A DiffServ–IntServ Integrated QoS Provision Approach in BRAHMS Satellite System

Guido Fraietta[1], Tiziano Inzerilli[2], Valerio Morsella[3], Dario Pompili[4]

University of Rome "La Sapienza", Dipartimento di Informatica e Sistemistica,
Via Eudossiana 18, 00184-Rome, Italy
[1]guifra@inwind.it ,[2]inzerilli@tiscalinet.it, [3]vmaolr@tiscalinet.it, [4]dariopompili@libero.it

Abstract: *This document illustrates the Quality of Service (QoS) architecture that has been developed within the BRAHMS (BRoadband Access for High Speed Multimedia via Satellite) IST project. In the target satellite access system, which is named BMSS (Broadband Multimedia Satellite System), User Terminals are provided with a transport service, based on the Internet technique, through which both user-to-user and user-to-network configurations (see* ***Figure 1****) are allowed. Besides the traditional best effort transport service, QoS treatment is provided in a framework that combines both DiffServ [IETF RFC 2474], [IETF RFC 2475] and IntServ [IETF RFC 1633] QoS models into a unique platform.*

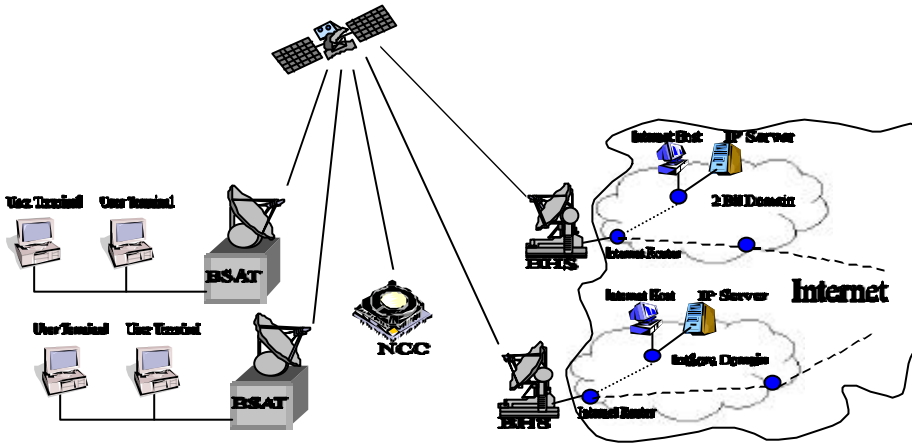

Figure 1: BRAHMS Scenario

I. Two Bit Architecture

In document simplified DiffServ approach, named *Two Bit Architecture* [IETF RFC 2638], is considered instead of the traditional DiffServ one. The Two Bit Architecture is suggested as a first stage for DiffServ implementation, as it only considers two different services with better QoS guarantees than Best Effort, thus simplifying traffic control operations. Furthermore, the Two Bit Architecture is easily extendible and will be completely compatible with approaches that would define more levels of differentiation within a particular service, as standard DiffServ approach.

The Two Bit Architecture services are:

- An **"**Assured" service to assign "expected capacity" usage profiles that are statistically provisioned. The assurance that the user of such a service receives is that traffic is unlikely to be dropped as long as it stays within the expected capacity profile. An Assured service traffic flow may exceed its profile. In this case it receives a lower assurance level.
- A "Premium" service that is provisioned according to peak capacity profiles that are strictly not oversubscribed and that is given its own high-priority queue in routers. A Premium service traffic flow is shaped and hard-limited to its provisioned peak rate and shaped so that bursts exceeding it are never injected into the network.

In order to discriminate the two services from the traditional best-effort one, two bits in the IP header are used, which are called A and P bits.

II. Dynamic Service Selection

When a user requests a connection with a remote Internet host, it sends its QoS request to the Satellite Terminal (BSAT) which it is connected to, through the RSVP signalling protocol.
The BSAT is provided with a specific table, called *Next Domain Sub-nets Table*, containing Hub Station's (BHS) layer 2 addresses, which are associated with the list of Two Bit sub-nets that are directly connected with each BHS. If the destination IP sub-net address is contained in the table, the BSAT assumes that the destination host is within a Two-Bit domain directly connected to the HS. Thus, the BSAT entity treats this incoming request as a Two-Bit request. It first checks if there are sufficient resources for the incoming flow and then "simulates" the RSVP protocol operations, sending a RESV message to the User that originated the request. Otherwise, the destination IP sub-net is not present in the table, it treats the incoming request as a standard IntServ request.

