IIT KHARAGPUR

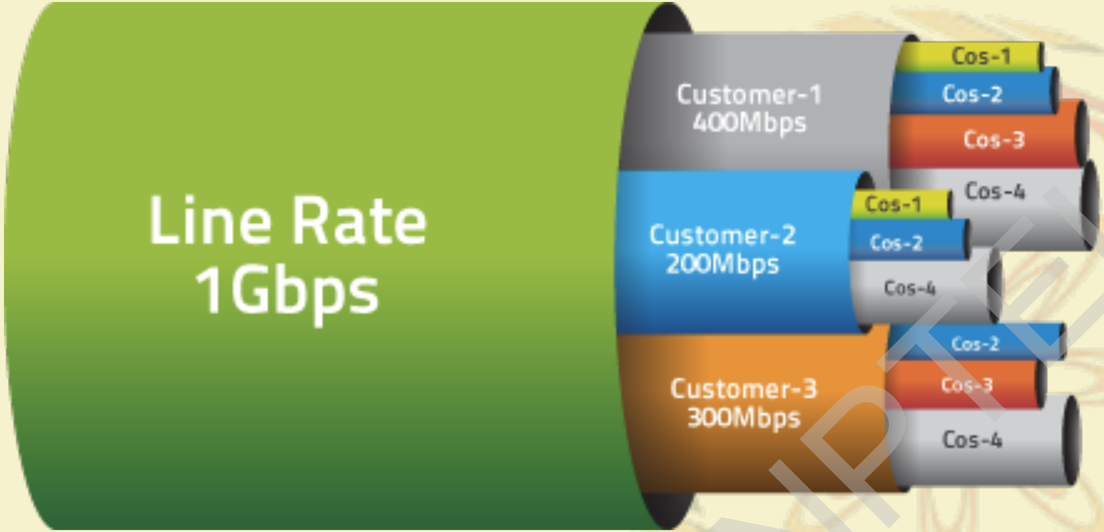
NPTEL ONLINE CERTIFICATION COURSES

NPTEL

COMPUTER NETWORKS AND INTERNET PROTOCOLS

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR



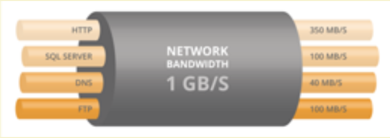
Internet QoS

What is QoS

Revisiting Congestion

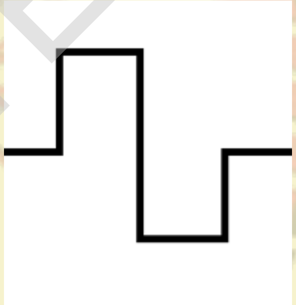
- Does TCP Congestion Control ensure NO CONGESTION in the network?

- How does congestion impact network performance?



Bandwidth

Delay



Jitter

Loss

Network Bandwidth

- Amount of data that can be transmitted over a link within a fixed amount of time.
- "*When a drain chronically runs slow even though it isn't plugged, it's time to get a bigger pipe.*" – QoS vs more bandwidth, by Tim Greene
- Some applications in the network are bandwidth hungry – video applications; congestion limits per user bandwidth.
- Improve bandwidth – design networks with high capacity

Delay

- Three components – (a) **transmission delay**, (b) **propagation delay,** (c) **queueing delay**
- **Transmission Delay**: Amount of time to push all the packet bits in the network. Bandwidth 8 Mbps, Packet size (including headers) 1 MB, Transmission delay?
- **Propagation Delay:** Time to transfer one bit from one end of the link to another end of the link; usually depends on the underlying communication media
- **Queuing Delay:** Delay at the interface buffer; the major delay component

Delay

- In general,

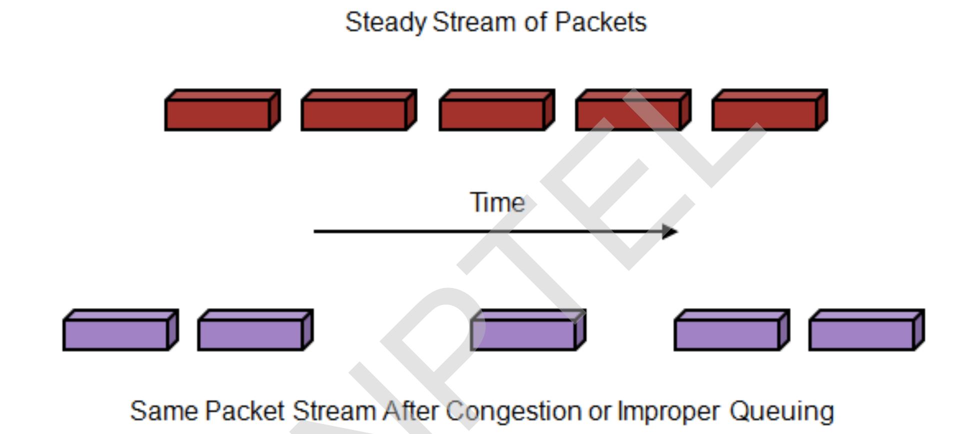
  Queuing delay >> Transmission delay + Propagation delay

- Packet multiplexing in the network devices (like routers, switches) impact the queuing delay

- Impact of congestion – increase in queuing delay

Jitter

- Variation in End to End delay



- Why jitter impacts application performance – video streaming; consider delay variation among different video frames

Loss

- A relative measure of the number of packets (or segments or bits) that were not received compared to the total number of packets (or segments or bits) transmitted.

- Loss is a function of availability
  - If the network is available (capacity more than the demand) then loss would be generally zero (**Note: This assumption is not true for wireless networks)**

- Congestion increases data loss from the intermediate network devices

Application QoS

- Different application requires different level of QoS – delay, jitter and bandwidth

	Loss	Delay (One-way)	Jitter	Bandwidth
Voice	$\leq 1\%$	$\leq$ 150ms	$\leq$ 30ms	21 Kbps - 320 Kbps
Interactive Video	$\leq 1\%$	$\leq$ 150ms	$\leq$ 30ms	On demand
Streaming Video	$\leq 5\%$	$\leq$ Buffer time	On buffer time	On demand
Data	-	-	-	Best Effort

Source: http://www.ciscopress.com/articles/article.asp?p=357102

A Formal Definition of QoS

"Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal 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. "

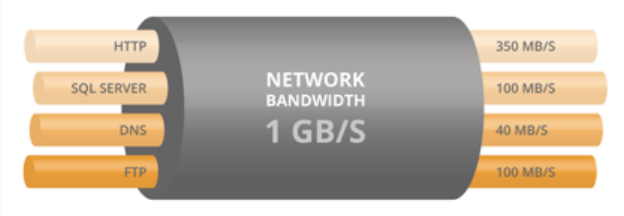
Source: Cisco - http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

Ensure QoS over a Packet Switching Network

- What applications need from the network
- How to regulate the traffic that enters the network
- How to reserve resources at router to guarantee performance
- Whether the network can safely accept more traffic

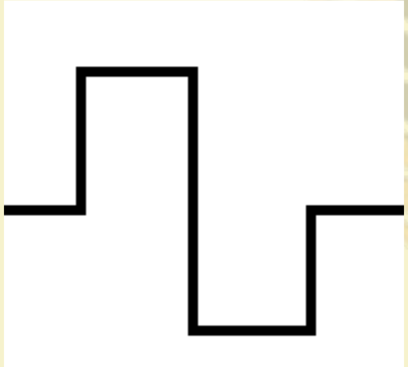
Section 4, Chapter – THE NETWORK LAYER, Computer Network by Tanenbaum

Primary QoS Parameters



Bandwidth

Delay



Jitter

Loss

Flow

- A stream of packets from a source to a destination is called a **flow.**

- Source to Destination:
  - Machine to Machine
  - Process to Process
  - Application to Application
  - Socket to Socket

- Different flows require different levels of QoS

Why QoS is Considered at the Network Layer

- Maintaining QoS requires both per-hop and end-to-end behavior

- End-to-end performance needs to be monitored
  - End-to-end delay
  - End-to-end bandwidth
  - End-to-end jitter
  - Total end-to-end data loss

Why QoS is Considered at the Network Layer

- However, resource reservation needs to be on per-hop basis – otherwise end-to-end requirements can not be guaranteed

- Network layer bridges end-to-end (Transport) and Per-hop (Data Link Layer)

Application Classes based on QoS

- Constant bit rate (e.g. telephone applications – VoIP)
- Real time variable bit rate (e.g. videoconferencing)
- Non real-time variable bit rate (e.g. on demand video streaming – IPTV)
- Available bit rate or Best effort (e.g. File transfer)

thank you!

