DMT: A new Approach of DiffServ QoS Methodology

Rashid Hassani, Amirreza Fazely
Department of Computer Science
University of Rostock
Rostock, Germany
rashid.hassani@uni-rostock.de
amirreza.fazelyhamedani@uni-rostock.de

Peter Luksch, Abbas Malekpour
Department of Computer Science
University of Rostock
Rostock, Germany
peter.luksch@uni-rostock.de
abbas.malekpour@uni-rostock.de

Abstract—**Quality of service (QoS) refers to the ability to provide guarantees w.r.t. to bandwidth, latency, jitter, etc., to certain classes of network traffic. The effectiveness of QoS strategies and their implementation depend on a large number of factors, e.g., the size of the network and the complexity of services the network is intended to provide to users. In this paper, we propose a layered QoS which guarantees that the available bandwidth is assigned to users proportionate to the subscribed bandwidth even in case of congested backbone links. The key issue to achieve this is effective prioritization of management traffic. We have implemented our QoS strategy in a laboratory environment and have monitored its performance under simulated traffic. Our method has significantly reduced the total amount of packet loss. Bandwidth utilization on the congested link was increased by 60 percent.**

Keywords-QoS; traffic management; DiffServ; DMT; BGP.

I. INTRODUCTION

By considering the future of the Internet, it will be seriously overburdened by different traffic sources such as real time traffic (e.g., video/voice) and huge traffic generated by e-commerce transactions. In this variety of traffic, network congestion is a concern that can bring different problems to any data network. This issue is even more serious when data network should be accessed, managed and monitored from distance. Mostly, on each ISP network, the essential traffic may be considered as management traffic for remote access and controlling the network devices and traffic of voice/video. In order to design a network properly to support management traffic, QoS mechanisms require to be implemented in order to guarantee that management traffic is prioritized properly.

QoS is a technique to prioritize certain classes of traffic while at the same time maximizing resource utilization. It cannot increase the bandwidth capacities, but by using QoS, network administrator priorities the traffic in a way that if a link is congested, they could choose purposely to drop lower priority traffic so the higher priority traffic will be gradually served. Therefore, QoS doesn't help to avoid dropping the traffic, but it can facilitate the traffic flow in such a way that sensitive traffic continually is serving the network.

Management traffic must have highest priority, because resource management, recovery from failure, and other management services can only be effective if they can reliably and quickly reach each device at any time. Integrated Services (IntServ) and Differentiated Services (DiffServ) [2] are two architectures that have been developed by IETF for applying QoS in IP-networks. Based on the researches, DiffServ so called flow aggregation model can offer the same or even better QoS than the reservation based model [6] (i.e., IntServ).

There are many DiffServ QoS techniques available which have been investigated by several projects e.g., RMD [10], IntServ over DiffServ [11], Bandwidth Broker [12] and Pre Congestion Notification (PCN) [13]. RMD has two ways to control network traffic. The first is to control the flows entering the network and the second one is an algorithm that terminates the required amount of flows if the network is congested within the domain. RMD was developed to provide dynamic QoS within a DiffServ network in a scalable way. IntServ over DiffServ is an end-to-end QoS which is applied by using the IntServ model across a network with one or more DiffServ areas. A Bandwidth Broker (BB) is a centralized agent which has information about the bandwidth precedence and policies in a network and assigns bandwidth by considering those policies. There are other architectures that use this technique (BB) for example: the TEQUIL [14], AQUILA [15] and Internet2 QBone [12]. The Pre Congestion Notification (PCN) is a DiffServ technique in which the PCN-enabled Interior nodes try to detect congestions.

Along with consideration of above techniques, we looked for a simple and cost-effective solution to be applicable for the ISP's backbone network especially for the region in which limited bandwidth, highly flooded real time network traffic, network device overhead and lack of redundancy are vital points for that ISP.

