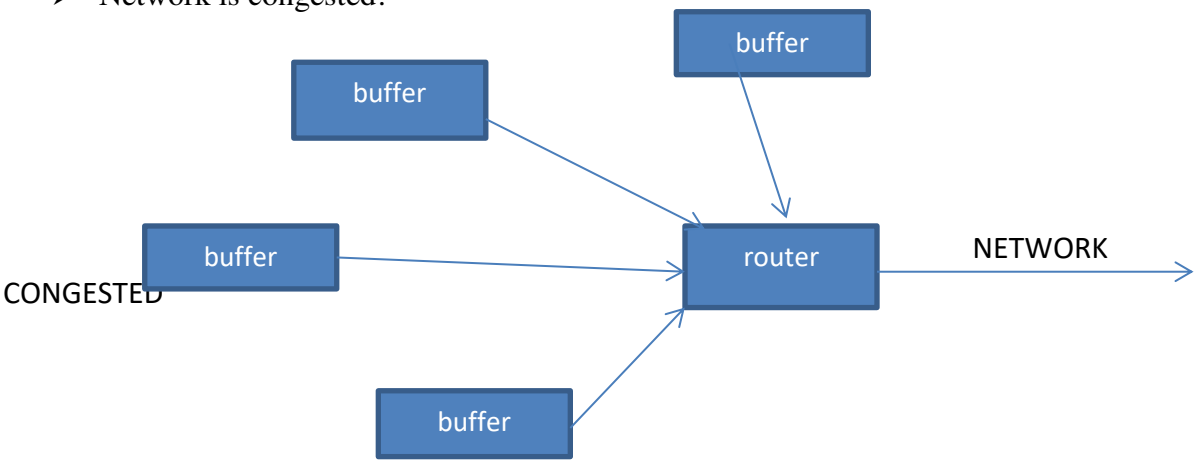
WHAT IS CONGESTION?

Congestion is a situation in communication network in which too many packets are present in a part of the subnet or network so that the

- The queue overflows
- Packets get dropped
- Network is congested!