IIT KHARAGPUR

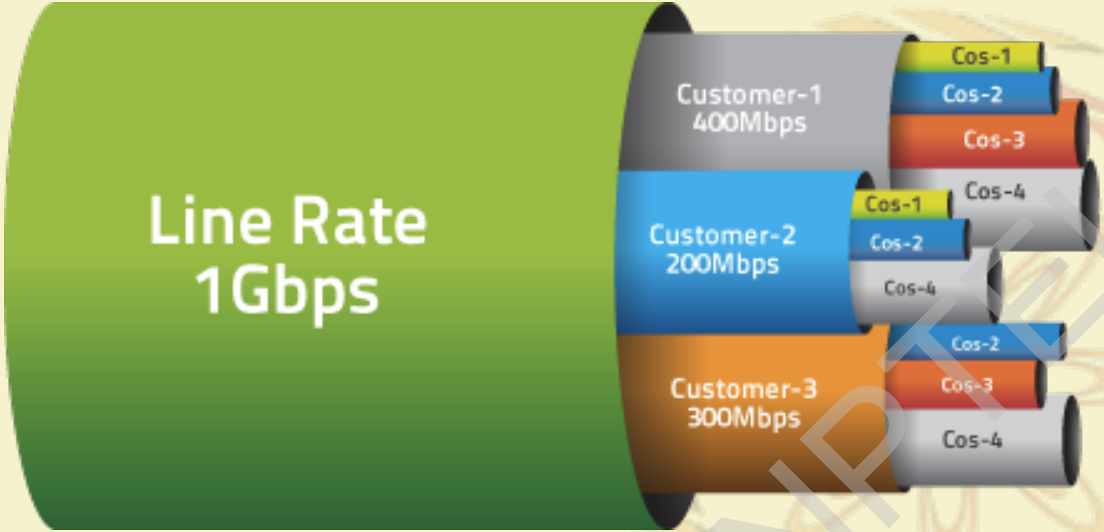
NPTEL ONLINE CERTIFICATION COURSES

NPTEL

COMPUTER NETWORKS AND INTERNET PROTOCOLS

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

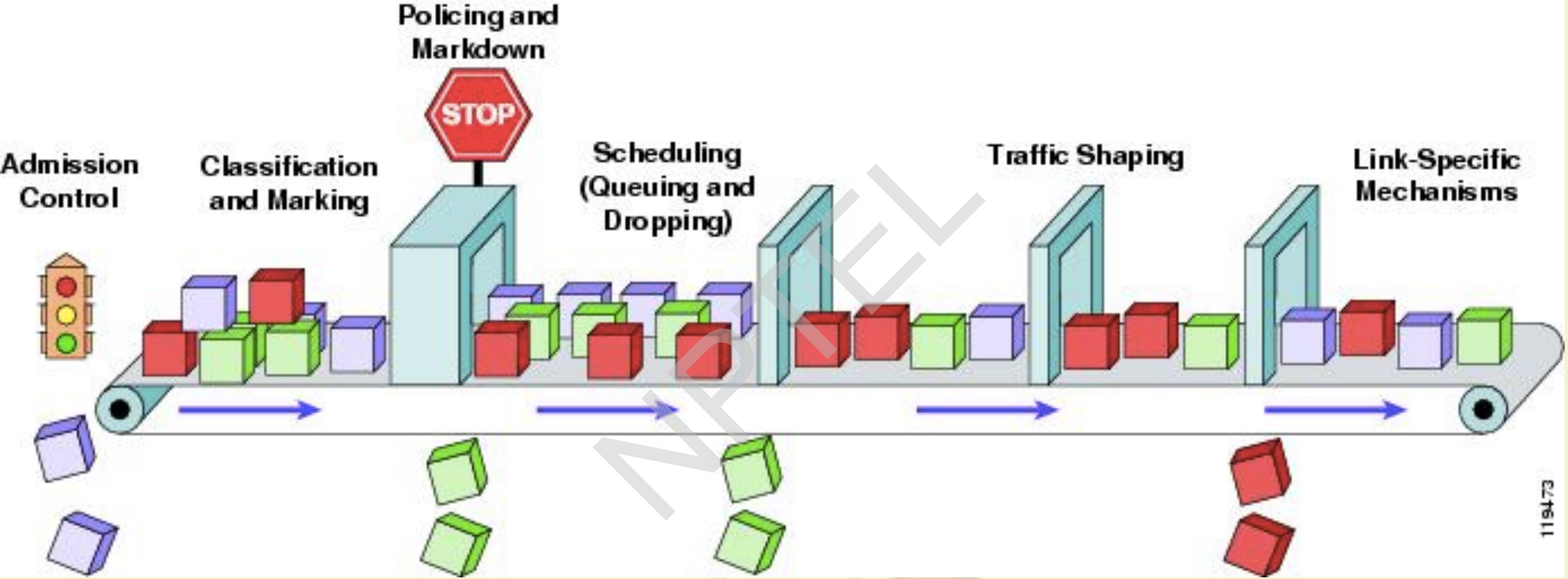
SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR



Internet QoS

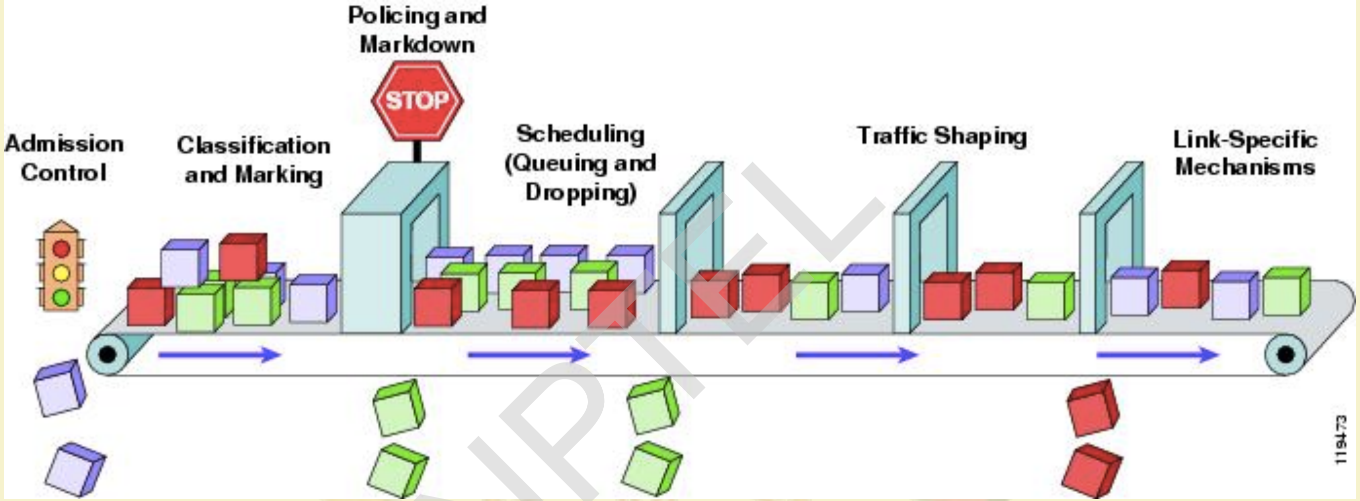
Basic QoS Architecture

Basic QoS Architecture



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

Basic QoS Architecture



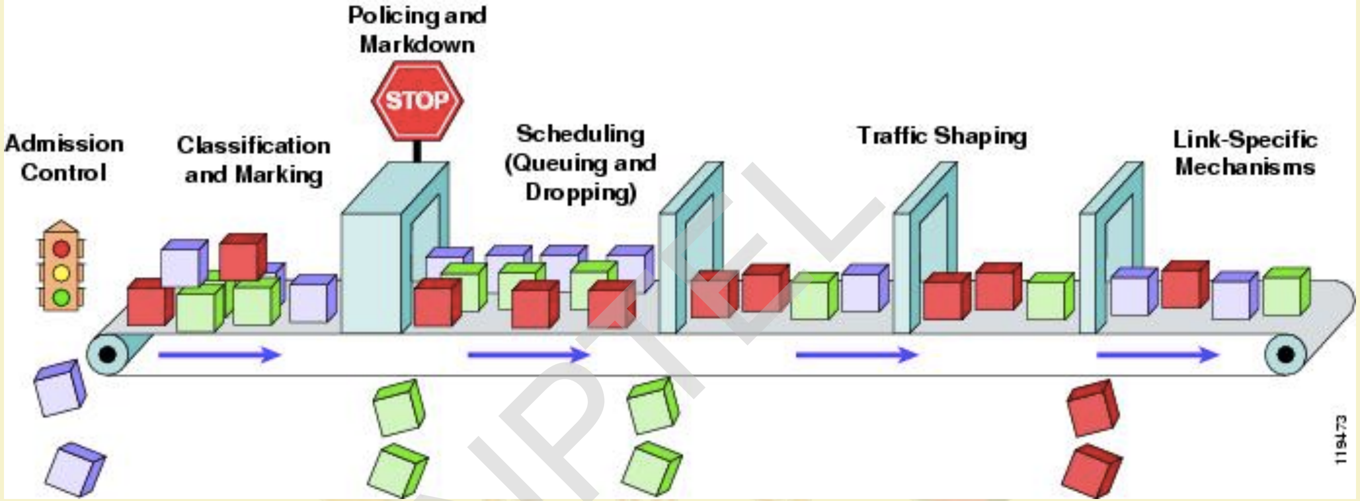
- **Admission Control:** Ensures that new flows are entered in the network only if the QoS of all the existing flows along with the new flows can be satisfied

Admission Control

- Remember the phase from cellular networks – *“all lines are busy; please dial after sometimes”*

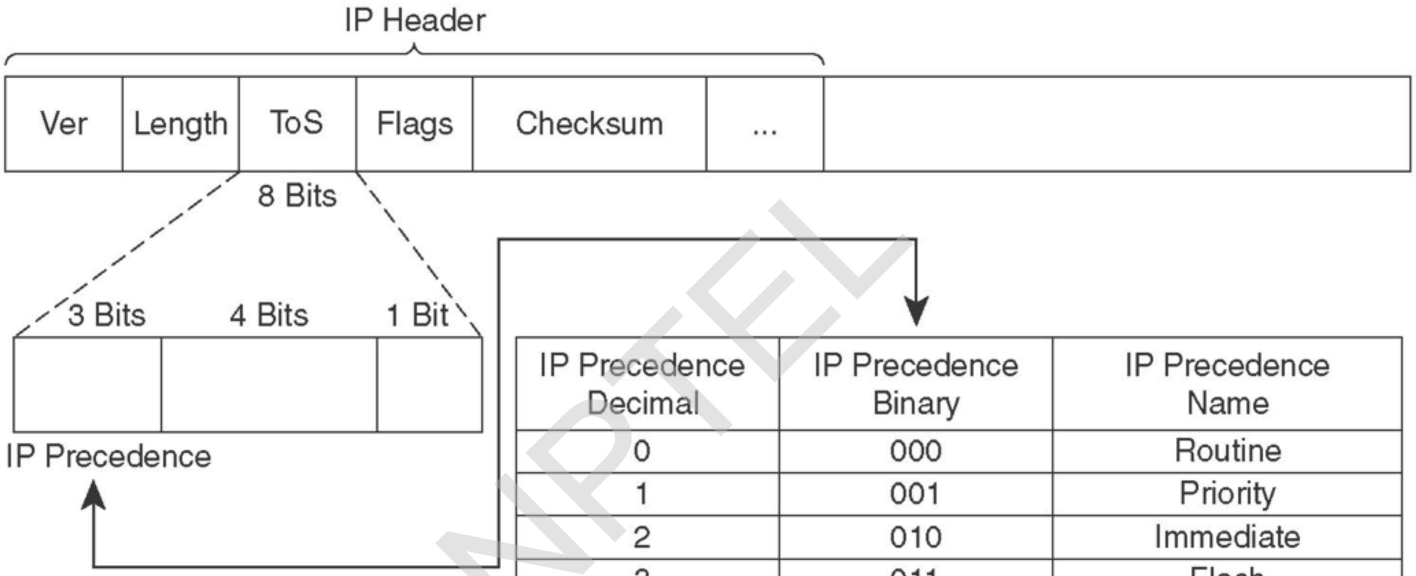
- The network does not allow new flows if all the network resources are blocked in servicing the existing flows based on their QoS requirements

Basic QoS Architecture



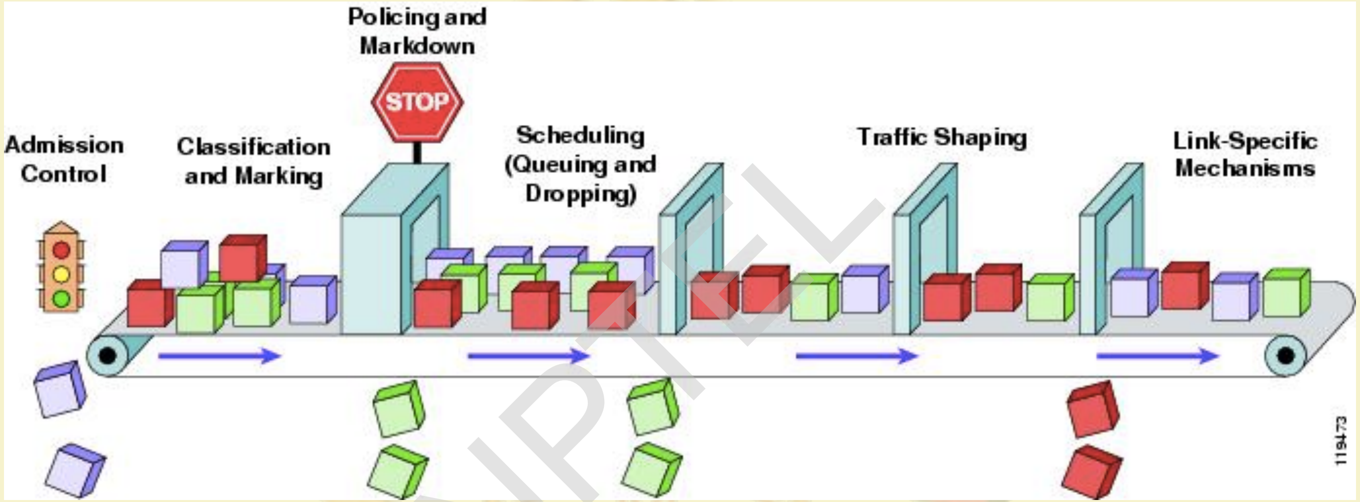
- **Classification and Marking:** Classifies the packets based on their application QoS requirements, and mark the packets accordingly