III. Traffic Control

The traffic control module inside the BSAT includes individual policer for each flow whose QoS parameters have been advertised by RSVP signalling, as described before. GS [IETF RFC 2212] and CL [IETF RFC 2211] policing will be described later. Packets belonging to different flows are classified in individual queues and scheduled for transmission through the satellite link according to an Earliest Deadline First (EDF) scheduling policy. Resource allocation in the BSATs assures that the total amount of resources currently assigned to the BSAT will be at least equals to the global resources necessary to respect all the individual QoS flows' requests. The remaining amount of resources is left for BE traffic packet transmission.
In the BHSs, a mechanism to allocate resources according the given Service Level Agreements (SLA) to Assured packet flows coming from the external Internet is employed.. In this framework, it is assumed that the BHS meters the aggregate average rate of the global Assured traffic. When the classifier receives a new Assured packets' flow from one of the DiffServ boundary routers to which it is connected, it lets this new flow pass through the downstream meter. If the measured rate is below a threshold previously agreed in the SLA, the new incoming flow is accepted. Otherwise, packets belonging to the new flow are dropped by the Classifier.
In the proposed architecture, Assured traffic flows are policed in an aggregate way whereas Assured packet flows coming from the Internet will be classified in a unique queue.

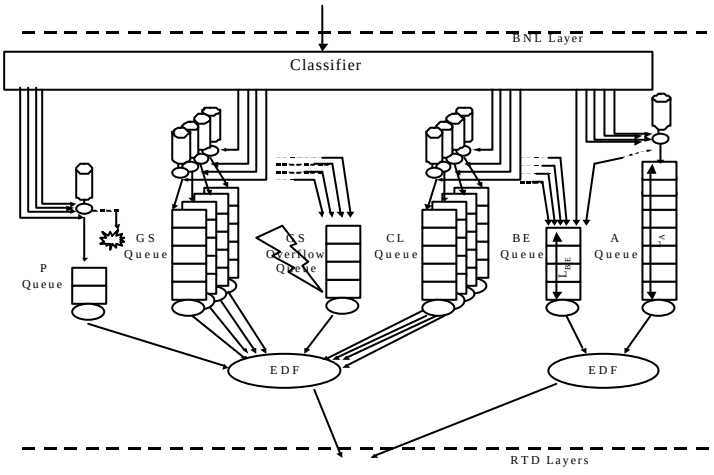

Figure 2: BRAHMS Global Traffic Control

A high-level scheme of the BHS traffic control module is depicted in Figure 2. With reference to the scheme, IntServ and DiffServ flows are treated in an integrated way to respect both IntServ Services delay constraints, high priority delivery for P Service packets, and low drop probability for Assured packets. After being classified and before being enqueued packets pass through a DLB (Dual Leaky

Bucket) [ELWALID] that measures the incoming flow and separate compliant traffic from non-compliant one.
Non-Compliant GS packets coming from different flows are enqueued in an aggregate way in the GS Overflow Queue, where they remain until they are not expired. The spare rate, used to extract packets from this extra-queue, prevent them to expire and thus from being discarded, maximizing as a result the total number of GS packets sent.

IV. DLB model

Dual Leaky Buckets (DLBs) [ELWALID] can be used as a traffic envelope:
- to describe traffic profile on connection establishment;
- to police the traffic flow according to a given QoS contract;
- to shape traffic in a congestion control algorithm by smoothing peaks of traffic.

The first two functions are proper of connection-oriented architectures provided with an admission control module and with negotiation capabilities. The last function can be present in a connectionless environment as well.
A DLB is defined by three parameters:
- token rate "r"which specifies the average rate;
- token bucket size "b" that a measure of the degree of burstiness of the flow;
- peak rate "p" that specifies the maximum allowed bit rate;