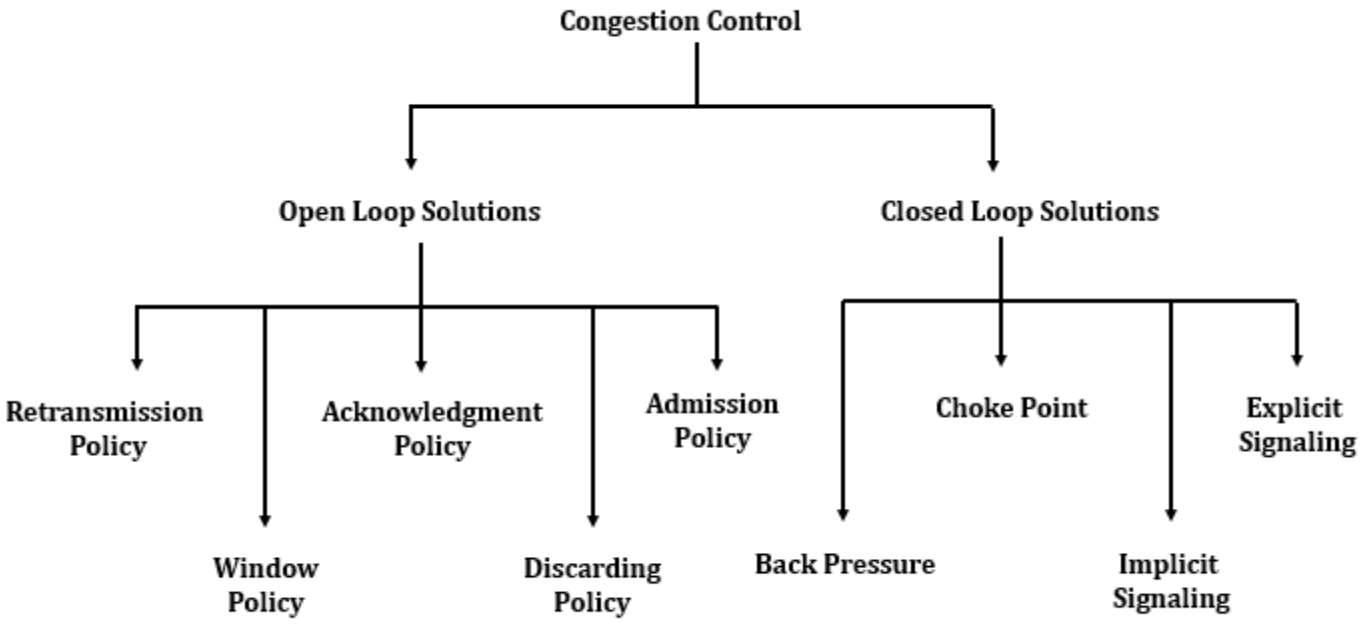
Factors that Cause Congestion

- Packet arrival rate exceeds the outgoing link capacity.
- Insufficient memory to store arriving packets
- Bursty traffic
- Slow processor
- Low Bandwidth
- Multicasting
- Artificial Congestion
- Border Gateway Protocol
- Bad Configuration Management
- Outdated Hardware
- Adding Retransmitting Hubs

Costs of congestion

- large queuing delays
- unneeded retransmissions by the sender

Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Open loop congestion Prevention mechanism

In this method, policies are used to prevent the congestion before it happens.

Congestion control is handled either by the source or by the destination.

1. Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

.

2. Window Policy

• To implement window policy, selective reject window method is used for congestion control in which it sends only the specific lost or damaged packets.

3. Acknowledgement Policy

• If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.

4. Discarding Policy

- A router may discard less sensitive packets when congestion is likely to happen

5. **Admission Policy**

- A router can deny establishing a virtual circuit connection if there is congestion

6. **Routing Algorithm**

- spreading the traffic over all the lines

Closed Loop Congestion Control Mechanism

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

Back Pressure Method: It is a node to node congestion control mechanism. In this method, congested node sends a feedback to its immediate sender indicating congestion.

Choke Packet: In this method, congested node directly sends a feedback to the source saying that there is congestion and source needs to slow down sending packets.

CONGESTION CONTROL IN TCP:

TCP must define policies:

- Accelerate (increase) the data transmission when there is no congestion in the network.
- Decelerate (decrease) the transmission when there is congestion in the network.

Hence TCP defines another variable called CONGESTION WINDOW, cwnd, whose size is controlled by the congestion situation in the network.
Now 'rwnd' and 'cwnd' both control the size of the window in TCP.
Rwnd= controls congestion at the end.(Receiving Window)
Cwnd= controls congestion in the middle.(Congestion Window)
Hence:
Actual window Size=minimum (rwnd , cwnd)

