Issues In Differentiated Services: A Review

Pawansupreet Kaur/ Student of MTech
Student of Computer Science and Engineering Department
SBS College of Engineering and Technology, PTU
Ferozepur, India
Meens399@gmail.com

Monika Sachdeva/Assistant professor
Assistant Professor of Computer Science and Engineering
SBS College of Engineering and Technology, PTU
Ferozepur, India
Monika.sal@rediffmail.com

Abstract- Differentiated services is the most advanced method for traffic management. Differentiated services utilize 6 bits of the 8 bit type of service field of the IP header. This allows up to 64 possible classes. In Differentiated Services this field is referred to as differentiated services code point. Differentiated Services standards define two types of per hop behaviors (PHB's): Expedited forwarding and Assured forwarding. EF is the highest priority traffic. Packets marked with EF PHB should be forwarded with highest rate or rate equal to its arrival. AF defined four classes with three drop precedence.

Edge routers perform two main functions, traffic classification and traffic conditioning, also known as admission control. Both functions are governed by service level agreement (SLA). Generally, packets conforming to SLA are considered as in-profile and packets exceeding SLA are considered as out of profile. The classification process examines incoming packets at the ingress routers against the rules specified by SLA. Packets are assigned the appropriate class (EF or one of the AF classes) by marking them with corresponding DSCP field value. The conditioning process ensures that flows stay within the SLA. Depending on flow characteristics and network conditions, out-of-profile packets are marked with higher drop precedence, delayed in the queue or dropped. A commonly used admission control technique is token bucket algorithm. With complexity pushed to edge routers, core routers have simpler functions in Differentiated Services. PHB's are defined for each class. The router simply checks DSCP field and performs the appropriate action.

Keywords-Diffser; Assured forwarding; scheduling; Quality of service; fairness;

I. INTRODUCTION

The Internet was designed as a best effort network for transporting computer-to-computer traffic. However, as the footprint of the Internet grew, a wide variety of applications emerged. The growth in the diversity and volume of Internet applications made it essential to discover and implement new techniques that support different levels of service for different classes of traffic. These techniques are collectively referred to as Quality of Services (QoS) techniques.

They are generally classified into micro-level or fine grained techniques and macro-level or coarse grained techniques [1]. Micro level techniques operate at the flow level. Routers need to keep track of the status of each flow during the connection lifetime. This results in a better service quality but involves design complexities and processing overhead [2]. Macro level techniques attempt to overcome these complexities by operating at a higher aggregate or class level rather than on the flow level. The Integrated Services (IntServ) architecture is an example of micro-level techniques. In IntServ, not only the flow states need to be maintained by each router, but also end-to-end resources need to be reserved for each flow during the lifetime of the connection. IntServ is obviously unsuitable for large scale networks, including the Internet. In such networks, it is difficult for routers to keep track of the large volume of active flows. Resource reservation is also inefficient, especially in under provisioned networks. The Differentiated Services (DiffServ) architecture [3] has been designed to overcome the scalability problems of IntServ. DiffServ is a macro-level approach. In DiffServ, flows are assigned to classes and each class gets a different level of service. However, there is no differentiation between flows within the same class, except for the drop precedence. As a result, many fairness problems have been observed and discussed in published literature. These include fairness between TCP and UDP flows sharing the same class, and fairness between TCP flows with different parameters (window sizes, round-trip times) sharing the same class [4, 5]. In addition, our study has shown that there is unfairness in the bandwidth sharing between UDP flows with disparate packet sizes or arrival rates within the same DiffServ class. While different scheduling mechanisms are employed for managing the queues of different classes, flows within the same class are generally served on a FIFO basis. A large packet waiting in the queue can force many smaller packets to be delayed, which unfairly increases the overall delay of the system.

The rest of this paper is organized as follows. Section 2 provides an overview of the DiffServ architecture. It also discusses its deficiency in handling heterogeneous traffic flows sharing the same class. Section 3 reviews the research work related to this area. Section 4 describes the PER HOP BEHAVIOR in details. Section 5 demonstrates the traffic classification and conditioning. Section 6 describes advantage of the differentiated services. Section 7 describes the issues in differentiated services. And Section 8 concludes the paper.