We propose a new QoS strategy which is based on the differentiated services mechanism (i.e., a standardized mechanism of classifying and managing network traffic). In our solution, the traffic that enters a DiffServ domain from outside is classified by marks. It has to be decided to what extend this classification is *trusted*. As we use _D_iffServ

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-199-1

with _M_arking and _T_rusting on the backbone, we call our method as **DMT**.

Section II consists of problem statement and its proposed solution. Section III describes the scenario and its implemented procedure in details. Finally, Section IV and V present experimental results and conclusion respectively.

II. PROBLEM STATEMENT AND PROPOSED SOLUTION

In general, this paper tries to provide a solution for the following problem: The ISP which we consider is located in the geographical area in which the ISP's internet bandwidth might be very expensive and the users may experience the lack of bandwidth. The inadequate internet links are regularly congested so the total bandwidth of an area in congested times is distributed to the users proportionate to the subscribed bandwidth. Therefore regarding management and maintenance issues, ISP suffers from lack of bandwidth and redundancy [4]. The resulting solution must fit with the hardware capabilities of the devices, which are used in the network. In this work, there were some vital points that are essential to be considered, such as:

- It should be considered where management traffic originally must be marked, or classified, and which devices should do the marking.
- Different network devices have different traffic management capabilities. Therefore to conquer these differences there should be a way to employ an ordinary packet marking policy.
- When network traffic is transferred between the LAN and WAN, it must be determined how to map marking policies between OSI Layer-2 (Data Link) and Layer-3 (Network) levels.

In order to find and apply the proper QoS mechanism on the network, we considered different solutions. The solution which could provide all requirements, prioritizes the overall traffic flows to ISP nodes in order to facilitate remote management in the network is chosen to be proposed here. Other solutions are either unsuccessful in experiments or incoherent in the existing topology of the network.

III. DMT APPROACH

Nowadays, the routing architecture specially used in internet is based on the *best effort* communication model [8]. For some kinds of traffic like web, best effort is regularly good enough but it does not guarantee actual delivery or timeliness [3]. If packets get lost somewhere on their way to their destination, the end hosts (senders) must retransmit the missing packets. However, specific packets like management traffic require better performance; therefore, this kind of traffic should be considered as the highest possible priority.

The Internet consists of thousands of various networks which are managed and controlled by either a single administrator or institution that is called Autonomous System (AS). BGP (The Border Gateway Protocol) is the routing protocol designed to exchange information between these ASs [5]. There are other routing protocols such as IS-IS, RIP and EIGRP but they cannot operate and be used in the same way and for the same purpose that BGP does [9]. Therefore for this scenario the BGP is employed as a routing protocol between different routers and switches as necessitate of ISP to manage where broadcast packets have to be forwarded.

DiffServ is a widely used networking architecture mechanism for traffic management and provides QoS on modern IP networks. *DiffServ* operates on the standard that is called traffic classification by placing each data packet into a limited number of traffic classes. DiffServ uses the 6 most significant bits field in IP packet header which is called DSCP. DSCP bits are used instead of TOS (Type Of Service) field which is now outdated.

As shown in Figure 1, DiffServ Field has 8 bits which are separated in to two parts; one DSCP with six bits (DS5-DS0) and second ECN with two bits. In the real networks with DiffServ as a QoS mechanism, each packet is marked by using the DiffServ field so that it is given at each network node a specific forwarding behavior.

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Figure 1. DiffServ field

In the architecture of DiffServ, a field called DiffServ field (DS) has been defined, which is replaced the TOS field in IPv4. It is used to decide about packet classification and different traffic conditioning purposes such as metering, policing, marking and shaping.

Table I shows different Precedence Levels which are shown by DSCP decimal for each level.

