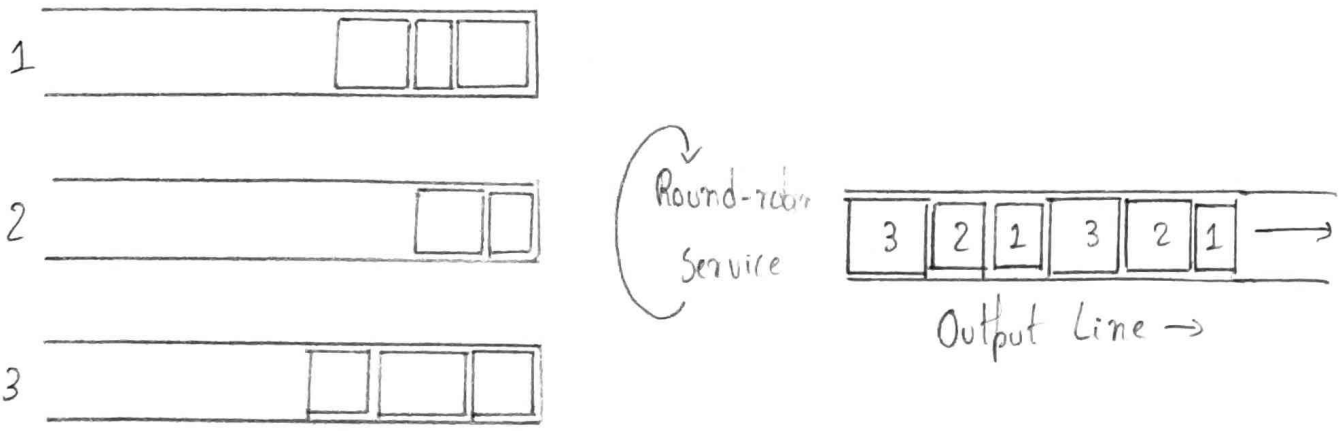
→ An Improvement (Byte-by-Byte Fair Queueing):-

* To prevent that issue an improvement of using Byte-by-Byte fair queueing was suggested.

* The improvement involves computing a virtual time representing the round at which each packet would finish being sent.

* Each round drains a byte from packets from all queues with data to send.

* Packets are sorted based on their finishing time and sent accordingly.



* Fair Queueing approximates the ideal byte-by-byte scheme by considering finish times.
* It does not preempt packets currently being transmitted.
* The sending order is based on finish time and fair queueing stays within one packet transmission of ideal scheme.
* The main limitation in fair queueing is that it assigns equal priority to all hosts which may not be ideal in certain situations where differentiated priorities are needed.

③ Weighted Fair Queueing :- (WFQ)

* WFQ addresses the priority issue by assigning different weights to flows.

* Formula for computing the finish time :-

$$F_i = \max(A_i, F_{i-1}) + L_i / W$$

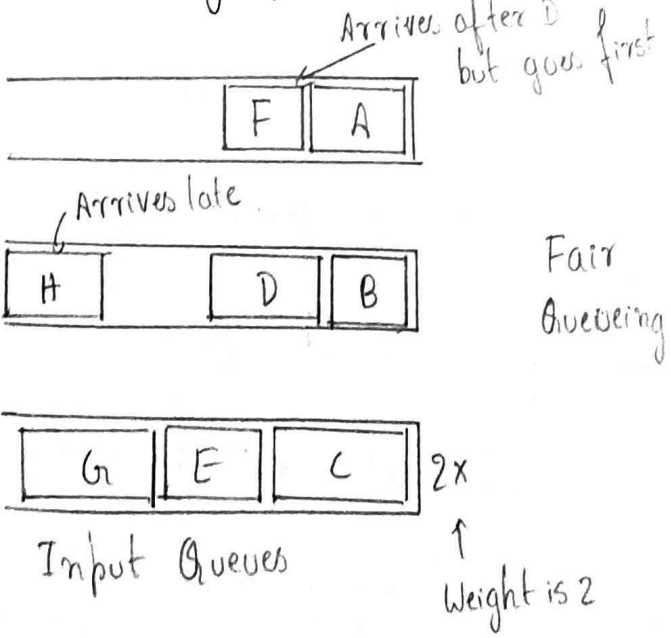
$F_i \rightarrow$ Finish time

$A_i \rightarrow$ Arrival time

$L_i \rightarrow$ Length of packet 'i'

$W \rightarrow$ Weight of flow i.e number of bytes per round.