II. OVERVIEW OF DIFFSER ARCHITECTURE

DiffServ [3]was introduced in the late 1990s in response to the need for a simple, yet effective QoS mechanism suitable for implementation on the Internet. It was realized that the IntServ was too extreme an alternative to the best effort service. In other words, there was a need for a solution that can do a little better than the best effort, while providing a higher level of scalability and simplicity than IntSer [6]. Differentiated services has been proposed as an efficient and scalable traffic management mechanism way to ensure internet QOS. In Differentiated services, traffic flows having similar

QOS requirements is aggregated into common service class at the edge and is forwarded using certain PHB at the core router. The PHB

to be applied is indicated by differentiated services code point value in the IP header of each packet.

Differentiated Services (DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic. Differentiated Services can, for example, be used to provide low latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.

Differentiated Services operates on the principle of *traffic classification [7]*, where each data packet is placed into a limited number of traffic classes. Differentiated Services relies on a mechanism to *classify* and *mark* packets as belonging to a specific class. Each router on the network is configured to differentiate traffic based on its class. Each traffic class can be managed differently, ensuring preferential treatment for higher-priority traffic on the network.

BA (Behavior aggregate) classifier uses only the DSCP to determine the queue to which packet should be directed. Each queue executes a buffer management algorithm to determine whether a packet should be stored or discarded. The packet scheduler determines which queue is to be serviced next. This may be based on the relative priority of the queues, or weighted fair bandwidth sharing policy or some other policies. The scheduler in fact determines the bandwidth bet flow out of the queue. Bandwidth allocation, queuing delay and packet loss are some characteristics metrics to specify certain level of PHB forwarding. While Differentiated Services does recommend a standardized set of traffic classes [7].

A. Classification and Router operations

DiffServ utilizes 6 bits of the 8-bit Type of Service (TOS) field of the IP header [8]. This allows up to 64 possible classes. In DiffServ, this field is referred to as Differentiated Service Code Point (DSCP) or forwarding class. Some DSCP values are reserved for different purposes. DiffServ standards define two types of per hop behaviors (PHBs): Expedited Forwarding (EF) [9], and Assured Forwarding (AF) [10]. EF is the highest priority traffic. Packets marked with EF PHB should be forwarded at a higher or at least equal rate as its arrival rate. AF defines four classes with three drop precedence levels for each class.

Edge routers perform two main functions, traffic classification and traffic conditioning, also known as admission control. Both functions are governed by the Service Level Agreement (SLA). Generally, packets conforming to SLA are considered in-profile and packets exceeding SLA are considered out-profile. The classification process examines incoming packets at the ingress router against the rules defined by SLA. Packets are assigned the appropriate class (EF or one of the AF classes) by marking them with the corresponding DSCP field value. The conditioning process ensures that flows stay within the SLA. Depending on flow characteristics and network conditions, out-profile packets are either marked with higher drop precedence, delayed in the queue or dropped [6]. A commonly used admission control technique is the Token Bucket algorithm [11].

With complexity pushed to edge routers, core routers have simpler functions in DiffServ. PHB actions are defined for each class. The router merely checks the DSCP field and performs the appropriate action. Queue management and scheduling techniques are used at both edge and core routers.

B. Diffser Deficiencies in Handling Heterogenous Traffic

Despite its success as a scalable QoS architecture, Diff-Serv suffers from some deficiencies that have been identified in published literature. In particular, several fairness problems have been pointed out [12-16]. These problems fall under two categories, inter-class fairness and intra-class fairness [13]. Inter-class fairness refers to the fair share of resources (queue size and bandwidth) between different AF classes. It also includes the sharing of excess bandwidth when the network is underutilized. Some studies have shown that flows in a higher class can get worse performance than flows in lower class due to unbalanced distribution of bandwidth [14]. Intra-class fairness refers to the fair sharing of resources between different flows in the same AF class. Flow-based QoS cannot be guaranteed because Diff-Serv routers do not keep track of individual flows. In heterogeneous networks, different types of flows may share the same DiffServ class, e.g., TCP flows with different window sizes, a mix of TCP and UDP flows, or UDP flows with different average packet sizes. In all of these and other scenarios, some flows will gain higher bandwidth than others, although they have the same service priority. The main cause of intra-class fairness problems is the aggregate nature of DiffServ. This type of unfairness may be unavoidable because of the framework of DiffServ. However, some of these problems can be alleviated using efficient scheduling mechanisms.