When a DLB (p, r, b) declaration for a data flow is given, the following relations for R(t) (the number of bytes which has been issued up to the instant t) has to be satisfied for any interval (t_0,t_1):

$$R(t1)-R(t0) \leq \min(b+ r*(t_1-t_0), p*(t_1-t_0)).$$

When a DLB is employed for policing purpose, the flow is given initially b bytes of credit to use. The transmission consumes this credit at the source rate and at the same time the bucket is fed at a rate of r bit/s. If the token bucket gets completely emptied during the transmission, the subsequent packets are kept in the packet buffer to give the bucket time to accumulate new credits. When new tokens are available, the transmission can recommence. If, on the contrary, the bucket reaches b bytes of credits, it stops being fed. An additional constraint imposes to the admitted traffic rate not to go over the peak rate p in any case. The DLB described above, shown in Figure 3, is named ***DLB with delayed control*** and it realizes a delayed control on the incoming packets, buffering those which cannot be transferred due to the lack of tokens in the bucket. Packets that cannot be stored anymore in the buffer hereafter are considered non-compliant.

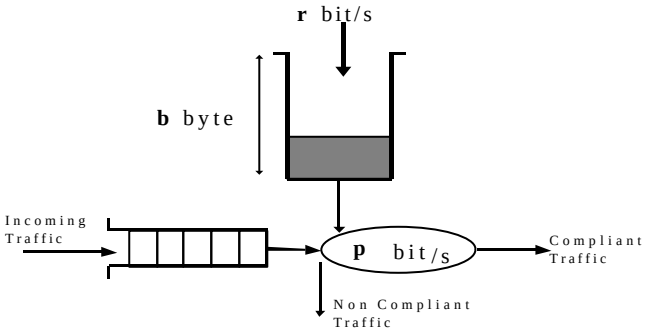

Figure 3: The dual leaky bucket model

The main difference between the traditional model and the one which has been selected in the BRAHMS architecture (called **"DLB with instantaneous control"**) is that the algorithm is performed for each incoming packet, in order to decide as promptly as possible if there are enough tokens to sent the packet. In other words, when a packet arrives at the DLB, the algorithm is performed to decide if it respects the nominal average and peak rates, taking into account the previous packet arrivals. While the algorithm is running, the packet is stored in an input queue, that should not have more than one packet at any time. If the packet can be sent, it is immediately transferred to the DLB output queue, otherwise it is immediately transferred to the overflow queue. Unlike the traditional implementation,

packets that cannot be sent immediately are not put in the input queue waiting for the DLB to gain enough tokens. As it will be clearer in the simulation results, this strategy makes it possible to obtain a sharper distinction between compliant traffic from non-compliant one, with respect to the traditional implementation. In the proposed approach, thanks to the better performance as concerns compliant traffic treatment, end-to-end delays control is made easier, making it possible, at the same time, to send more non-compliant traffic in order to maximize throughput.

V. EDF Scheduler

The Earliest Deadline First (EDF) scheduler is a dynamic priority scheduler as packet's priority is decided at its arrival. More precisely, upon packet arrival, it is assigned a *deadline* which the sum of its *arrival time* and the *delay guarantee* associated with the flow (characterized by peak rate, average rate and burst size) the packet belongs to. The EDF scheduler selects the packet with the smallest deadline for transmission on the considered link.

The dynamic nature of the priority in the EDF scheduler is evident from the fact that the priority of the packet increases with the amount of time it spends in the system. This ensures that packets with loose delay requirements obtain better service than they would in a static priority scheduler without affecting delay guarantees of other flows.

An advantage of EDF is to minimize the maximum latency of packets. Here, *latency* is defined as the difference between the deadline of a packet and the time it is actually transmitted on the link.

Besides its simplicit, the main advantage of the EDF policy is that it allows the separation of delay and throughput guarantees for a flow.

As it will be illustrated through simulation results, Voice applications, which are among the most delay-sensitive sources, can guaranteed of their complete bandwidth, i.e. they can transmit at their peak rate without receiving interference from the remaining queues.

The result of this dynamic share is that, even if a queue can sometimes be assigned a greater bandwidth, in the steady state, delay-insensitive queues are assigned an amount of bandwidth equal to the average rate of the correspondent sources (see Figure 4).