IP Type of Service (ToS) Field



IP Precedence Decimal	IP Precedence Binary	IP Precedence Name
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-Override
5	101	Critical
6	110	Internetwork Control
7	111	Network Control

Basic QoS Architecture



- **Policing and Markdown:** Monitor the flow characteristics and take appropriate actions based on the flow QoS

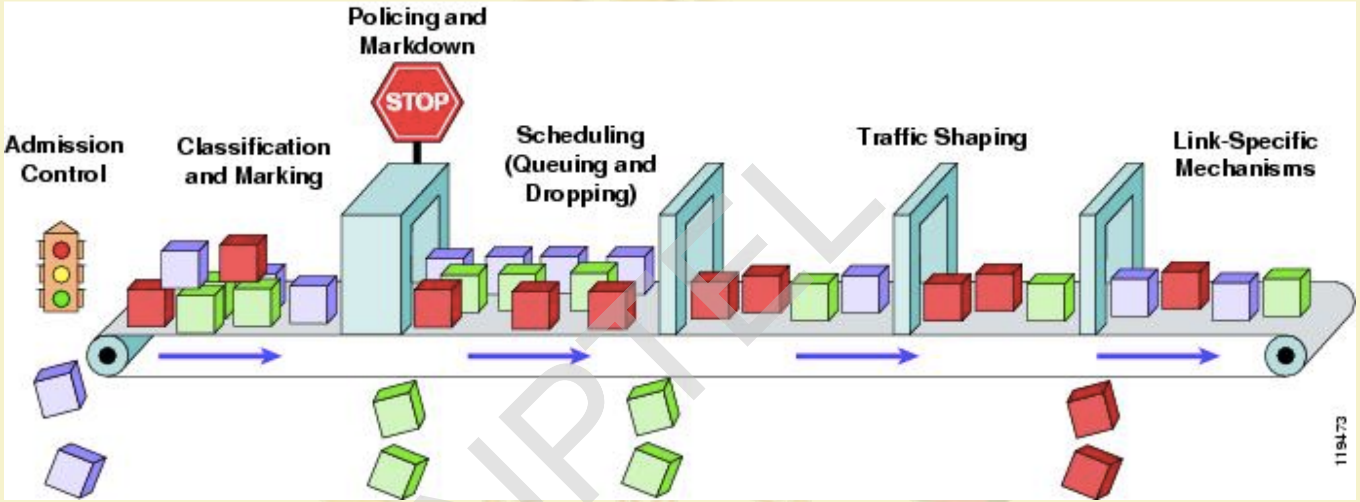
Traffic Policing

- **Service Level Agreements (SLA)**: An agreement or a contract between the customer and the service provider to maintain QoS of an application

```
ip sla 11
   icmp-echo 10.0.10.11 source-ip 68.68.1.2
   frequency 5
!
track 10 ip sla 11 reachability
   delay down 15 up 15
!
ip sla schedule 11 life forever start-time now
ip sla enable reaction-alerts
```

- **Traffic policing** monitors the flow of traffic and mark them to take appropriate actions (reduce priority, drop etc.)

Basic QoS Architecture



- **Scheduling:** Based on markdown by the traffic policers, schedule the traffic into output buffers of an interface

Traffic Scheduling based on Queuing

- Maintain multiple Queues at the interface, the scheduling mechanism services the queues based on the scheduling policy

- Example: **Priority Queuing**

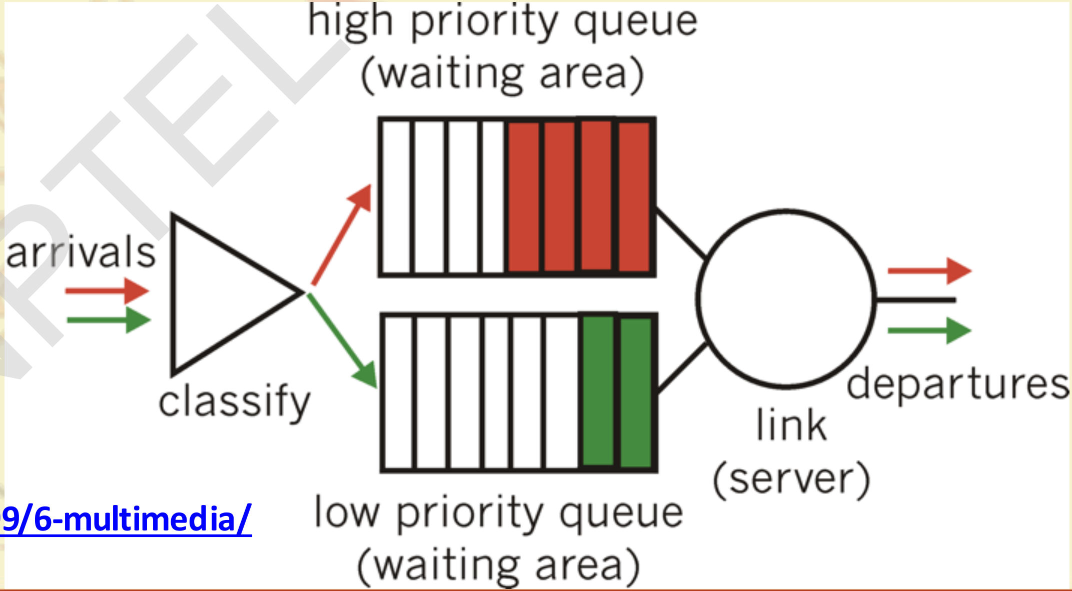
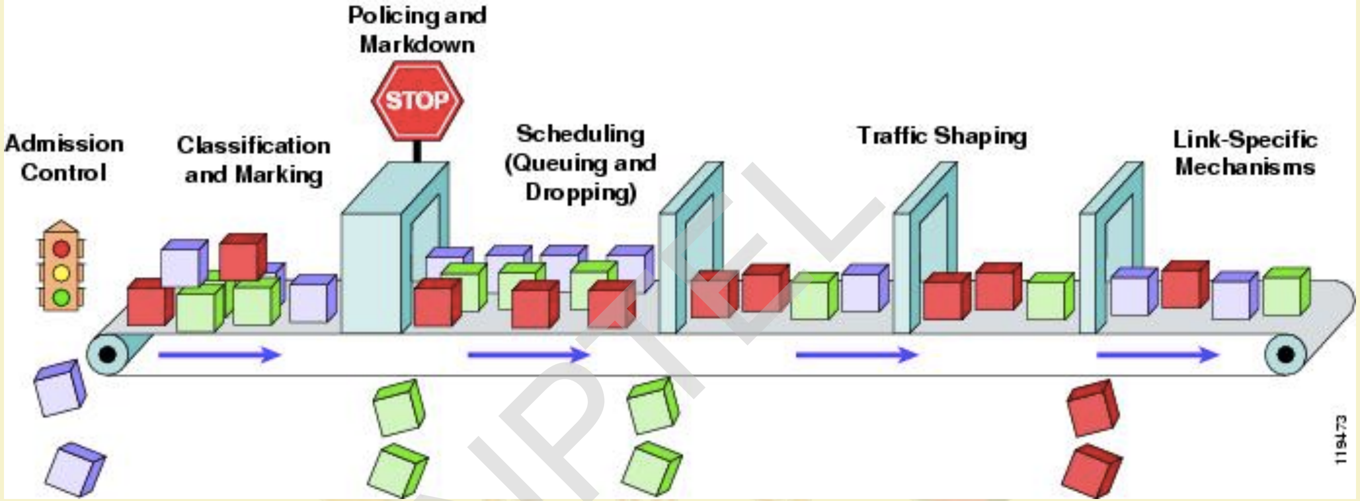


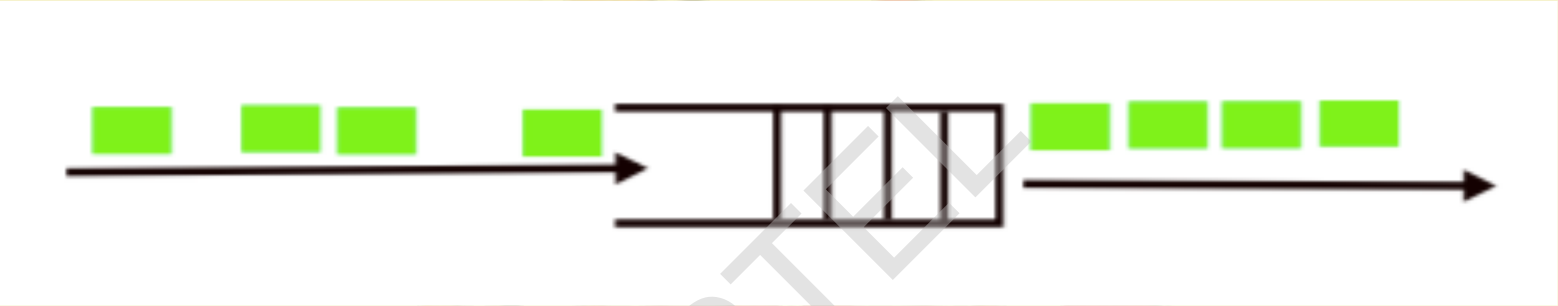
Image source: http://www2.ic.uff.br/~michael/kr1999/6-multimedia/

Basic QoS Architecture



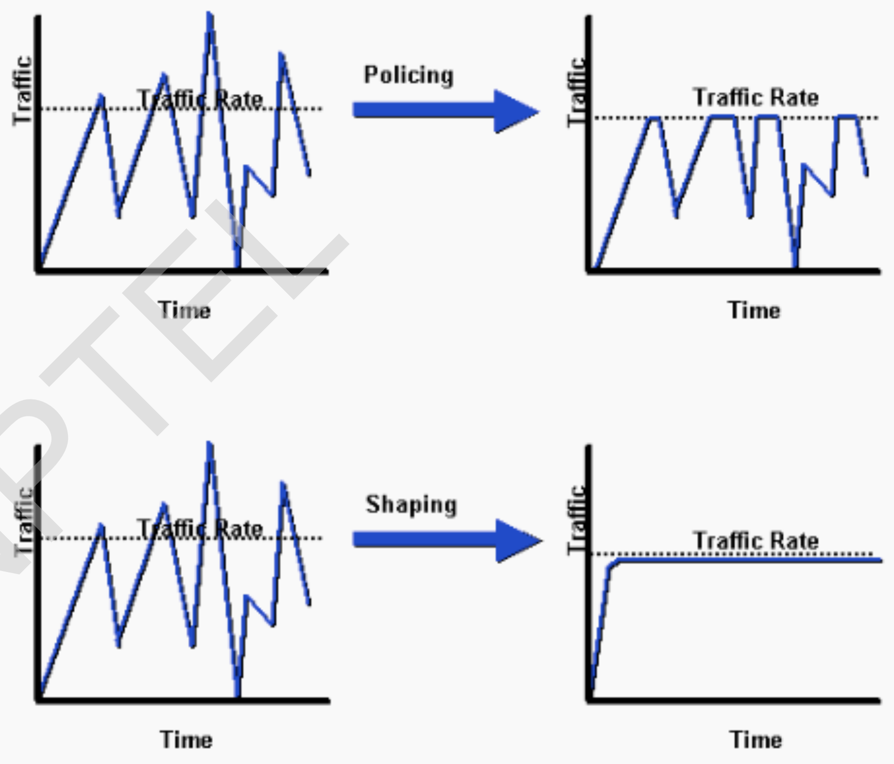
- **Traffic Shaping:** Control the outgoing traffic rate irrespective of the incoming traffic rate (e.g. constant bit rate output from the interface buffer)