III. RELATED WORK

One of the more challenging research issues in Differentiated Services networks is the fair distribution of bandwidth among aggregates sharing the same AF class. Several studies have shown that the number of Micro flows in aggregates, the round trip time, the mean packet size and TCP/UDP interactions are key factors in the throughput obtained by aggregates using this architecture. AFC (Aggregate Flow Control) is an edge-to-edge control mechanism that combined with Differentiated Services traffic conditioning, addresses these fairness issues for AF-based services. The AFC mechanism is based on some control TCP connections associated with each customer's traffic aggregate.

Fairness requirements of assured services cannot be met under some circumstances. Via simulation studies, these works confirm that the number of micro flows in aggregates, the round trip time and the mean packet size are critical factors for the fair distribution of bandwidth among competing aggregates belonging to the same AF class. Additionally, the interaction between responsive TCP traffic and unresponsive UDP traffic impacts the TCP traffic in an adverse manner.

Many smart packet marking mechanisms have been proposed to overcome these fairness issues. Adaptive Packet Marking (APM) [12] is one of these schemes able to provide soft bandwidth guarantees, but it has to be implemented inside the TCP code itself and thus, requires varying all TCP agents. Intelligent traffic conditioners proposed in handle a subset of these fairness problems using a simple TCP model when marking packets. However, these conditioners require external inputs and cooperation among markers for different aggregates complicating both implementation and deployment.

Another marking algorithm based on a more complex TCP model is Equation-Based Marking (EBM). This scheme solves the fairness problems associated with heterogeneous TCP flows under diverse network conditions. EBM behavior depends on the quality of the estimation of the current loss rate seen by TCP flows. Unfortunately, the calculation of this estimate is not an easy problem and complicates the deployment of the scheme extremely.

An RTT-RTO (RTT-Retransmit Time Out) aware conditioner is proposed, but this scheme only mitigates RTT bias. A different

approach consists of addressing these problems by enhanced RIO queue management.

IV. PER HOP BEHAVIOR

The differentiated services architecture introduced the concept of PHB at different routers in DS domain with the aim of providing quality of service for different kinds of traffic [3].

The Per-Hop Behavior is determined by the differentiated services (DS) field of the IPv4 header or IPv6 header. The DS field consists of a 6-bit differentiated services code point value. PHB's are implemented in nodes by means of some buffer management and packet scheduling algorithm. A PHB is selected at node by mapping of the DS code point in a received packet. Standardized PHBS have recommended code point. All code points must be mapped to some PHB; in the absence of some local policy, code points which are not mapped to a standardized PHB in accordance with that PHB specification should be mapped to default PHB.

In theory, a network could have up to 64 (i.e. 2^6) different traffic classes using different markings in the DSCP. The Differentiated Services RFCs recommend, but do not require, certain encodings. This gives a network operator great flexibility in defining traffic classes. In practice, however, most networks use the following commonly-defined Per-Hop Behaviors:

- Default PHB (Per hop behavior)—which is typically best-effort traffic.
- Expedited Forwarding (EF) PHB—dedicated to low-loss, low-latency traffic.
- Assured Forwarding (AF) PHB—gives assurance of delivery under prescribed conditions.

A. Default PHB

A default PHB is the only required behavior. Essentially, any traffic that does not meet the requirements of any of the other defined classes is placed in the default PHB. Typically, the default PHB has best-effort forwarding characteristics. The recommended DSCP for the default PHB is '000000' (in binary).

B. Expedited Forwarding

The IETF defines Expedited Forwarding behavior [9]. The EF PHB has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for voice, video and other real time services. EF traffic is often given strict priority queuing above all other traffic classes. Because an overload of EF traffic will cause queuing delays and affect the jitter and delay tolerances within the class, EF traffic is often strictly controlled through admission control, policing and other mechanisms. Typical networks will limit EF traffic to no more than 30%—and often much less—of the capacity of a link. This also has been defined as the PREMIUM SERVICE, which requires that customers generate traffic with fixed peak bit rate specified by SLA. The customer is responsible for not exceeding contracted peak rate, otherwise excess traffic will be dropped. The ISP guarantees that contracted bandwidth will be available when traffic is sent. The premium service is suitable for internet telephony, video conferencing, and other mission critical services.