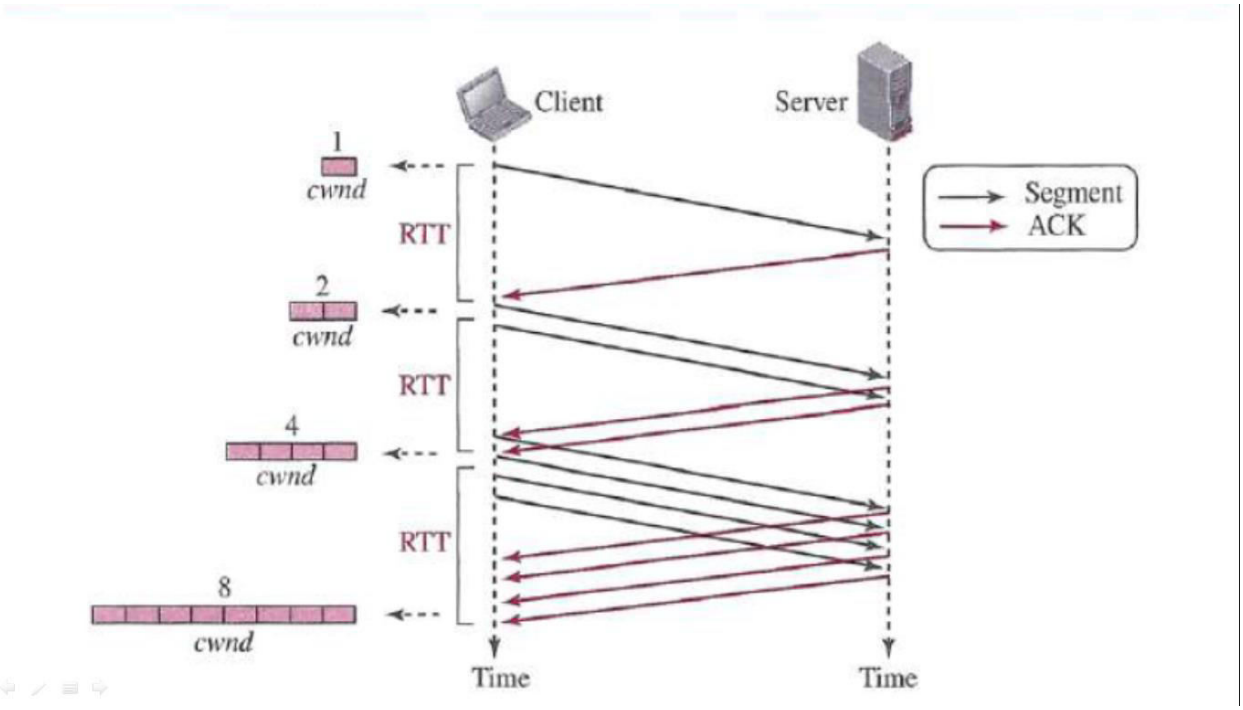
Congestion policies in TCP

Three ALGORITHMS :

- Slow Start
- Congestion Avoidance
- Congestion detection

Slow start: Exponential Increase

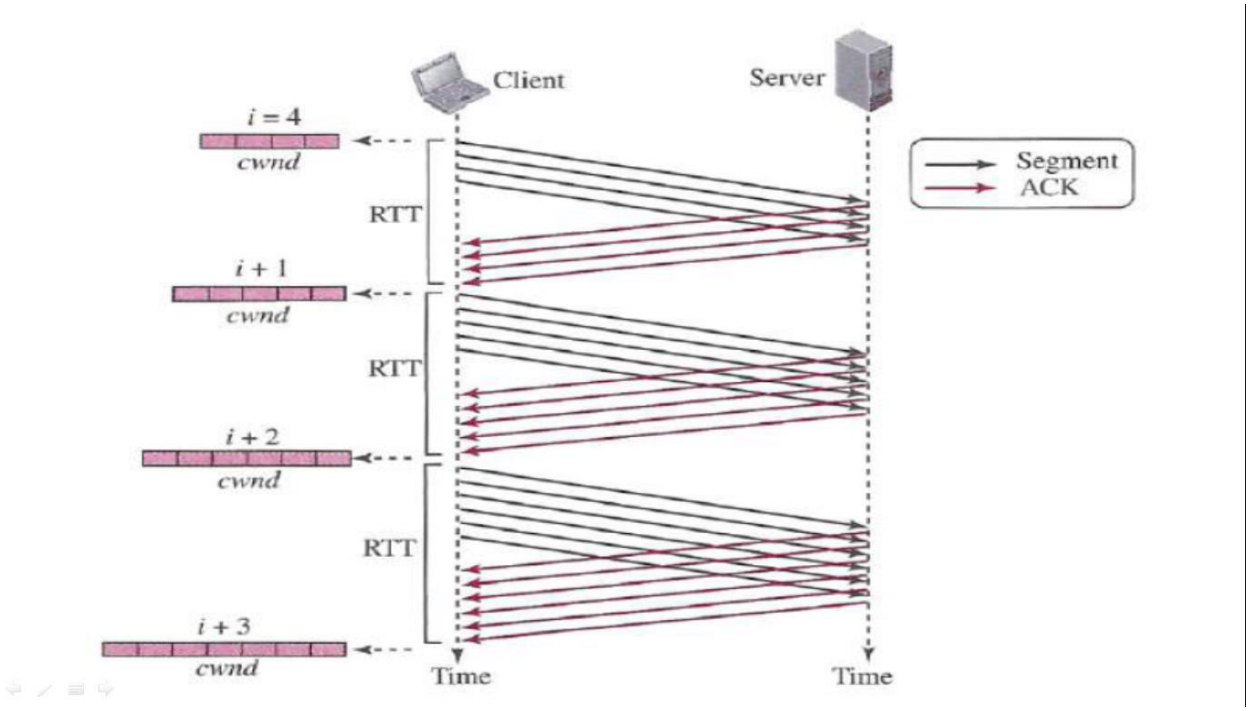
- When a new connection is established the congestion window is **initialized to one MSS**(Maximum Segment Size).
- Each time an ACK is received, the congestion window is **increased by one MSS**.
- The sender can **transmit up to the minimum of the congestion window** and the advertised receiver window size.
- Thus, the size of **congestion window increases exponentially** until a threshold value is reached.