* The WFQ's implementation complexity involves sorting packets by finish time, which can be challenging for many flows in high speed routers.



Fair Queueing

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

* The sorting takes O(logn) per each packet out of n packets but an alternative called Deficit Round robin was proposed by Shreedhar and Varghese where each packets takes O(1) time.

④ Priority Scheduling :-

* Each packet is marked with a priority and high-priority packets are sent before low-priority ones.

* i.e In a particular priority packets are sent in FIFO

* The main disadvantage is that a bursh of high priority packets can starve low priority packets and they will have to wait indefinitely.

* WFQ provides better alternative for this issue by adjusting weights. High priority queue are given larger weight, high priority packets will often go through a short line. Yet some packets of low priority will continue to be sent even if there is high traffic. This is essentially a two-Queue WFQ in which high priority has infinite weight.

(5) Timestamp - based Scheduling :-

* A Scheduler can use timestamps on packets to send them in timestamp order.
* Clark etal. described a design where the timestamp records how far the packet is behind @ ahead of schedule as it is sent through a sequence of routers on path.
* Packets that are queued behind other packets are tend to be behind schedule and the packets that have been serviced first are tend to be ahead of schedule.
* Sending packets in order of their timestamp has the effect of speeding up slow packets and at the same time slowing down the fast packets.
* This results that all packets are delivered by the network with a more consistent delay which is a good thing.

⇒ Integrated Services :-

* The Internet Engineering Task Force (IETF) dedicated efforts between 1995 and 1997 to develop an architecture for streaming multimedia.

* The outcome of this efforts resulted in over two dozen RFC's from RFC 2205 through RFC 2212. This collective work is called Integrated Services.

* The architecture was designed to cater both Unicast and Multicast applications.

⇒ RSVP - The Resource reSerVation Protocol :-

* The primary component of Integrated services visible to network users is RSVP.

* RSVP is detailed in RFC 2205 through 2210 and is used for making reservations in network.

* It enables multiple senders to transmit to multiple group of recievers, allowing individual recievers to switch channels freely.

- RSVP optimizes bandwidth utilization and eliminates congestion.
- RSVP employs multicast routing using spanning trees.
- Each group is assigned a group address and sender includes this address in its packets.
- The multicast routing algorithm builds a spanning tree covering all group members, with periodic multicast messages conveying additional information to routers.
- Recievers in a group can send a reservation message up the tree to sender for better reception and congestion elimination. This message is forwarded using reverse path forwarding Algorithm.
- At each hop, routers note the reservation and reserve necessary bandwidth.
- The bandwidth reservation is acheieved using a weighted fair queueing scheduler, if insufficient bandwidth is available system reports back a failure.

⇒ Differentiated Services:-

* The flow-based algorithms reserve resources along the route for one or more flows, offering good QoS
* But there are some disadvantages init like need for advance setup for each flow, scalability issues with thousands of flows, vulnerability to router crashes and complex router-to-router exchanges.
* To overcome this, IETF developed a QoS known as Class-based differentiated services, described in RFC 2474 and 2475.
* These services can be implemented locally in each router without advance setup.
* Differentiated services can be offered by a set of routers forming an administrative domain, the administration defines service classes with corresponding forwarding rules.

⊛ The customer packets entering the domain are marked with specific class they belong to in differentiated services field of IPV4 and IPV6 packets.

⊛ Classes are defined as per-hop behaviours, indicating the treatment packets will recieve at each router.

⊛ Premium service may be provided to packets with specific per-hop behaviours.

⊛ Traffic within a class may be required to conform to specific shapes such as a leaky bucket with specified drain rate.

⇒ Expedited Forwarding :-

⊛ It is one of the network-independent classes defined by IETF ~~in~~ described in RFC 3246.

⊛ There are 2 classes of service, regular and expedited

⊛ The majority of traffic is expected to be regular but a limited fraction of packets are expedited. Expedited packets should traverse the network as if no other packets were present ensuring low loss, jitter and delay.