This can be implemented as follows: at the customer side, some entity will decide which application flows can use the premium service, the leaf nodes directly connected to the senders will classify and shape the traffic. Traffic shaping is necessary to avoid packet dropping by forcing the traffic in compliance with SLA. After the shaping, the DSCP code for EF PHB is tagged to the packets. At the provider side, the ingress routers will police the traffic. Excess traffic is dropped. All packets with the EF DSCP will enter the premium queue and all packets with AS DSCP enter an assured queue. Packets in the former queue will be sent before the packets in latter queue. As the premium traffic can potentially use the 100% of the bandwidth of the link, it is necessary to limit the traffic in order to avoid the compete starvation of the low priority assured service and to avoid low resource utilization due to peak rate bandwidth allocation. The recommended DSCP for expedited forwarding is 101110_B (46 or $2E_H$).

C. Assured Forwarding

Assured forwarding allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs. Assured service is intended for customers that need reliable services, even during network congestion.

The AF behavior group defines four separate AF classes [10]. Each class is given a certain amount of buffer space and interface bandwidth, dependent on the SLA with the service provider/policy. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from AF11 through AF43.

AF Forwarding Behavior Group

	Class 1	**Class 2**	**Class 3**	Class 4
Low Drop	AF11	AF21	AF31	AF41
Med Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

Some measure of priority and proportional fairness is defined between traffic in different classes. Should congestion occur *between* classes, the traffic in the higher class is given priority. If congestion occurs *within* a class, packets with high drop precedence are discarded first. the Assured service is implemented as follows: firstly classification, DSCP marking, and policing are done at the ingress routers of ISP networks. If the assured service traffic does not exceed the bit rate specified by SLA, it is considered in profile, otherwise excess packets are considered out-of-profile. One bit in the AF DSCP can be used to differentiate in and out packets, secondly, all packets in and out are put into the same queue to avoid out of order delivery. Thirdly queue is managed by queue management scheme called random early detection (RED) with In and Out (RIO).

RED is queue management scheme that drops packets randomly[17]. This will prevent the TCP flow control mechanisms at different hosts to reduce transmissions rate at different times. By doing so, RED can prevent the queue at the routers from overflowing, and therefore avoid the tail drop behavior (avoiding all the subsequent packets when queue overflows). It causes network utilization to oscillate and can degrade performance significantly. Red has been proven to be useful and widely deployed.

RIO is more advanced RED scheme [18]. It basically maintains two RED algorithms, one for in packets and one for out packets. There are two thresholds for each queue. When the queue size is below the first threshold, no packets are dropped, when the queue size is between the two thresholds only out packets are randomly dropped, when the queue size exceeds the second threshold, indicating possible network congestion, both in and out packets are randomly dropped, but out packets are dropped more aggressively.

As resources are allocated to in packets with priority during congestion, the customers will perceive a predictable service from the

network if they keep the traffic in-profile. When there is no congestion, out packets will also be delivered.

Rather than using strict priority queuing, more balanced queue servicing algorithms such as fair queuing or weighted fair queuing are likely to be used. To prevent issues associated with tail drop, the random early detection (RED), RED for In and Out (RIO) .

Usually, traffic policing is required to encode drop precedence. Typically, all traffic assigned to a class is initially given low drop precedence. As the traffic rate exceeds subscription thresholds, the police will increase the drop precedence of packets that exceed the threshold.

V. TRAFFIC CLASSIFICATION AND CONDITIONING

Differentiated services are extended across a DS domain boundary by establishing a SLA between an upstream network and a downstream DS domain [19]. The SLA may specify packet classification and re-marking rules and may also specify traffic profiles and actions to traffic streams which are in or out-of-profile. The TCA between the domains is derived (explicitly or implicitly) from this SLA.

The packet classification policy identifies the subset of traffic which may receive a differentiated service by being conditioned and/or mapped to one or more behavior aggregates (by DS code point re- marking) within the DS domain.

Traffic conditioning performs metering, shaping, policing and/or re-marking to ensure that the traffic entering the DS domain conforms to the rules specified in the TCA, in accordance with the domain's service provisioning policy. The extent of traffic conditioning required is dependent on the specifics of the service offering, and may range from simple code point re-marking to complex policing and shaping operations.

A. Classifiers

Packet classifiers select packets in a traffic stream based on the content of some portion of the packet header. We define two types of classifiers. The BA (Behavior Aggregate) Classifier classifies packets based on the DS code point only. The MF (Multi-Field) classifier selects packets based on the value of a combination of one or more header fields, such as source address, destination address, DS field, protocol ID, source port and destination port numbers, and other information.