TABLE I: DSCP different Precedence Levels

Precedence Level	DiffServ Marking	Description
7	DSCP 56 (CS7)	Used for link layer and routing protocol keep alive
6	DSCP 48 (CS6)	Reserved for IP routing protocols
5	DSCP 40 (CS5)	Express Forwarding (EF)
4	DSCP 32 (CS4)	Class 4
3	DSCP 24 (CS3)	Class 3
2	DSCP 16 (CS2)	Class 2
1	DSCP 8 (CS1)	Class 1
0	DSCP 0 (Default)	Best Effort

The usage of the DSCP field can be categorized in to three ways:

- Classifier: Choose a packet by considering the contents of some parts of the packet header and by using the predefined DSCP value.
- Marker: By considering the traffic profile, it will set the DSCP field value.
- Metering: By using the sharper or dropper function, it will check the fulfillment of traffic profile.

The following scenario will clarify the above-mentioned problem.

A. Scenario

The Figure 4 represents the network topology, which is planned for this scenario. The main concern is to provide the way to overcome the management traffic problem in congested links with limited bandwidths. Therefore in our Lab scenario, the links with different bandwidths and network devices are only considered in order to simulate a real world network backbone environment. Other network issues such as routing are not taken in to the consideration.

In order to generate management traffic, we have used two computers and specific network management applications. Different capacities for the used links have been configured and some bottlenecks have been made to observe the efficiency of the QoS mechanism for the congested links. The computer on the left acts as a management server to generate various traffic. We have provided remote access to each device in the network such as routers, switches and etc., in order to monitor, control and manage the network traffic. Some of these operations such as configuration or monitoring could be done either manually (i.e., *telnet* protocol) or planned and implemented automatically by using particular network management software (e.g., Solarwinds application) [1]. Therefore, we have simulated an ISP core network to test guarantee delivery for the management traffic. In order to be sure about service consistency, different types of devices have been used in ISP core such as Cisco/Juniper routers and Switches.

B. Procedure

Before considering actual traffic, we have to classify the important traffic by marking them using DiffServ mechanism. In ordinary way of DiffServ implemented (only Marker) the DSCP and traffic precedence should be defined on all the routers and switches between source and destination. When this QoS method is applied over heavy traffic, the network may experience a very high CPU load on network devices on the path especially when a variety types of traffic have been flooded to them. Therefore, some of the devices may not be able to apply appropriate QoS mechanism on the traffic. However, in our solution, we specified a minimum bandwidth in the links for management traffic on all hops. The management traffic which is created from specific management application (Solarwinds) destined to some particular destinations is marked only at the first hop and then is ***trusted*** by all middle hops. Therefore, as one of the links became congested, the minimum bandwidth over the whole path is preserved for the management traffic.

As shown in Figure 4 the traffic generator client acts as a management server to generate various traffic in particular port such as port 23 for *telnet*. By using the *DiffServ* QoS, the traffic should be marked at the first router and the mark is proceeding along traffic to reach to the destination device. The traffic which is originated from/destined to these computers is marked as '*DSCP CS1*' (Differentiate Service Code Point, first precedence) by using DiffServ method for packet classification. The RFC 5865 "Configuration Guidelines for DiffServ Service Classes" was used as instruction to set the DSCP bits in the IP packet. DSCP defines the relative priority and drop precedence for IP packets in a network. As far as the minimum bandwidth of the link is considered for the management traffic, the management server is simply able to communicate with all devices in the network in spite of any links on the path congested or not. Without this mechanism, this communication will be tremendously slow and undergoes some problems when a link becomes congested.

To examine this scenario, a traffic generator on the management server is installed to create various familiar network traffic such as IP/ICMP/TCP/UDP to congest the links. To make a better conclusion on the QoS result after and before applying it to the traffic, the ping command is used to monitor and clarify the result. So the devices are configured to select the ICMP traffic.