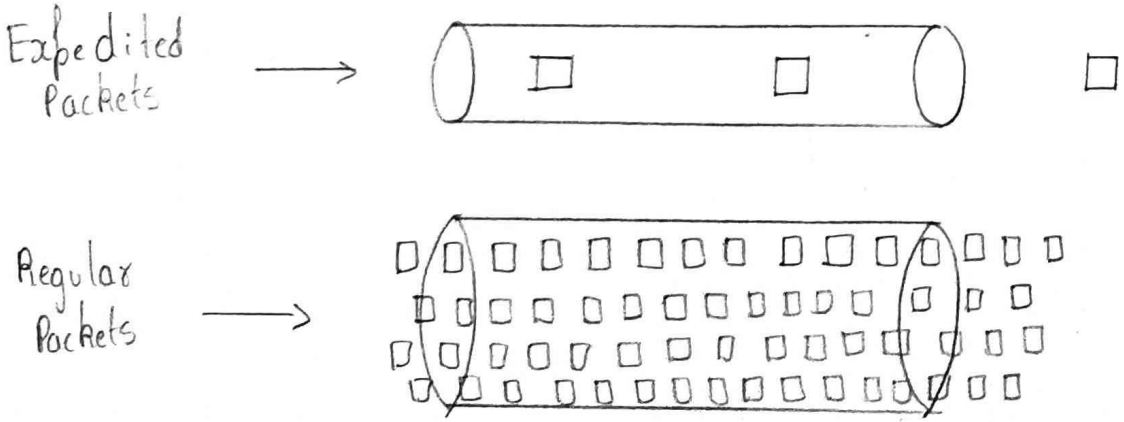
⊛ One way to implement expedited forwarding is to classify packets as expedited or regular and mark them accordingly.

⊛ Classification can be done on the sending host in the ingress router.

⊛ Host-based classification benifits from more information about packet flows, potentially done by networking software or the operating system.

⊛ VoIP (Voice Over IP) packets are commonly marked for expedited service by hosts.

⊛ If the host marks the packets, the ingress router may police the traffic to ensure customer do not send more expedited traffic than they have paid for.



⊛ Within the network, the routers may have 2 output queues for each outgoing line - one for expedited and one for regular packets.

⊛ The expedited Queue is prioritized, possibly using a priority scheduler, allowing expedited packets to experience an unloaded network even during heavy regular traffic loads.

⇒ Assured Forwarding :-

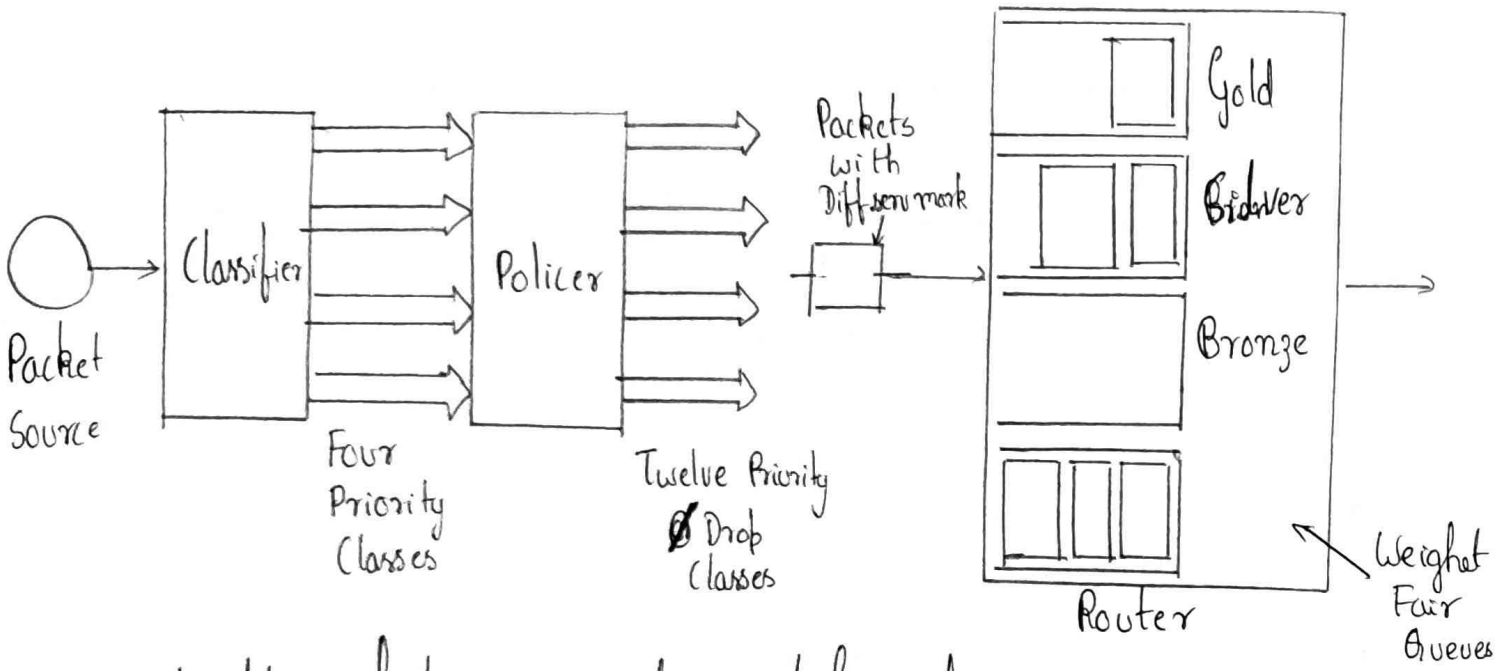
⊛ Assured forwarding is a more complex scheme for managing service classes detailed in RFC 2597.