Traffic Shaping



- Input traffic is bursty
- Output traffic has constant packet rate – reduces the jitter

Traffic Policing versus Traffic Shaping



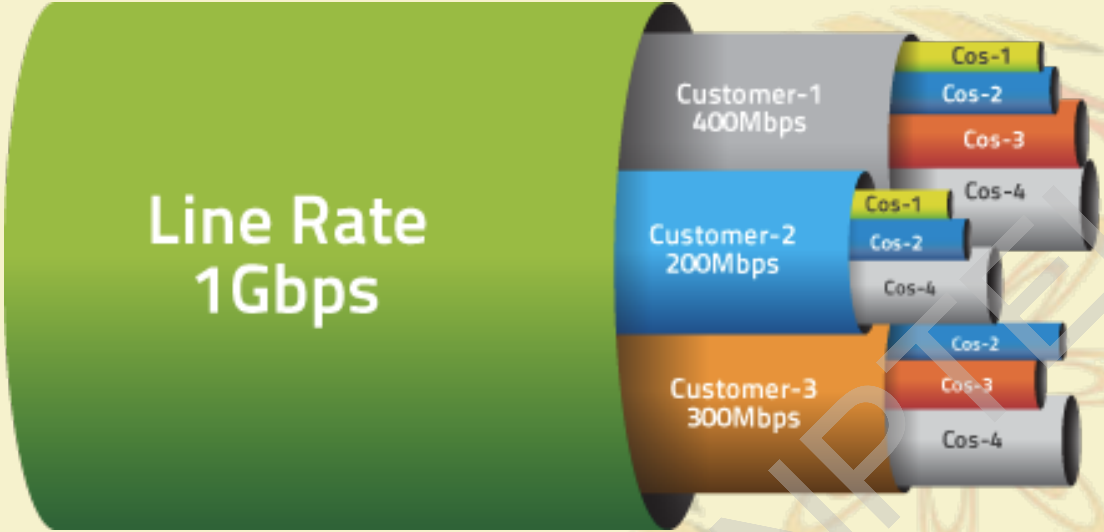
Source:
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

thank you!

COMPUTER NETWORKS AND INTERNET PROTOCOLS

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

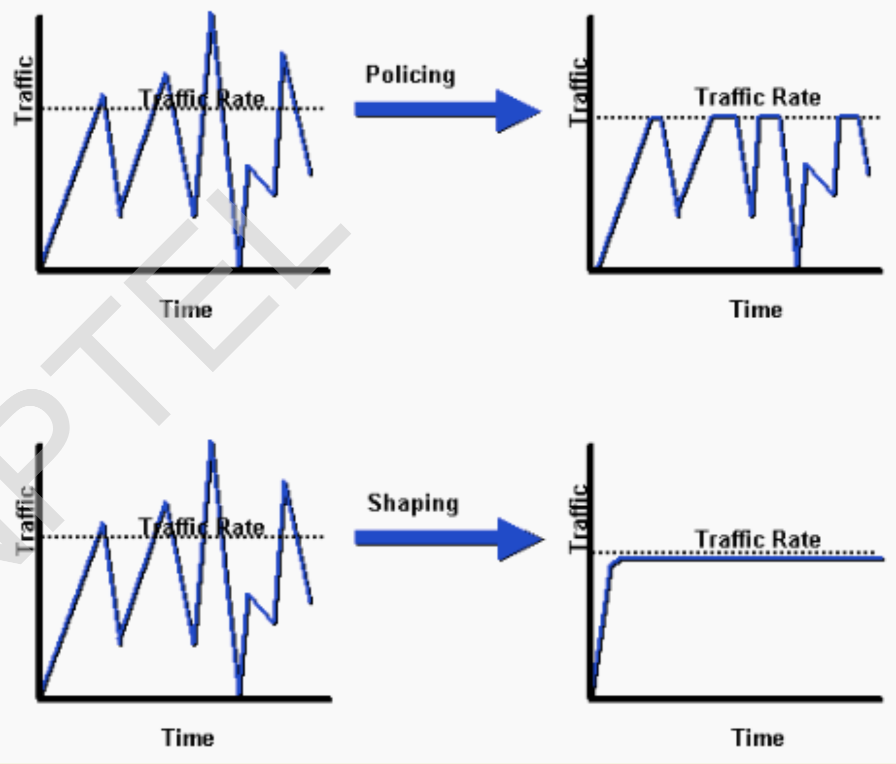
SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR



Internet QoS

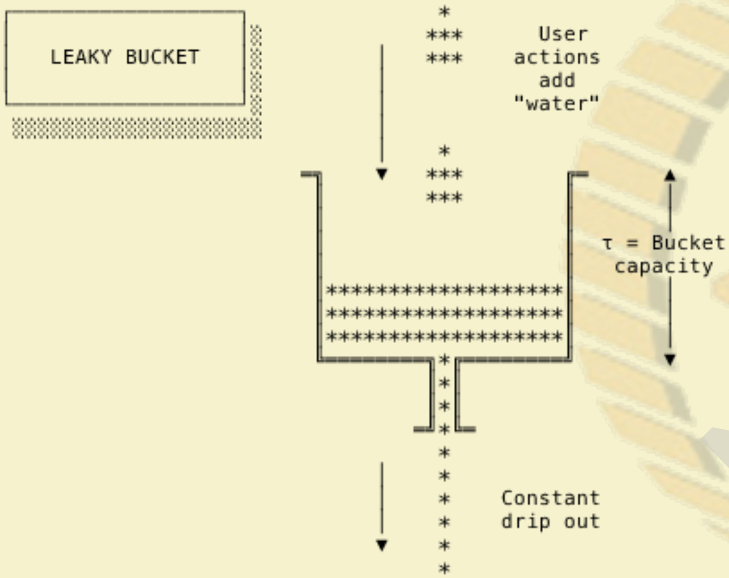
Digging Further - Policing, Shaping and Scheduling

Traffic Policing versus Traffic Shaping



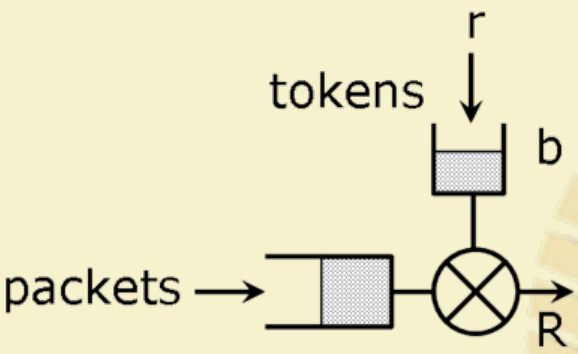
Source:
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

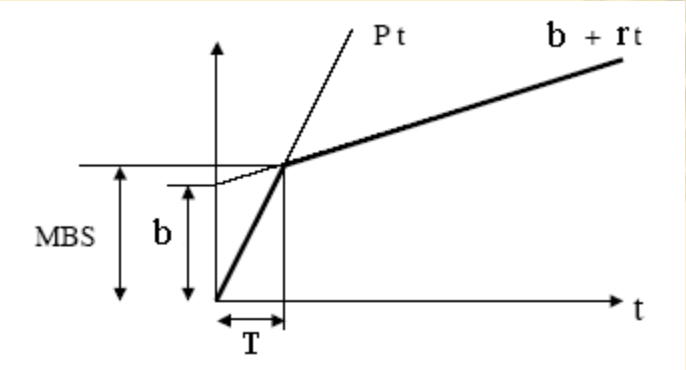
Leaky Bucket for Traffic Policing



- Incoming packets are put in the packet queue – the packet queue works as a bucket
- A single server queue with constant service time
- If the bucket overflows that the packets are discarded
- Input rate can vary but the output remains constant

Token Bucket for Traffic Policing





- Incoming packets are put in the packet queue.
- Token generation rate = r tokens/second, bucket size = b
- The rate of output traffic is bounded by the token generation rate
- Output rate $R(t) = \min(Pt, b + rt)$

Leaky Bucket versus Token Bucket

- **Leaky Bucket:** Smooth out traffic but does not permit burstiness

- **Token Bucket:** Smooth out traffic and also permits burstiness – if there is no incoming packet, tokens are get added in the token bucket, and the burst traffic is permitted up to the amount of token accumulated

- Both the leaky bucket and the the token bucket algorithms can be used for **traffic shaping**, with the addition of a **playout buffer**
  - A buffer to add some additional delay to the packets that arrived too early.

thank you!