Congestion avoidance: additive increase

IN this case when connection is established ,

- connection window is initialized to 1 MSS.
- Cwnd is incremented by 1 only when the acknowledgement for all the segments has arrived.



In the congestion avoidance algorithm, the size of the congestion window increases additively until congestion is detected.
PROBLEM: Slow data transmission.
BENEFIT: Linear growth rate so more conservative and reliable.

Congestion Detection:
Two events indicate congestion in a network

- Time-Out (Retransmission Trip Time)
- Three Duplicate ACKs.

Time-Out: If TCP sender do not receive ACK for a segment or a group of segments before time-out occurs, it assumes that the corresponding segment or segments are lost and loss is due to congestion. Sign of strong congestion in the network.
Three Duplicate ACKs: Means four ACKs with same acknowledgment number. When TCP sends three duplicate ACKs it is the sign of the missing segment which can be due to congestion in the network. But weak congestion.

Congestion control in Datagram Subnets

- Each line has a real variable, u, whose value between 0.0 and 1.0 reflects the recent utilization of that time.
- When u moves above the threshold the output line enters a **warning** state

The Warning Bit

- The warning state is set as a special bit in the packet's header.
- As long as the router was in the warning state, it continued to set the warning bit

- As long as the warning bit is set, the source continued to decrease its transmission rate.

Choke Packets

- In the warning state, the router sends a choke packet back to the source host.

QUALITY OF SERVICE(QOS)

Quality of service (**QoS**) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network.

QoS refers to traffic control mechanisms that seek to either differentiate performance based on application or network operator requirements, or provide predictable or guaranteed performance to applications, sessions, or traffic aggregates.

Flow Characteristics(QoS parameter)

Reliability

Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgment, which entails retransmission.

Capacity of the **network** to offer the same services even during a failure.

Delay

Delay is the latency in the arrival of packets from source to destination.

latency is the term used to indicate any kind of delay that happens in data communication over a network

Jitter

Jitter is the variation in delay for packets belonging to the same flow. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time. On the other hand, if the above four packets arrive at 21, 23, 21, and 28, they will have different delays: 21,22, 19, and 24.

Bandwidth

Bandwidth is also the amount of data that can be transmitted in a fixed amount of time.

Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

TECHNIQUES TO IMPROVE QoS

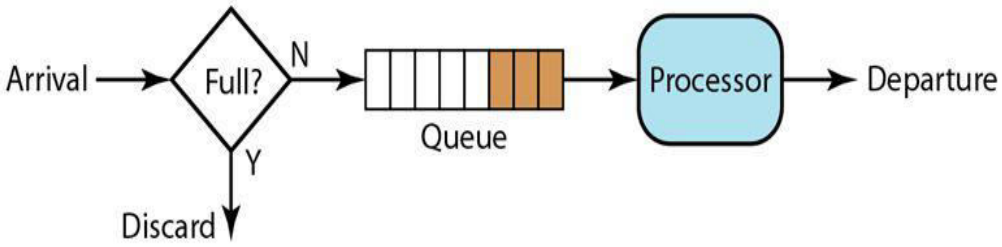
Overprovisioning

is the solution to provide so much router capacity , buffer space and bandwidth that the packets just fly through network easily.

Buffering

flows can be buffered at the receiver before being delivered.