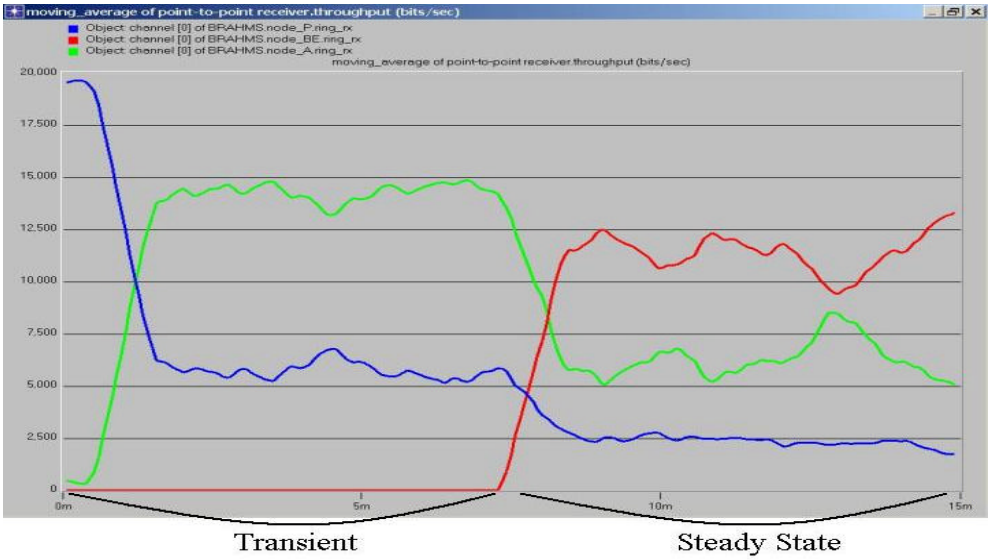

Figure 4: Example of bandwidth partion

In the steady state the output available bandwidth is partitioned proportionally to the incoming rate, as shown on the left-hand side of **Figure 4**. On the other
hand, in the transient period, or after a period in which sources have emitted data packets below their average rate, the spare bandwidth is given to sources with tighter delay constrains, i.e. with an inferior static priority value.

VI. Simulation Results

In this section, the results of the OPNET simulations are discussed. The behaviour of the two different DLB models described before are first compared. Afterwards, it will be shown how it is possible to respect the delay constrains for all the IntServ and DiffServ services.

It is worth point out that the DLB with instantaneous control is used only for Premium Service, Guaranteed Service and Assured Service (the latter in an aggregate way), while the DLB with delayed control is used with Controlled Load Service for traffic shaping thus allowing a greater number of packets to be ready for the transfer from the input DLB queue to the output DLB queue, being treated as compliant.

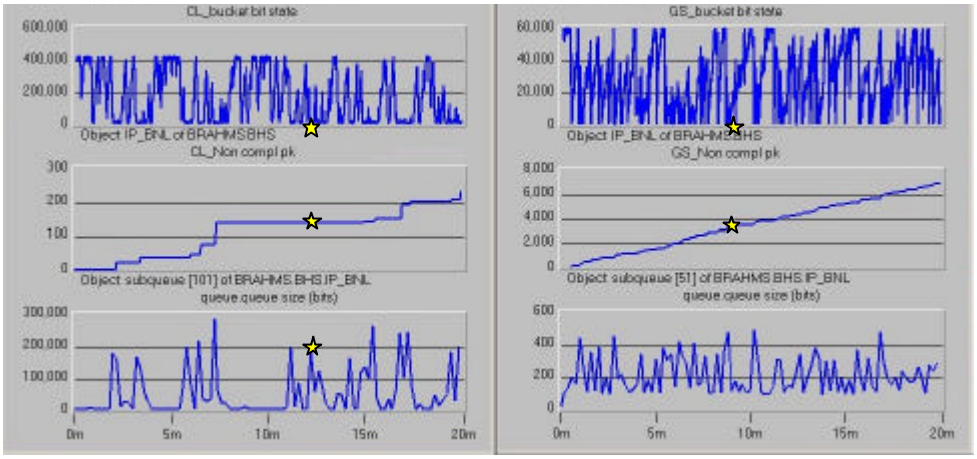

Figure 5: DLB with delayed and instantaneous control performances

Figure 5 shows a comparison between the DLB with
delayed control, used in this case for Controlled Load Service, and the DLB with instantaneous control, used for Guaranteed Service.

The top windows of the two figures show the number of bits present in the DLB token bucket at a given time, while in the second one the number of non-compliant packets, sent to the overflow queues, is represented.

It is worth remarking that in the DLB with delayed control it might happen that, although the bucket is empty and the source is sending packets (as it can be seen in third windows on the left-hand side in the highlighted yellow points), no packets are sent to the overflow queue (the profile of non-compliant packets remains flat).