⊛ It defines 4 priority classes with their own resources, named gold, silver, bronze and default class.

⊛ Additionally it specifies three discard classes for packets experiencing congestion : low, medium & high resulting in 12 service classes.

⊛ The first step is to classify the packets into one of 4 priority classes, which can be done on sending host @ ingress router.

* The next step is determining the discard class for each packet.



* A traffic policer, such as token bucket is used to identify packets fitting with small bursts as low discard those exceeding small bursts as medium discard and those exceeding large bursts as high discard.

* The combination of priority and discard class is then encoded in each packet.

* The routers in network process packets using a scheduler like WFQ with higher class given higher weights.

* Within a priority class, the packets from higher discard class can be preferentially dropped using RED.

* RED starts dropping packets as congestion builds, providing space to accept low discard packets while dropping high discard packets.

→ Differentiating Networks :-

* The differences in networks such as transition from Ethernet to Cellular can cause delays and overheads.

→ Some of the many ways network can differ :-

(i) Services offered :- Connectionless v/s Connection oriented

(ii) Addressing :- Different sizes, flat @ heirarchial, 32/128 bits
IPV4 @ IPV6

(iii) Broadcasting & Multicasting :- Present @ Absent

(iv) Packet Size :- Every network has its own maximum
Ethernet → 1500 MTU, Wifi :- 2272 MTU
MTU → Maximum Transmission Unit

(v) Ordering :- Ordered @ Unordered delivery

(vi) Quality of Service :- Present @ Absent. Which kind is present

(vii) Reliability :- Different network have different levels of loss

(viii) Security :- Privacy rules, encryption etc...

(ix) Parameters :- Different timeout, different flow specification etc...

(x) Accounting :- By connect time, packet @ byte @ not at all.

⇒ Packet Fragmentation :-

(*) Due to various limitations, each network has a maximum packet size limits. Ex :- Ethernet (1500 bytes), 802.11 (2272 bytes) and IP (65,515 bytes).

(*) Every network ensures that large packets do not encounter issues by determining Path Maximum Transmission Unit (Path MTU) dynamically.

(*) Source sends packets with headers indicating no fragmentation routers generates errors if MTU is exceeded.

(*) Source adapts size based on error feedback to match the current path MTU.

→ Transparent Fragmentation :-

* Router breaks up oversized packets into packets and reassembles them at common exit router.
* Requires end router to be aware of all fragments potentially limiting routing flexibility.
* May involve significant work for the router in buffering and managing fragments

→ Non - Transparent Fragmentation :-

* Routers treat each fragments as an original packet and reassembles only at destination host.
* Reduces workload on routers but can lead to higher overhead and potentiall issues with packet loss.