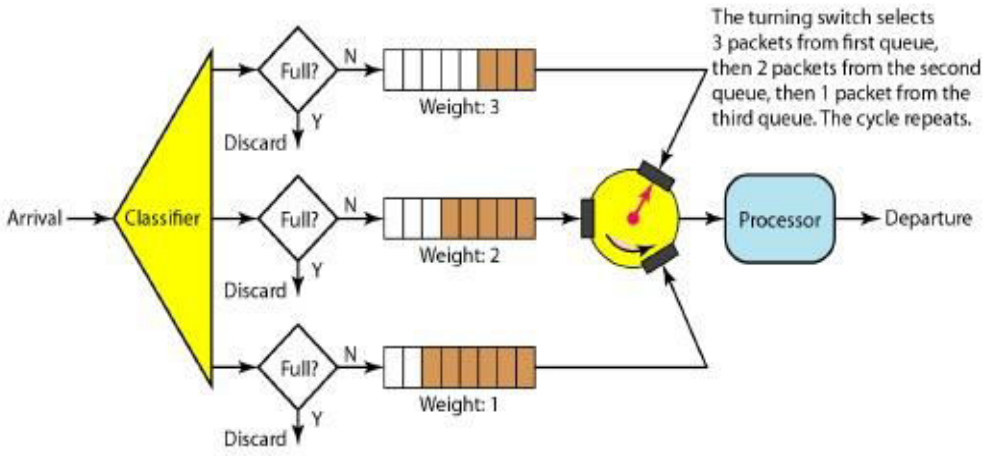
Scheduling: *First In First Out - FIFO queuing*



- In FIFO, packets wait in a buffer (queue) until the node is ready to process them.
- If the average arrival rate is higher than the average processing rate, the queue will fill up and new arriving packets will be discarded. (Just like queuing for bus scenario).

Weighted Fair Queuing

- The queues are weighted based on the priority of the queues
- The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the weight



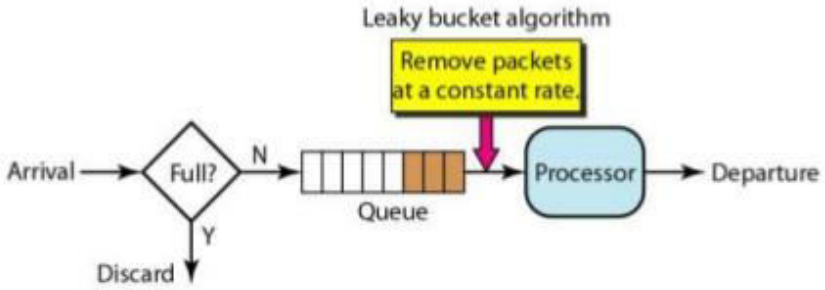
Traffic Shaping

Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket.

Leaky Bucket

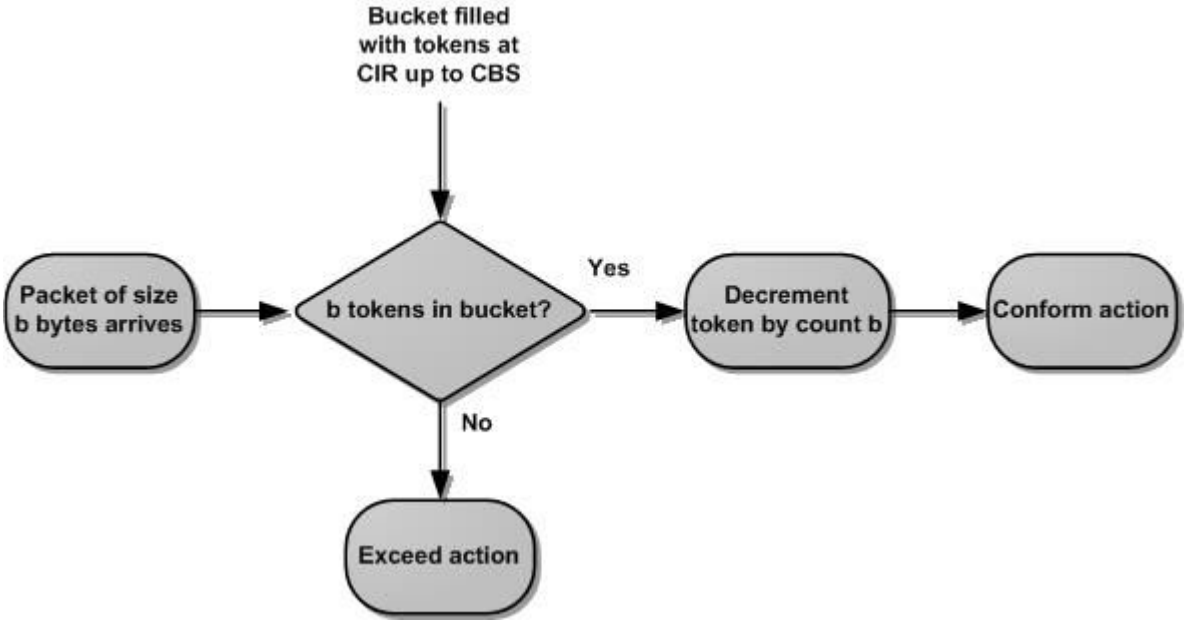
If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