This cannot happen in the DLB with instantaneous control, in which the input DLB queue is always empty (as it can be seen in the third windows on the right-hand side in the highlighted yellow points). With the proposed DLB implementation, on packet arrival, if there are no tokens in the bucket, the packet is immediately sent in the overflow queue.

In the designed traffic control an optimisation of bandwidth allocation for Assured and Premium aggregated Services has been proposed. This optimisation concerns the dynamic allocation of bandwidth consequent to a new flow arrival at the BHS. Instead of allocating statically all the bandwidth according to the SLA for Assured and Premium Services, a new portion of bandwidth is allocated each time a new flow is detected.

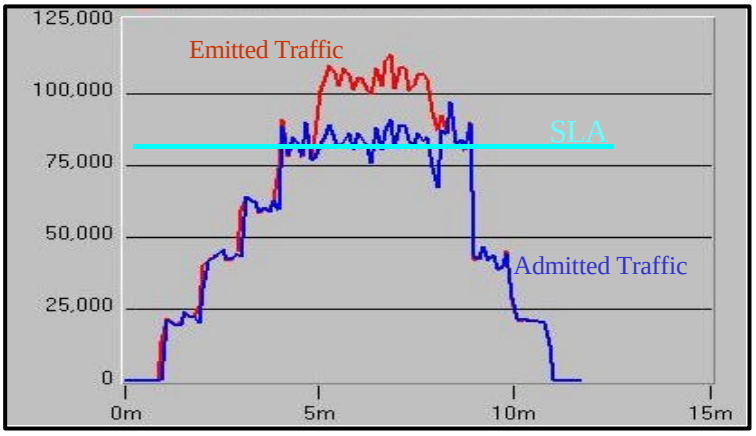

Figure 6: Dynamic allocation of bandwidth for aggregated Services

Figure 6 shows the allocation of bandwidth in the case of five different sources emitting towards the same BHS. In the considered example, only four out of these five can be accepted according to the static SLA.

The main result of the simulation is that with the proposed combined IntServ-DiffServ Traffic Control architecture it is possible to respect all the quality requirements for different flows.

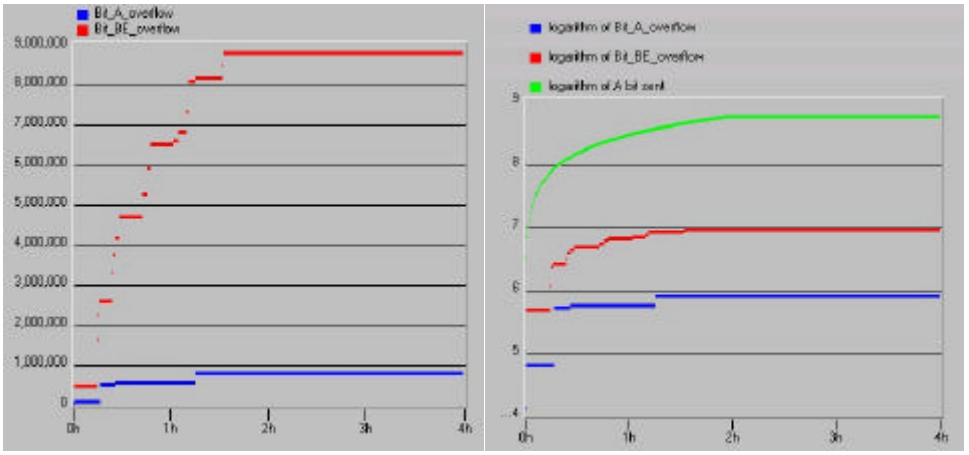

Figure 7:Number of discarded bit for Assured Service and Best Effort

Figure 7 illustrates the different levels of discarded bit for Assured and Best Effort Services. As it is clearly shown the percentage of Assured bits discarded is much lower than the percentage of Best Effort one, being the number of bits sent the same for both services, as it was required in the DiffServ Two Bit specification.