At the first hop, an access-list is configured in the router (Router1-2821) to select which traffic, QoS mechanism should be applied on it. This configuration is applied only once at the first hop. On the middle hops, the other classes are configured supposing that the management traffic is generated and already tagged by *dscp CS1* elsewhere not close to the first hop. This traffic passes through these routers as middle hops so that the required QoS function should be applied on it. The class is used at the same policy-map ultimately; the policy map should be applied on the egress interface of the router as output service policy. On the switch, the configuration undergoes a slight difference. The switch is configured to ***trust*** the DSCP values on some certain interfaces connected to the core network otherwise it resets the DSCP values by default. The bandwidth capacity for the link between the Cisco router (core 7200) and the Juniper is only 2mbps and therefore can be considered as the bottleneck of the network. So when the traffic flows from client to the server (from left to right), the majority of the packet drops happen in Csico router (core 7200). The numbers of packets marked in the first hop (Router1-2821) for the management server are significantly high since the *telnet* and ICMP traffic are generated here to different destinations. When all devises on the network are configured as mentioned above, a traffic generator program which is installed on the Management server starts to generate some TCP traffic along with management traffic to make the connected links to be congested. Meanwhile, to observe the QoS result on the selected traffic, the ping result is monitored on the end-to-end computers.

IV. EXPERIMENTAL RESULTS

To prepare network devices for the test and to choose the management traffic in order to apply the QoS on it, at the router Router1-2821, an access-list is configured and commands are applied only once and at the first hop, as one can see in Figure 2.

```
ip access-list extended MGMTRF_TEST_QOS
permit tcp host 192.168.208.252 any eq telnet
permit tcp host 100.100.100.1 eq telnet host 192.168.208.252
permit icmp any any
```

Figure 2. Defined access list

As Figure 4 shows, the IP address of the host which acts as management server is ‘192.168.208.252’. Therefore, in Figure 2, the second line selects and permits the traffic originated by this host and the third line selects and permits the returning traffic. Fourth line is configured to choose and permit the ICMP traffic.

As one can see in Figure 3, to apply QoS function, the following class/policy-map is defined on the selected traffic.

```
class-map match-all MARK_MGMTRF
match access-group name MGMTRF_TEST_QOS
!
policy-map MGMTRF_OUT
class MARK_MGMTRF
bandwidth 20
set dscp CS1
```

Figure 3. Marking the selected traffic

After all configurations done on the network devices and generating heavy traffic, the ping is performed in one of the computers (management server) to the router. The result of the above test could reveal how successful the solution is. We specified higher priorities to the ICMP packets in order to facilitate the test. The ping times are monitored before and after applying DMT methodology (our proposed solution) for QoS mechanism. Without DMT, result shows that the average ping time never significantly falls from high level (approximately 350ms). However, after applying the DMT methodology on the selected traffic, the ping time significantly drops from 370ms to approximately 6ms (improved by about 85%).

There are several protocols and applications which can be used to create management traffic flow like Telnet, FTP, SMTP, etc. We examined *Telnet* operation, because it performs two important functions: first, it interacts with the user terminal on the local host and second, exchanges messages with the destination Telnet host (i.e., network devices). During the *Telnet* operation, the TCP connection continues for the whole period of the login session. The client and the server retain the connection, even while the user disrupts the transfer of data [7].

Before applying the DMT methodology on the congested link, the *telnet* from the management server to the routers worked extremely slowly; but, after applying the DMT methodology, the *telnet* operations seemed very usual.

Figure 5 and Figure 6 demonstrate the tests we have done to examine the simulated network packet loss before and after applying the DMT methodology respectively. By comparing the graphs, before applying DMT methodology (Figure 5) the average packet loss was extremely high in congested links (up to 85%) but after applying DMT in the network (Figure 6), the loss rate has been significantly reduced (about 25%). Therefore, the bandwidth utilization for defined traffic is highly optimized (about 60 percent).