IIT KHARAGPUR

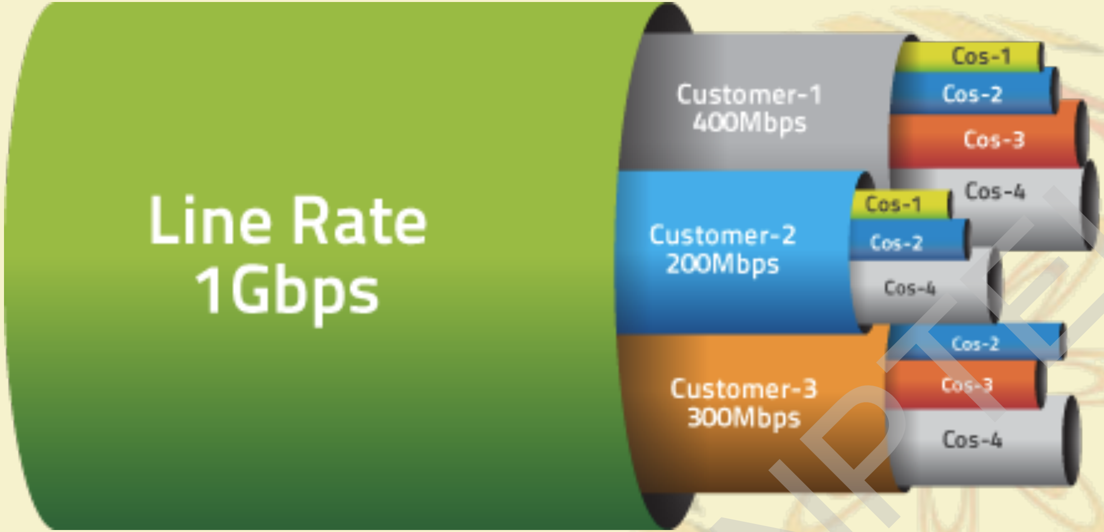
NPTEL ONLINE CERTIFICATION COURSES

NPTEL

COMPUTER NETWORKS AND INTERNET PROTOCOLS

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

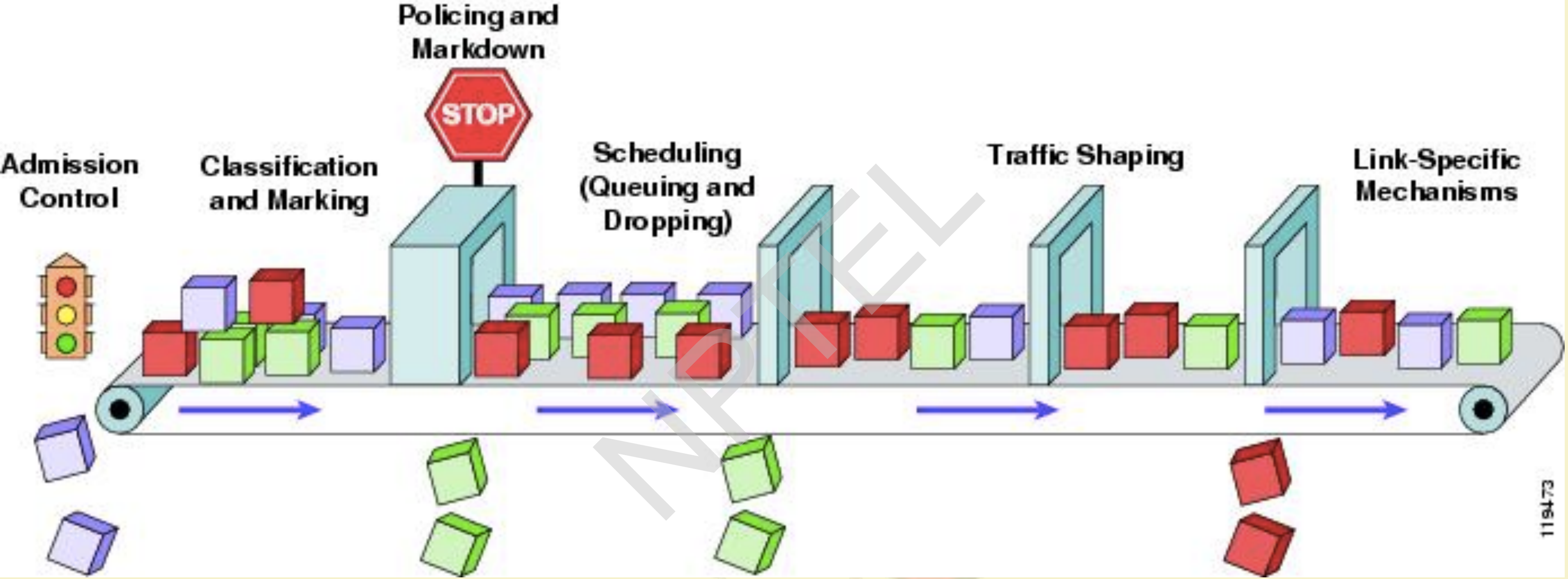


Internet QoS

Digging Further -

Queuing and Congestion Avoidance

Basic QoS Architecture



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

Scheduling

- Classification and Marking - marked the data packers into different traffic classes.
  - The marked traffics are of different priority classes and require different level of QoS based on their SLA.
    - High priority delay-sensitive traffic (VoIP)
    - High bandwidth requirements (VoD, IPTV)
    - Best Effort services (HTTP, FTP)

Multi-Class Scheduling

- We call them as different “class”es of traffic
  - Traffic class 1: High priority delay sensitive traffic
  - Traffic class 2: Medium priority bandwidth hungry traffic
  - Traffic class 3: Low priority best effort traffic

- Different classes of traffic requires different treatments

Multi-Class Scheduling

- Different classes of traffic requires different treatments
  - Traffic class 1: Ensure minimum queuing delay for the packets
  - Traffic class 2: Ensure sufficient bandwidth for the packets
  - Traffic class 3: No specific requirements, serve using best-effort services

- Use different queuing strategies

Queuing for Multi-Class Scheduling

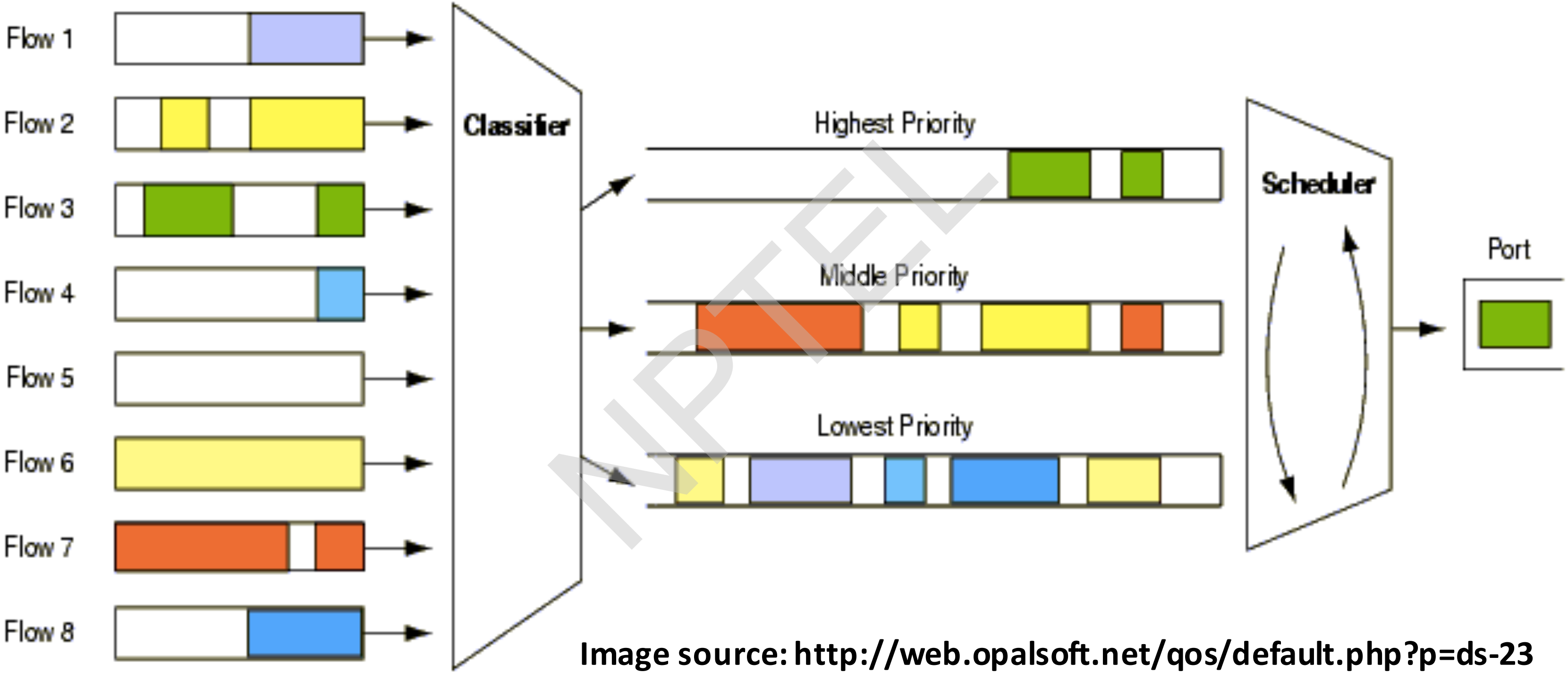
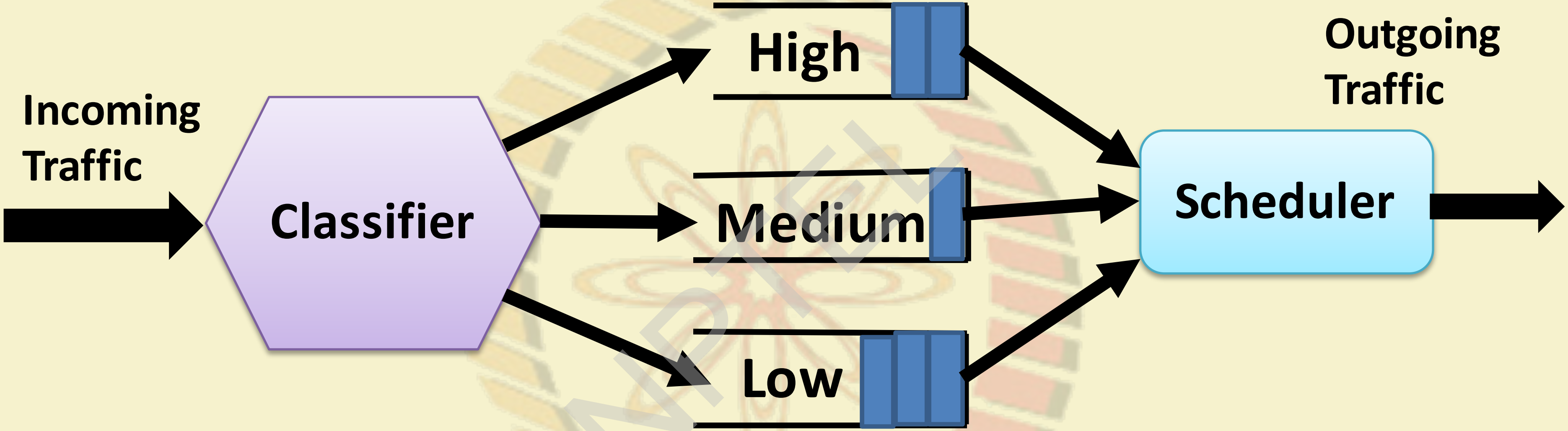


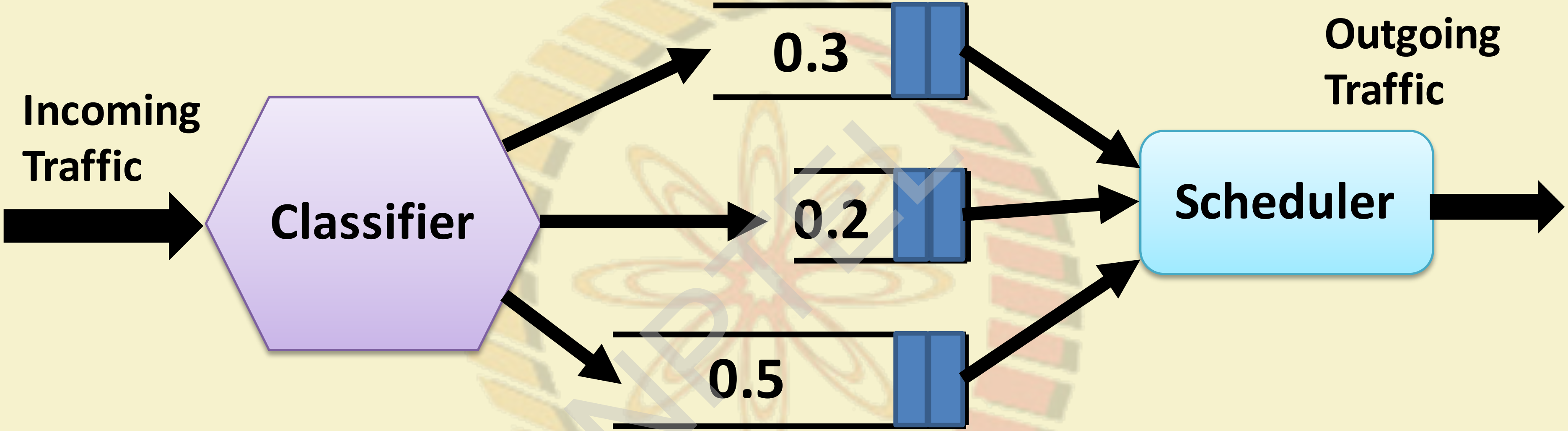
Image source: http://web.opalsoft.net/qos/default.php?p=ds-23