Classifiers are used to "steer" packets matching some specified rule to an element of a traffic conditioner for further processing. Classifiers must be configured by some management procedure in accordance with the appropriate TCA.

B. Traffic Profile

A traffic profile specifies the temporal properties of a traffic stream selected by a classifier. It provides rules for determining whether a particular packet is in-profile or out-of-profile. For example, a profile based on a token bucket may look like:

Code point=X, use token-bucket r, b

The above profile indicates that all packets marked with DS code point X should be measured against a token bucket meter with rate r and burst size b. In this example out-of-profile packets are those packets in the traffic stream which arrive when insufficient tokens are available in the bucket.

Different conditioning actions may be applied to the in-profile packets and out-of-profile packets, or different accounting actions may be triggered. In-profile packets may be allowed to enter the DS domain without further conditioning; or, alternatively, their DS code point may be changed. The latter happens when the DS code point is set to a non-Default value for the first time [DSFIELD], or when the packets enter a DS domain that uses a different PHB group or Code point->PHB mapping policy for this traffic stream. Out-of-profile packets may be queued until they are in-profile (shaped), discarded (policed), marked with a new code point (re-marked), or forwarded unchanged while triggering some accounting procedure. Out-of-profile packets may be mapped to one or more behavior aggregates that are "inferior" in some dimension of forwarding performance to the BA into which in-profile packets are mapped. A traffic profile is an optional component of a TCA and its use is dependent on the specifics of the service offering and the domain's service provisioning policy.

C. Traffic Conditioners

A traffic conditioner may contain the following elements: meter, marker, shaper, and dropper. A traffic stream is selected by a classifier, which steers the packets to a logical instance of a traffic conditioner. A meter is used (where appropriate) to measure the traffic stream against a traffic profile. The state of the meter with respect to a particular packet (e.g., whether it is in- or out-of-profile) may be used to affect a marking, dropping, or shaping action. When packets exit the traffic conditioner of a DS boundary node the DS code point of each packet must be set to an appropriate value.

Fig. shows the block diagram of a classifier and traffic conditioner. Note that a traffic conditioner may not necessarily contain all four elements. For example, in the case where no traffic profile is in effect, packets may only pass through a classifier and a marker.

1) Meters:

Traffic meters measure the temporal properties of the stream of packets selected by a classifier against a traffic profile specified in a TCA. A meter passes state information to other conditioning functions to trigger a particular action for each packet which is either in- or out-of-profile (to some extent).

2) Markers:

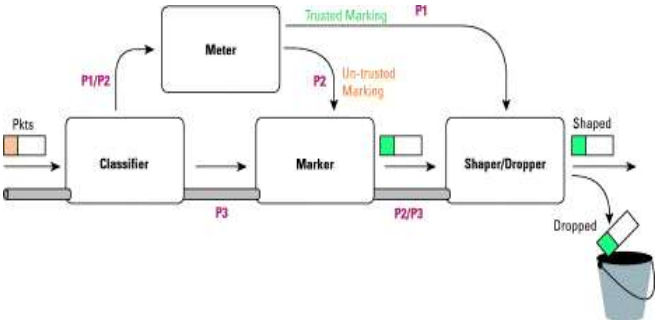
Packet markers set the DS field of a packet to a particular code point, adding the marked packet to a particular DS behavior aggregate. The marker may be configured to mark all packets which are steered to it to a single code point, or may be configured to mark a packet to one of a set of code points used to select a PHB in a PHB group, according to the state of a meter. When the marker changes the code point in a packet it is said to have "re-marked" the packet.

3) Shapers:

Shapers delay some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. A shaper usually has a finite-size buffer, and packets may be discarded if there is not sufficient buffer space to hold the delayed packets.

4) Droppers:

Droppers discard some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. This process is known as "policing" the stream. Note that a dropper can be implemented as a special case of a shaper by setting the shaper buffer size to zero (or a few) packets.



D. Packet Scheduling Mechanisms

Packets that are ready for forwarding or delivery are placed into egress queue. The queues are then serviced according to predefine configurable scheduling method. Scheduling is also called egress queuing or congestion management.