Leaky Bucket Implementation



- Algorithm for variable-length packets:
  1) Initialize a counter to n at the tick of the clock
  2) If n is greater than the size of the packet, send packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size
  3) Reset the counter and go to step 1

TOKEN BUCKET ALGORITHM:



The token bucket allows bursty traffic at a regulated maximum rate.

Algorithm:

For each tick of the clock, the system sends *n* tokens to the bucket.
The system removes one token for every byte of data sent. For example, if *n* is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume these tokens for sending up to data of 10,000bytes.

Resource Reservation

A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The quality of service is improved if these resources are reserved beforehand.

RSVP(RESOURCE RESERVATION PROTOCOL)

The Resource Reservation Protocol (RSVP) is a signaling protocol to help IP create a flow and consequently make a resource reservation.

- *RSVP Messages*
  RSVP has several types of messages. However, for our purposes, we discuss only two
  of them: **Path** and Resv

1. **Path** Messages
   A Path message travels from the sender and reaches all receivers in the multicast path. On the way, a Path message stores the necessary information for the receivers.

2. **Resv** Messages
   After a receiver has received a Path message, it sends a *Resv* message.
   The Resv message travels toward the sender (upstream) and makes a resource reservation
   on the routers that support RSVP.

Reservation Styles

When there is more than one flow, the router needs to make a reservation to accommodate all of them. RSVP defines three types of reservation styles.

- Wild card filter
- Fixed filter
- Shared explicit filter

Wild Card Filter Style In this style, the router creates a single reservation for all senders.

Fixed Filter Style In this style, the router creates a distinct reservation for each flow. This means that if there are *n* flows, *n* different reservations are made.

Shared Explicit Style In this style, the router creates a single reservation which can be shared by a set of flows.

Admission Control

Admission control refers to the mechanism used by a router to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of

bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.

FUNCTIONS OF IPQoS

classification

process of distinguishing between packets belonging to different classes of service and for sending packets to appropriate path of handling.it is done by a classifier.

policing

process of monitoring contracted traffic profile.

scheduling

manages access to the link when more than one packet in the queues. It is done by a scheduler.

shaping

shape traffic, if it is needed. It is done by a shaper. A shaper uses the information received from the meter to reshape the traffic if it is not compliant with the negotiated profile.

Admission control

Admission control refers to the mechanism used by a router to accept or reject a flow based on predefined parameters called flow specifications.

INTEGRATED SERVICE

Integrated Services, sometimes called IntServ, is *a flow-based* QoS model, which means that a user needs to create a flow, a kind of virtual circuit(path), from the source to the destination and inform all routers of the resource requirement.

Key Features of IntServ

- Reserve Resources-> A router must know what amount of resources has to be reserved for any packet flow at a time.
- Call setup(call Admission): Call setup includes the following steps,

Signaling

The integrated service uses a signaling protocol for making a reservation of the resources required. This protocol is called Resource Reservation Protocol (RSVP).