Scheduling – Priority Queuing



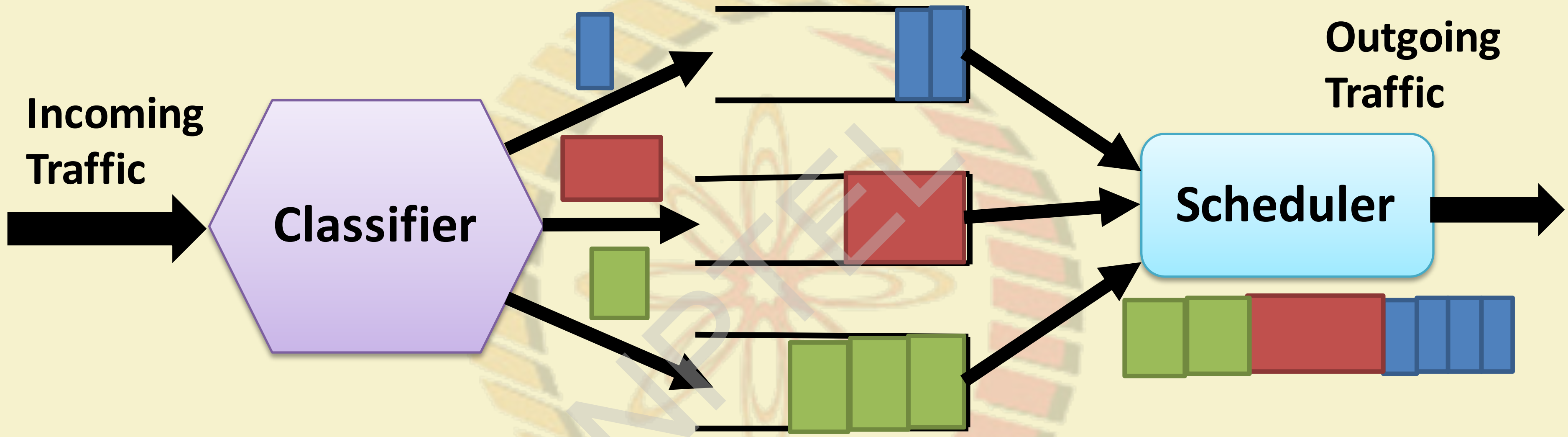
- Transfer traffic from lower priority queues once the higher priority queues are empty

Scheduling – Custom Queueing



- Different queues are of different size – works like transmission window
- Supports guaranteed bandwidth

Scheduling – Weighted Fair Queuing (WFQ)



- Ensure fairness among the flows – every flow will get equal amount of bandwidth
- Queues can be assigned with a weight – fairness proportional to the weight

Congestion Avoidance in the Internet

- Avoid congestion by controlling the queue parameters

- **Different from TCP congestion control**
  - TCP response on detection of the congestion
  - **Congestion avoidance** – ensure that a flow performance does not get affected by the congestion

- If congestion avoidance is there at the network layer, do we still need congestion control at transport layer?

Why Congestion Avoidance is Necessary for QoS

- Internet carries multiple data packets from different applications having different QoS requirements

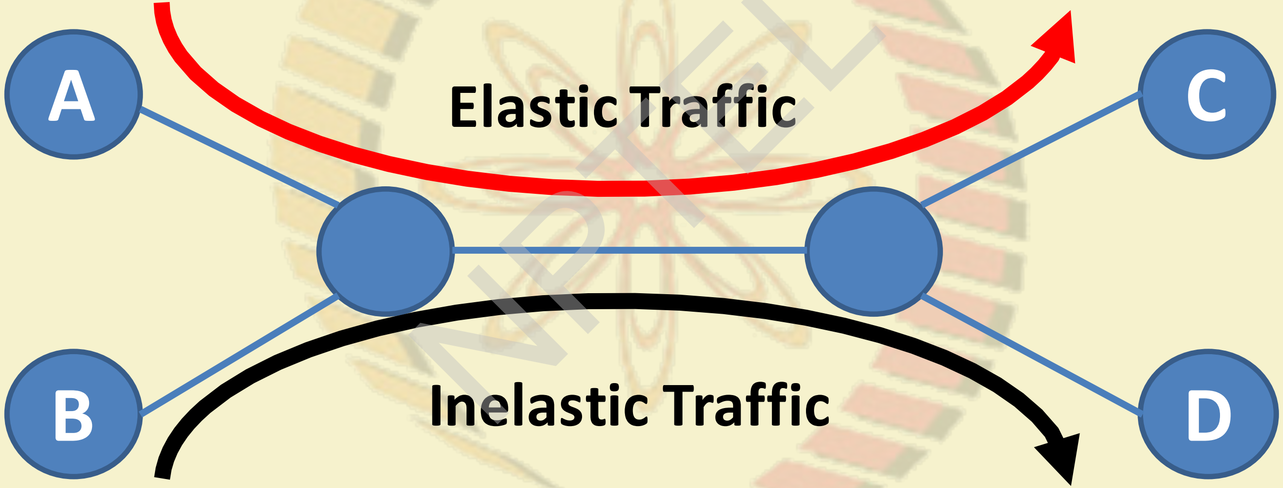
- **Elastic traffic** – TCP like traffic, elastic nature of flow control based on AIMD

- **Inelastic Traffic** – UDP traffic, smoothed or controlled or constant bit rate traffic

- **Inelastic traffic is preferred for real time applications – Can you say why?** (NB: Don't confuse with YouTube!)

Why Congestion Avoidance is Necessary for QoS

- Which traffic will dominate over the link?

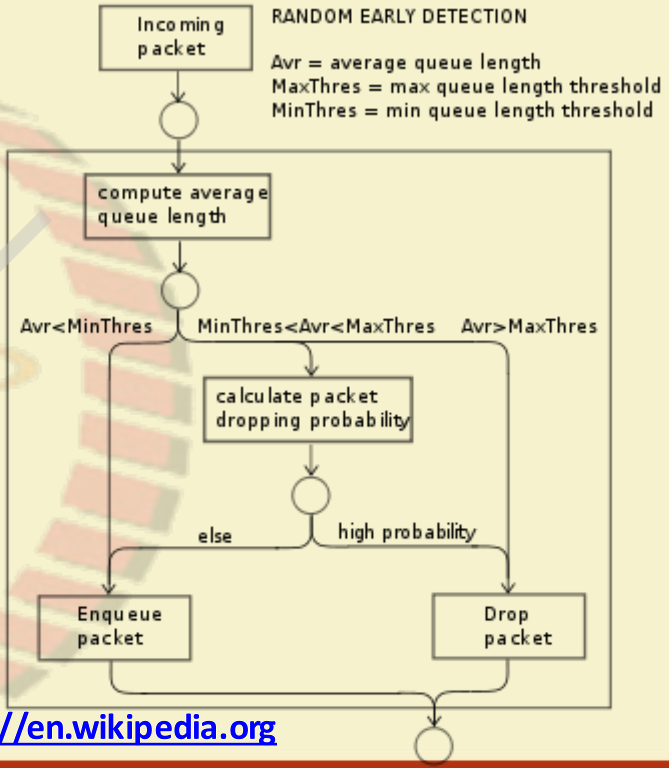


Random Early Detection (RED)

- Drop probability if different for different traffics, depending on the nature – elastic or inelastic
- RED smooths out the drop probability across all the flows depending on the congestion probability
- Detect the possibility of congestion in the Internet. If congestion possibility is high, **RANDOMLY** drop packets before the enqueue

Random Early Detection (RED)

- Determine the possibility of packet drop by observing the average queue length

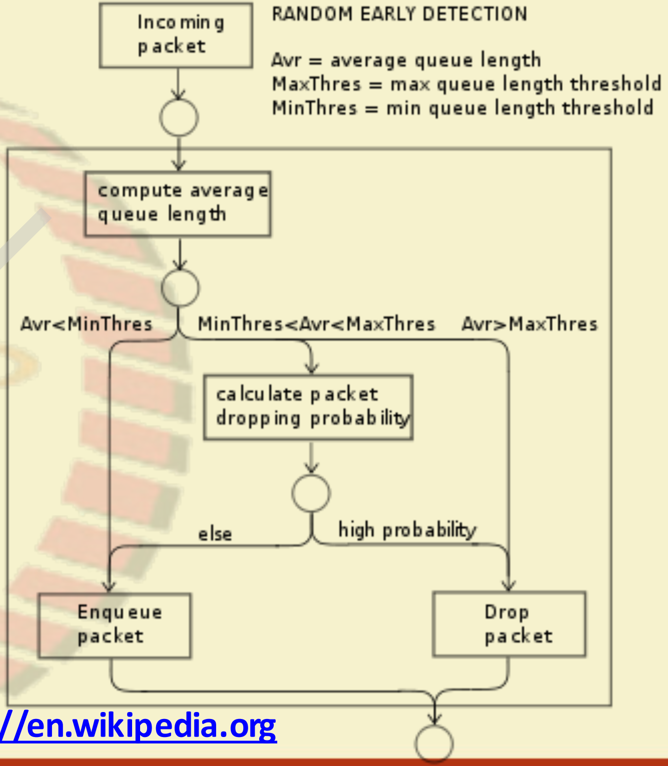


Source: https://en.wikipedia.org

Random Early Detection (RED)