In the left windows of Figure 8 the number of non-compliant bits discarded for CL service is shown while the right one shows the number of non-compliant packets expired for GS service (GS packets have been assumed having a constant bit size). With reference to these graphs it is worth observing that all the compliant packets of both services can be sent, while a considerable percentage of the packets that are classified by the DLBs as non-compliant can be prevented from being discarded

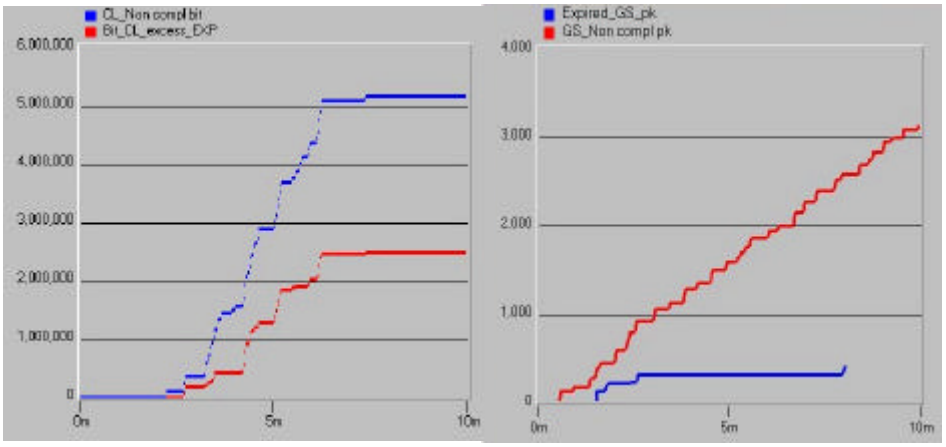

Figure 8: Number of expired packets for GS and discarded bit for CL

Figure 9 shows the performances of IntServ and DiffServ flows with respect to the transfer delay. As it is evident from the figure, the different classes of service can be properly differentite with respect to transfer delay, including in the simulation the GEO satellite propagation delay.

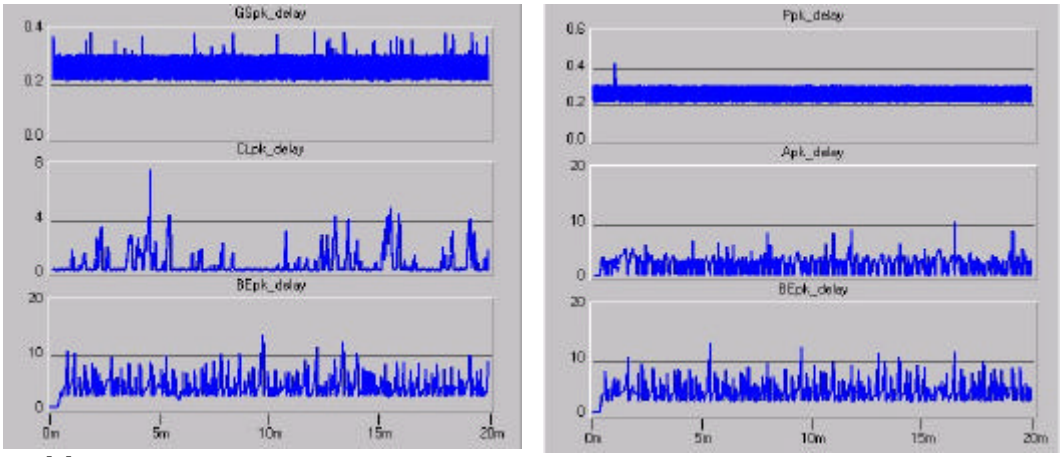

Figure 9: Delay Results for the IntServ flows and DiffServ packet

References

[IETF RFC 1633] Braden, R., Clark, D. and S. Shenker, "Integrated Services in the Internet Architecture: An Overview", RFC 1633, July 1994.

[IETF RFC 2205] Braden, B., Zhang, L., Berson S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[IETF RFC 2211] Wroclawski, J., "Specification of the Controlled-Load Network Element Service", RFC 2211, September 1997.

[IETF RFC 2212] Shenker, S., Partridge, C., and R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997.

[IETF RFC 2474] Nichols K., Blake, S., Baker, F. and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[IETF RFC 2475] Blake S., Black, D., Carlson, M., Davies, E., Wang, Z. and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[IETF RFC 2638] K. Nichols, V. Jacobson, and L. Zhang, "A Two Bit Differentiated Services Architecture for the Internet", RFC 2638, November 1997.

[ELWALID] A.Elwalid and D. Mitra, "Traffic Shaping at a Network Node: Theory, Optimum Design, Admission control".