Flow Specification

When a source makes a reservation, it needs to define a flow specification. A flow specification has two parts: Rspec (resource specification) and Tspec (traffic specification). Rspec defines the resource that the flow needs to reserve (buffer, bandwidth, etc.). Tspec defines the traffic characterization(data amount and rate) of the flow.

Admission

After a router receives the flow specification from an application, it decides to admit or deny the service.

Service Classes

Two classes of services have been defined for Integrated Services: guaranteed service and controlled-load service.

Guaranteed Service Class This type of service is designed for real-time traffic that needs a guaranteed minimum end-to-end delay.

Controlled-Load Service Class This type of service is designed for applications that can accept some delays

Problems with Integrated Services

- Scalability
- Service-type limitation.

DIFFERENTIATED SERVICE

Differentiated Services is a class-based QoS model designed for IP. It has the ability to handle different "classes" of traffic in different ways within the internet.

The Diffserv architecture consists of two sets of functional components:

Edge Function (Packet Classification and traffic Conditioning): At the incoming edge of the network, the arriving packets are marked with some value in the DS field of packet header. The mark that a packet receives identifies the class of traffic to which it belongs.

Core Function (Forwarding): When a DS-marked packet arrives at the Diffserv-capable-router, the packet is forwarded to the next hop according to the so-called per-Hop behavior.

Per-Hop Behavior Per-Hop behavior is defined as the "externally observable forwarding behavior of the Diffserv-capable nodes". So far two PHBs are defined:EF PHB, and AF PHB.

EF PHB The EF PHB (expedited forwarding PHB) provides the following services:

Low loss

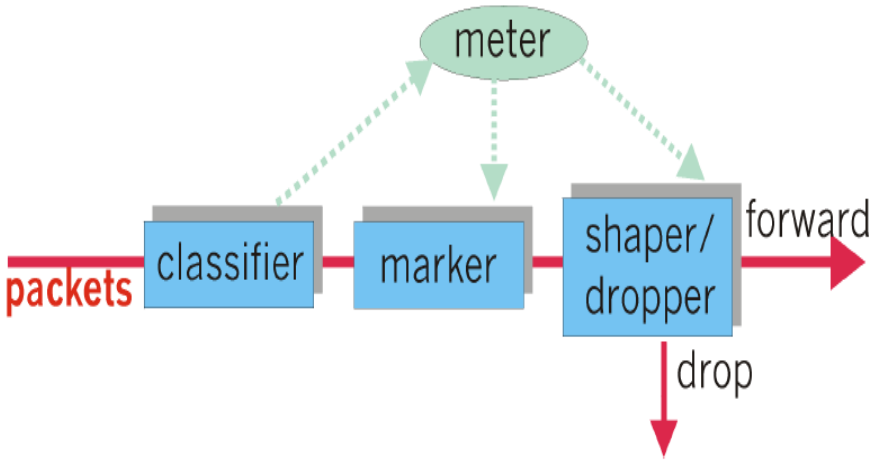
Low latency

Ensured bandwidth

AF PHB (assured forwarding PHB) delivers the packet with a high assurance as long as the class traffic does not exceed the traffic profile of the node.

Traffic Conditioner

To implement diffserv, the OS node uses traffic conditioners such as meters, markers, shapers, and droppers.



Classifier it classifies the type of service class specified in a packet.
Meters The meter checks to see if the incoming flow matches the negotiated traffic profile. The meter also sends this result to shaper.
Marker A marker can remark a packet that is using best-effort delivery or down-mark a packet based on information received from the meter. Down marking occurs if the flow does not match the profile.
Shaper A shaper uses the information received from the meter to reshape the traffic if it is not compliant with the negotiated profile.
Dropper A dropper discards packets if the flow severely violates the negotiated profile.

Difference between integrated service and differentiated service.

Integrated service	Differentiated service
It is a flow-based service	It is a class based service
It has service type limitation.	It doesn't have service type limitation.
Main processing lies on the core of the network	Main processing lies on the edge of the network
It has scalability issue	It solves the scalability issue by having per flow specification rule.