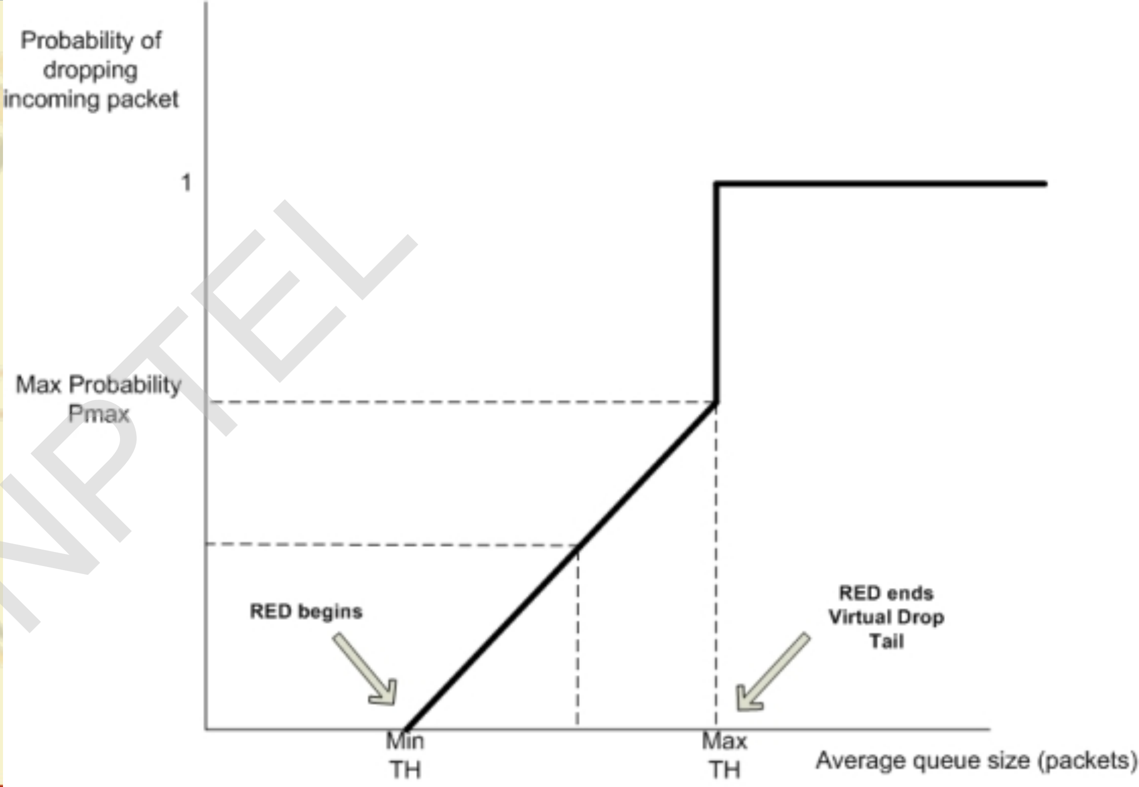
- Let *d(k)* denotes the packet drop probability and Max_p be the maximum packet drop probability

$$d(k) = Max_p \times \left(\frac{k - MinThresh}{MaxThresh - MinThresh}\right)$$



Source: https://en.wikipedia.org

Random Early Detection (RED)



Source: http://www.eng.uwi.tt/

thank you!

IIT KHARAGPUR

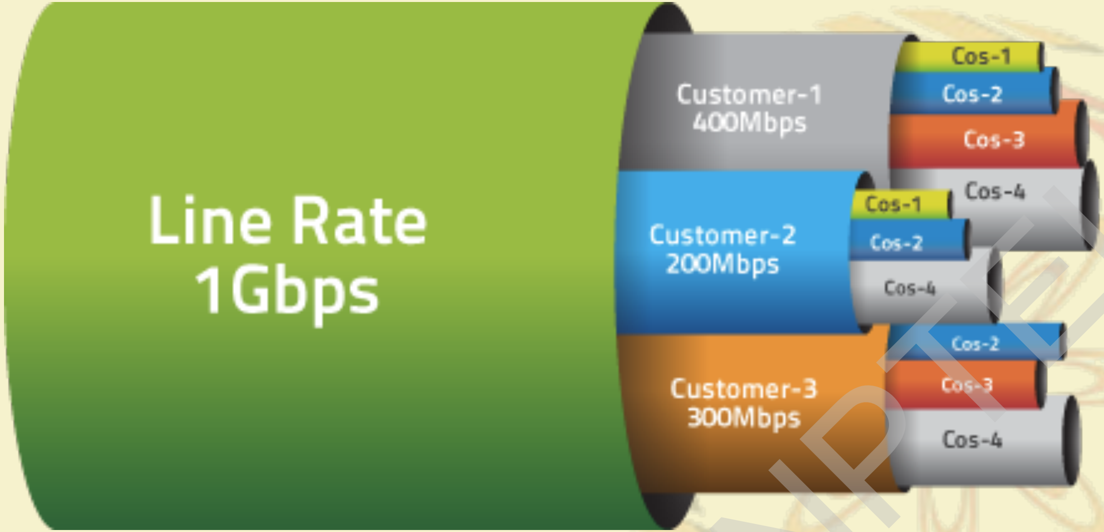
NPTEL ONLINE CERTIFICATION COURSES

NPTEL

COMPUTER NETWORKS AND INTERNET PROTOCOLS

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR



Internet QoS

IntServ and DiffServ Architectures

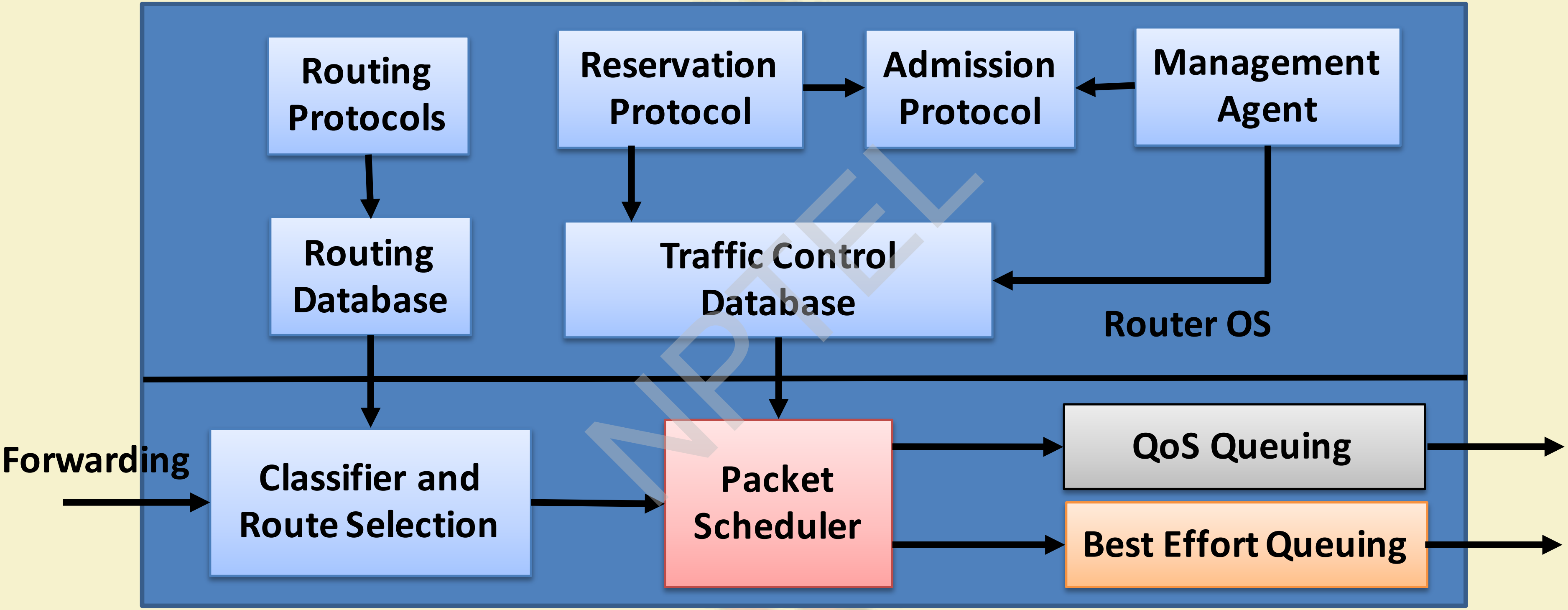
Internet Service Architecture (ISA)

- Integrated Service (IntServ) QoS architecture over the Internet
- **Admission Control**
  - For QoS, reservation required for new flow
  - Resource Reservation Protocol (RSVP)
- **Routing Algorithm** - routing decision based on QoS parameters

Internet Service Architecture (ISA)

- **Queuing**
  - Take account of different flow requirements
- **Discard Policy**
  - Avoid congestion to meet QoS

ISA in a Router



Resource Reservation Protocol (RSVP)

- A network control protocol that allows data receiver to request a special end to end quality of service for its data flows

- A network control protocol, not a routing protocol - although works over IP

- Designed to operate with current and future unicast and multicast routing protocols

ISA and RSVP

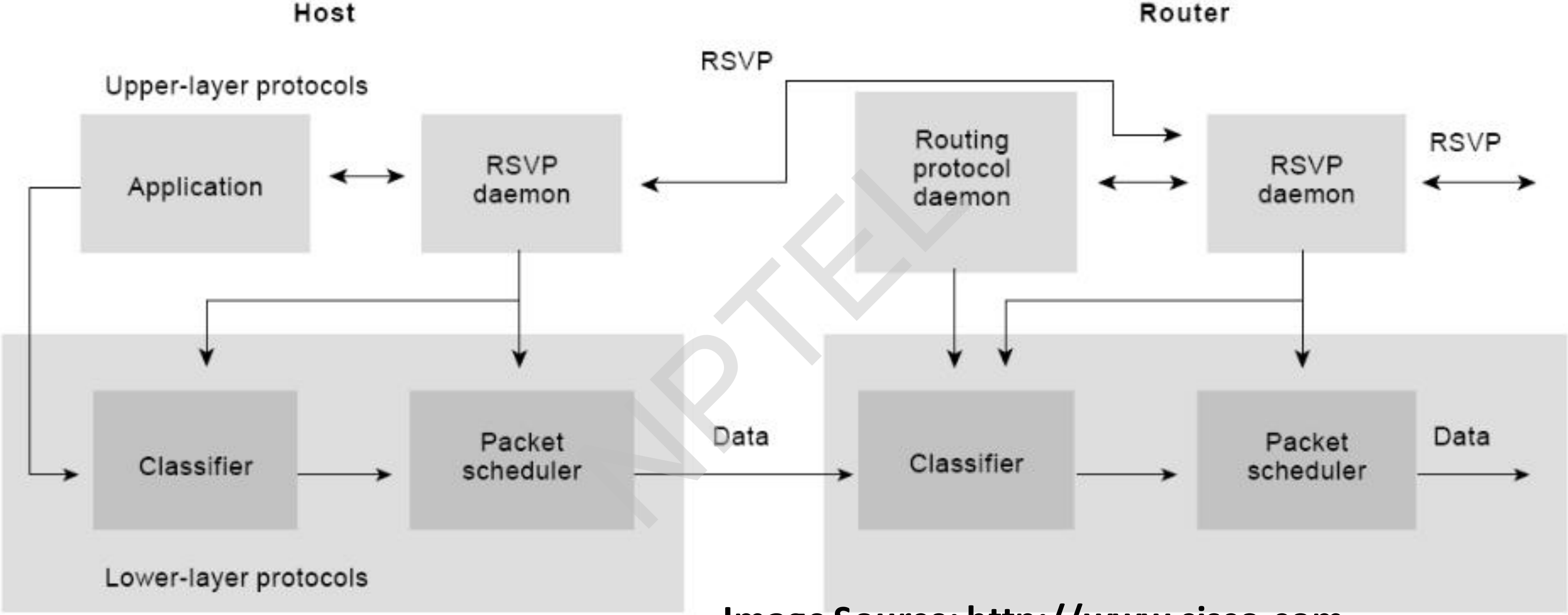


Image Source: http://www.cisco.com

RSVP Terminologies

- Quality of Service is implemented for a particular data flow by a mechanism called “traffic control”
- **Packet Classifier**: Determines the QoS
- **Packet Scheduler**: Link layer dependent mechanism to determine which particular packets are forwarded
  - For each outgoing interface, the scheduler achieves the desired QoS.

RSVP Reservation Procedure

- During reservation setup, an RSVP QoS request is passed to two local decision modules: 1. Admission control 2. Policy control.