The most common queuing mechanism for the output queue of a router or a switch or a router from a differentiated services perspective are as follows:

1) FIFO (First in first out): A work conserving, network-independent scheduler, considered as default choice of a typical router [20]. In FIFO packets that wants to use an output link are placed into output queue in the order in which they are arrive. FIFO offers high cost efficiency and no versatility.

2) PQ (Priority Queuing): A work conserving, network-independent and priority based scheduler [20]. A single queue is used for every QOS class and they are served by strict priority discipline; that is low priority packets are served if the high priority queues are empty. PQ offers inflexible versatility and with a possibility of resource starvation to all but highest priority class.

3) WFQ (Weighted Fair Queuing)

A work conserving, network-independent and priority based scheduler. A class –based WFQ [21] is used and made public by CISCO Systems. In class based WFQ packets are assigned to different queues based on the value of DS field. A weight is specified for each class and in periods of congestion, each class is assigned a percentage of output bandwidth equal to the weight of class. Higher DS field packets will be treated with more priority and lesser DS field packets will be treated with less priority. When the interface is not congested queues can use any available bandwidth .WFQ offers fairness and versatility by providing minimum bandwidth share for each service class.

4) CBQ (Class Based Queuing): A work conserving, network-independent and priority based scheduler. It is an attempt to provide fairness by prioritizing service classes, while not allowing any of the class of traffic to monopolize system resources and bandwidth. In addition, CBQ [22] is designed to support link-sharing which allows resource sharing among traffic classes. The packet scheduling is decomposed into two types of schedulers, the general scheduler and link sharing scheduler.

E. Congestion Avoidance

Switch port queues function to provide space for packets waiting to be transmitted when the port cannot transmit them immediately. if a port becomes congested the queue begins to fill. What happens the congestion is severe enough that the queue fill to capacity? New packets to be forwarded cannot be stored in a queue and must be dropped.

Somehow, a switch must anticipate or avoid severe congestion in advance using one of the following available methods:

- Tail Drop
- Weighted Random Early Detection

VI. ADVANTAGES

Under Differentiated Services, all the policing and classifying is done at the boundaries between Differentiated Services domains. This means that in the core of the Internet, routers are unhindered by the complexities of collecting payment or enforcing agreements. That is, in contrast to Integrated Services, Differentiated Services requires no advance setup, no reservation, and no time-consuming end-to-end negotiation for each flow.

VII. ISSUES

A. Fair distribution of bandwidth among aggregate sharing the same AF class

One of the more challenging research issues in Differentiated Services networks is the fair distribution of bandwidth among aggregates sharing the same AF class.. Fairness requirements of assured services cannot be met under some circumstances. Some studies have shown that, the number of micro flows in aggregates, the round trip time and the mean packet size are critical factors for the fair distribution of bandwidth among competing aggregates belonging to the same AF class.

Additionally, the interaction between responsive TCP traffic and unresponsive UDP traffic impacts the TCP traffic in an adverse manner.

B. End to End and Peering Problems

The details of how individual routers deal with the DSCP field is configuration specific, therefore it is difficult to predict end-to-end behavior. This is complicated further if a packet crosses two or more Differentiated Services domains before reaching its destination.

From a commercial viewpoint, this is a major flaw, as it means that it is impossible to sell different classes of end-to-end connectivity to end users, as one provider's Gold packet may be another's Bronze. Internet operators could fix this, by enforcing standardized policies across networks, but are not keen on adding new levels of complexity to their already complex peering agreements. One of the reasons for this is set out below.

Differentiated Services or any other IP based QOS marking does not ensure quality of the service or a specified service level agreements (SLA). By marking the packets, the sender indicates that it wants the packets to be treated as a specific service, but it can only hope that this happens. It is up to all the service providers and their routers in the path to ensure that their policies will take care of the packets in an appropriate fashion.

C. Effect of Dropped Packets

Dropping packets wastes the resources that have already been expended in carrying these packets so far through the network. Dropping packets amounts to betting that congestion will have

resolved by the time the packets are re-sent, or that (if the dropped packets are TCP Datagram) TCP will throttle back transmission rates at the sources to reduce congestion in the network. The TCP congestion avoidance algorithms are subject to a phenomenon called TCP global synchronization unless special approaches (such as Random early detection) are taken when dropping TCP packets. In Global Synchronization, all TCP streams tend to build up their transmission rates together, reach the peak throughput of the network, and all crash together to a lower rate as packets are dropped, only to repeat the process.

VIII. CONCLUSIONS

Differentiated Services Architecture achieves scalability by aggregating traffic classification state which is conveyed by means of IP-layer packet marking using the DS field [DSFIELD]. Packets are classified and marked to receive a particular per-hop forwarding behavior on nodes along their path. Network resources are allocated to traffic streams by service provisioning policies which govern how traffic is marked and conditioned upon entry to a differentiated Services capable network, and how that traffic is forwarded within that network.

A wide variety of services can be implemented on top of these building blocks including classification, marking, policing, and shaping operations to achieve the desired traffic conditioning and PHB.

REFERENCES

[1] U. Payer, "DiffSer, IntSer, MPLS", WWW.iaik.tu-graz.ac.at/traching.

[2] R. Mahajan, S. Floyd, "Controlling High Bandwidth Flows at the Congested Router", AT& T Center for Internet Research ICSI Technical Report TR-01-001, April 2001.

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

[4] C. Kim, Y. Kim, D. Montgomery, "Fairness-guaranteed per-Classtype Queueing and Hierarchical Packet Scheduling for DiffServaware- MPLS Network", IEEE Globecom 2004, Dallas, TX, USA, 2004, pp. 1718–1722.

[5] L. Dong, M. Robert, "Dynamics of Random Early Detection", Proceedings of the ACM SIGCOMM'97 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, ACM Press, Cannes, France, 1997.

[6] Z. Wang, "Internet QoS Architectures and Mechanisms for Quality of Service", Morgan Kuffmann Publishers, California, USA, 2001.

[8] ISI, "Internet Protocol – DARPA Internet Program Protocol Specification", RFC 791, January 1981.

[7] Kalevi Kilkki "Differentiated Services for the Internet" Macmillan Technical Publishing, Indianapolis, IN, USA, June 1999, is available in pdf-format..

[9] V. Jacobson, K. Nichols, K. Poduri, "An Expedited Forwarding PHB", RFC 2598, June 1999.

[10] J. Heinanen, T. Finland, F. Baker, W. Weiss, J. Wroclawski, AssuredForwarding PHB Group', RFC 2597, June 1999.

[11] G. Armitage, "Quality of Service in IP Networks", Macmillan Technical Publishing, Indiana, USA, 2000.

[12] H.T. Phan, D.B. Hoang, "-DiffServ: A new QoS architecture supporting resources discovery, admission and congestion controls", in: Third International Conference on Information Technology and Applications - ICITA'05, Sydney, Australia, 2005.

[13] Y. Sungwon, D. Xidong, G. Kesidis, C.R. Das, "Providing fairness in DiffServ architecture", in: IEEE Global Telecommunications Conference, GLOBECOM'02, 2002, pp. 1435–1439.

[14] J.-S. Li, C.-S. Mao, "Providing flow-based proportional differentiated services in class-based DiffServ routers", IEEE Proceedings on Communications 151 (1) (2004) 82–88.

[15] M. Li, D.B. Hoang, "Resource discovery and fair intelligent admission control over differentiated services networks for variable-length packets", in: Proceedings of the IEEE 10th Asia-Pacific Conference on Communications, Beijing, China, 2004, pp. 499–503.

[16] A. Sang, H. Zhu, S. Li, "Weighted fairness guarantee for scalable Diff Services Assured forwarding", in: IEEE International Conference on Communications - ICC, 2001, pp. 2365–2369.

[17] S. Floyd, V. Jacobson, "Random early detection gateways for congestion avoidance", IEEE/ACM Transactions on Networking 1 (4) (1998) 397–413.

[18] D. Clark, W. Fang, "Explicit allocation of best effort packet delivery", IEEE/ACM Transactions on Networking 6 (4) (1998) 362–373.

[19] A, DWEKAT ZYAD. "Construction and Evaluation of a Service Level Agreement Test- Bed", Master thesis, North Carolina State University, 2001.

[20] L Kleinrock, "Queuing Systems",Vol.2:Computer Applications, John Wiley & Sons, 1976.

[21] C patridge, "Queuing Systems",Vol.2:Computer Applications, John Wiley & Sons, 1994

[22] S, Floyd. and V. Jacobson, "Link-sharing and Resource Management Models for Packet Networks" IEEE/ACM Trans. Networking, vol. 3, August 1995