- **Admission Control**: Determines whether the node has sufficient available resources to supply the requested resources.

- **Policy Control**: Determines whether the user has administrative permission to make the reservation.

RSVP Reservation Procedure

- If both checks succeed, parameters are set in the packet classifier and in the link layer interface to obtain the desired QoS.

- If either checks fails, the RSVP program returns an error notification to the application process that generated the request.

RSVP Reservation Model

- An RSVP request consists of : `flowspec` together with a `filterspec`. This pair is called the "flow descriptor".
- The `flowspec` specifies a desired QoS.
- The `filterspec` together with the session specification defines the set of data packets.

RSVP Reservation Model

- The `flowspec` is used to set parameters in the packet scheduler, while the `filterspec` is used to set parameters in the packet classifier

- The `flowspec` in a reservation request will generally include a service class and two sets of numeric parameters:
  - `Rspec` - defines the desired QoS,
  - `Tspec` - describes the data flow.

flowspec Structure

```
typedef struct flowspec {
        ULONG TokenRate;
        ULONG TokenBucketSize;
        ULONG PeakBandwidth;
        ULONG Latency;
        ULONG DelayVariation;
        SERVICETYPE ServiceType;
        ULONG MaxSduSize;
        ULONG MinimumPolicedSize;
} FLOWSPEC, *PFLOWSPEC, *LPFLOWSPEC;
```

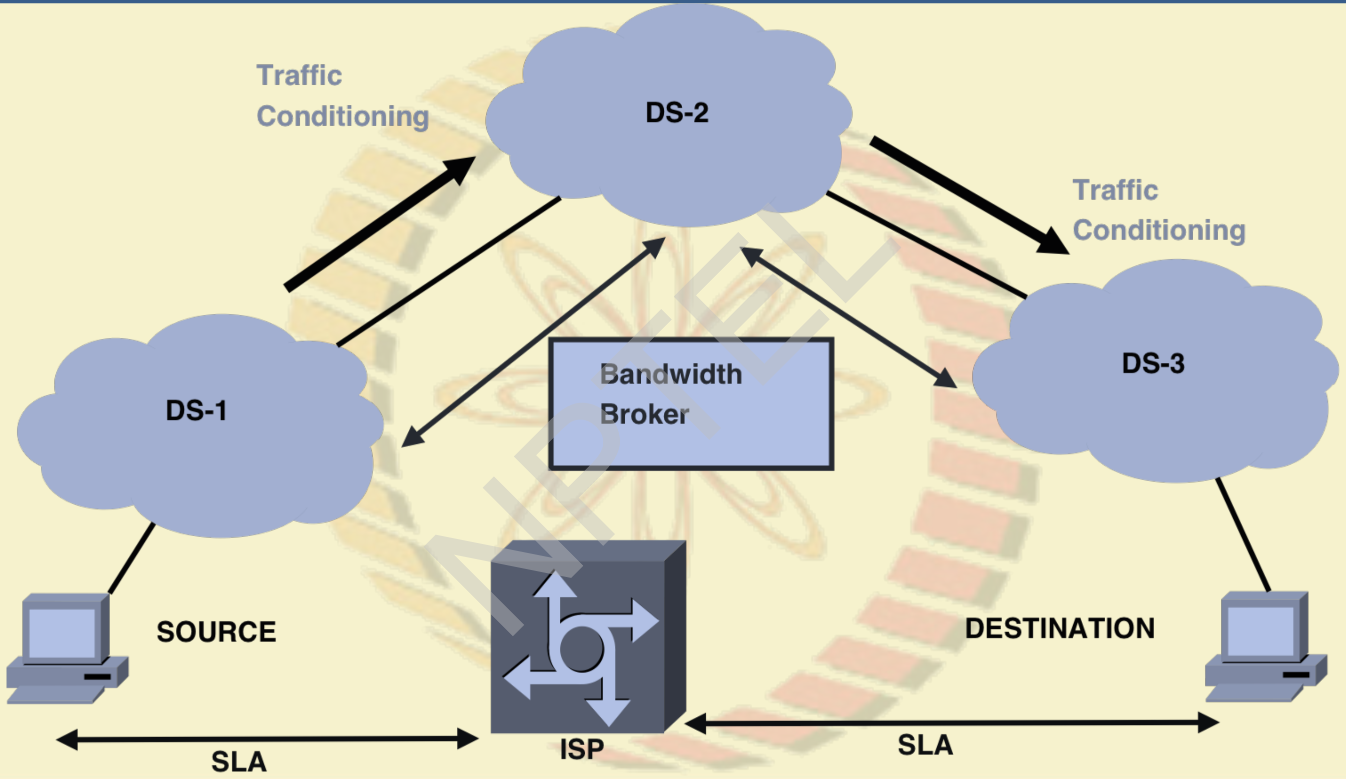
Problems with RSVP

- The RSVP daemon needs to maintain per-flow states at intermediate routers.
- Use of per-flow state and per-flow processing raises scalability concerns for large network.

Differentiated Service Architecture (DiffServ)

- Coarse-grained, class-based mechanism for traffic management
- **Packet classifier**: uses a 6-bit differentiated services code point (DSCP) in the 8-bit Differentiated Services field (DS field) in the IP header
- DiffServ-aware routers implement **per-hop behaviors** (PHBs) - defines the packet-forwarding properties associated with a class of traffic
- DiffServ recommends a standardized set of traffic classes.
- A group of routers that implement common, administratively defined DiffServ policies are referred to as a **DiffServ (DS) domain**.

DiffServ Architecture



Bandwidth Broker

- A **Bandwidth Broker** is an agent that has some knowledge of an organization's priorities and policies and allocates QoS resources with respect to those policies. (RFC 2638)

- In order to achieve an end-to-end allocation of resources across separate domains, the Bandwidth Broker managing a domain will have to communicate with its adjacent peers, which allows end-to-end services to be constructed out of purely bilateral agreements.

SLA and TCA

- **Service Level Agreement (SLA):** A set of parameters and their values which together define the service offered to a traffic stream by a differentiated service (DS) domain.

- **Traffic Conditioning Agreement (TCA):** A set of parameters and their values which together specify a set of classifier rules and traffic profile.

Traffic Classification and Conditioning

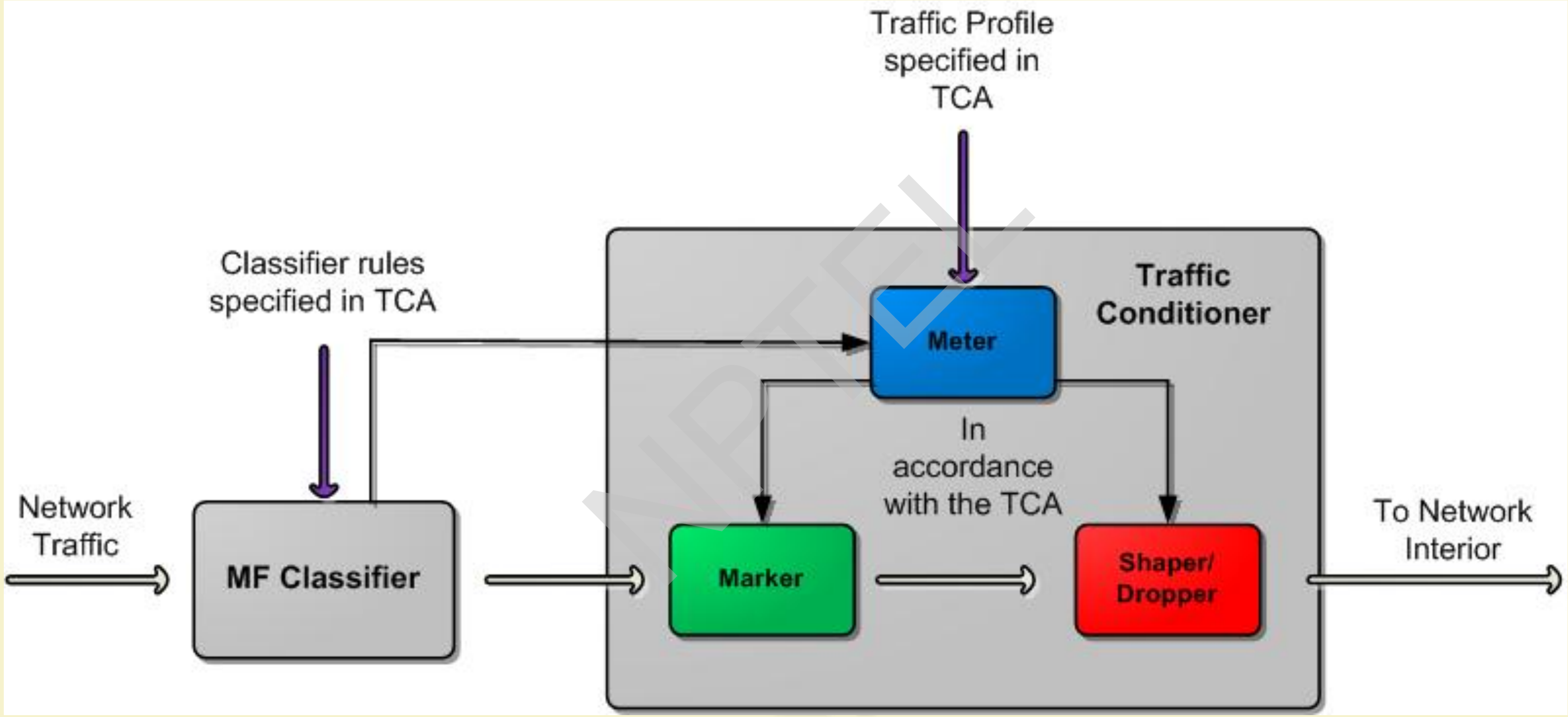
- In a DS domain, the boundary node interconnects the current DS domain to other DS or non DS capable domains.

- The **classification and conditioning process** of a boundary node in a DS domain is responsible for mapping packets to a forwarding class supported in the network and ensuring that the traffic from a customer conforms to their SLAs.

Traffic Conditioning

- Traffic conditioning is a *set of control functions* that is applied to classified packets streams in order to enforce traffic conditioning agreements; which are made between customers and service providers.
  - have four components - **meter**, **marker**, **shapers** and **droppers**
  - a meter is used to measure the classified traffic stream against a traffic profile.
  - the state of the meter may then be used to enable a marking, shaping or dropping action.

Traffic Conditioner



Classification and Marking - Per Hop Behaviors (PHB)

- **Default PHB** - for best-effort services
- **Expedited Forwarding (EF) PHB** - dedicated to low-loss, low-latency traffic
- **Assured Forwarding (AF) PHB** - gives assurance of delivery under prescribed conditions (different queuing behaviors)
- **Class Selector PHBs** - which maintain backward compatibility with the IP Precedence field.

Working Steps of a DS Domain

- The source (users) make a contract with the ISP for a specific SLA. Source sends request message to first hop router
- First hop router sends request to BB, which sends back either a accept or reject
- If accept, either source or first hop router will mark DSCP and start sending packets
- Edge router checks compliance with SLA and does policing. Excess packets are either discarded or marked as low priority to comply with the SLA
- Core routers will just look at DSCP and decide PHB

Further Readings

- Cisco White Papers on QoS -
  - https://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html
  - http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

thank you!