V. CONCLUSION AND FUTURE WORK

The congestion problem on the low bandwidth links under the heavy traffic situation cannot be avoided. Serving management and maintenance services on the backbone networks over the congested links is a main factor. The defined scenario in this paper demonstrates the effectiveness of the DMT methodology in ISP’s backbone network especially for the region in which limited bandwidth, highly flooded real time network traffic, network device overhead and lack of redundancy are vital points for ISPs. Therefore, DMT can be considered as a cost-effective and profitable *network based policy method* for reliable delivery of QoS by service providers. DMT methodology can be applied on any devices in the core network routers and layer-3 switches when the DSCP field on each packet remains unchanged through the path from base to destination. However, while the DSCP field is unrecognizable on some Layer-2 switches, this QoS mechanism will fail at these devices. Other defined QoS methods for managing the management traffic such as matching the L-3 traffic against the IP access-lists or assigning a fixed bandwidth to the management traffic, either decline the performance or they would be considerably costly comparing to the DMT method.

There are many interesting avenues for future work. In this paper, we have proposed a layered model of policy-based DiffServ QoS management system. We are currently at the stage of implementation this technique in a real more complex multi-domain environment with Linux-based router and also demonstrate the system on laboratory test beds.

Additionally, wireless link capacity is typically a limited resource that requires to be used efficiently. Therefore, it is important to find efficient technique of supporting QoS over wireless channels for real-time data (e.g., live audio/video streams) when capacity of the channels vary for different users. We plan to report outcome on detailed features of the proposed implementation model in future papers.

ACKNOWLEDGMENT

The authors are very grateful to the reviewers for their useful comments and suggestions.

REFERENCES

[1] Solarwinds Technologies, www.solarwinds.com, [retrieved: May, 2012].

[2] J. Polk, and F. Baker, “Configuration Guidelines for DiffServ Service Classes”, RFC 5865, 2010.

[3] N. Ye, E.S. Gel, and X. Li, “Applying scheduling rules from production planning”, Computers & Operations Research, Volume 32, Issue 5, May 2005, pp. 1147–1164.

[4] D.J. Songhurst and P.L. Eardley, "Guaranteed QoS Synthesis for admission control with shared capacity", BT Technical Report TR-CXR9-2006-001, Feb 2006.

[5] Y. Rekhter, and S. Hares, “A Border Gateway Protocol 4 (BGP-4)”, RFC 4271, 2006.

[6] J. Haju and P. Kivimaki, “Co-operation and comparison of DiffServ and IntServ: performance measurements”, ISBN:0-7695-0912-6, 25th Annual IEEE Conference on Local Computer Networks, 2000.

[7] D. Comer, “Internetworking With TCP/IP, Principles, Protocols and Architecture”, ISBN 0-13-187671-6, 5th edition, 2006.

[8] B. Smith and J.L. Aceves, “Best-Effort Quality-of-Service”, ICCCN’08, Aug 2008.

[9] M. Caesar and J. Rexford, “BGP routing policies in ISP networks”, IEEE Network, November/December 2005.

[10] Attila. B, G. Karagiannis ,and L. Westberg, “Qos signaling across heterogeneous wired/wireless networks”, QShine2005, p.p. 51.

[11] Y. Bernet, P. Ford, and R. Yavatkar, “A framework for integrated services operation over diffserv networks”, IETF, Nov 2000.

[12] B.Teitelbaum, S. Hares, and L. Dunn, “Internet2 qbone: Building a testbed for differentiated services”, IEEE Network, Oct 1999, pp. 8–16.

[13] B. Briscoe, P. Eardley, and D. Songhurst, “An edge-to-edge deployment model for pre-congestion notification: Admission control over a diffserv region”, IETF, June 2006.

[14] E. Mykoniati, C. Charalampous, and P. Georgatsos, “Admission control for providing qos in diffserv ip networks: The tequila approach”, IEEE Communications Magazine, Jan 2003, pp. 38–44.

[15] T. Engel, H. Granzer, and M. Winter, “Aquila: Adaptive resource control for qos using an ip-based layered architecture”, IEEE Communications Magazine, Jan 2003, pp. 46–53.

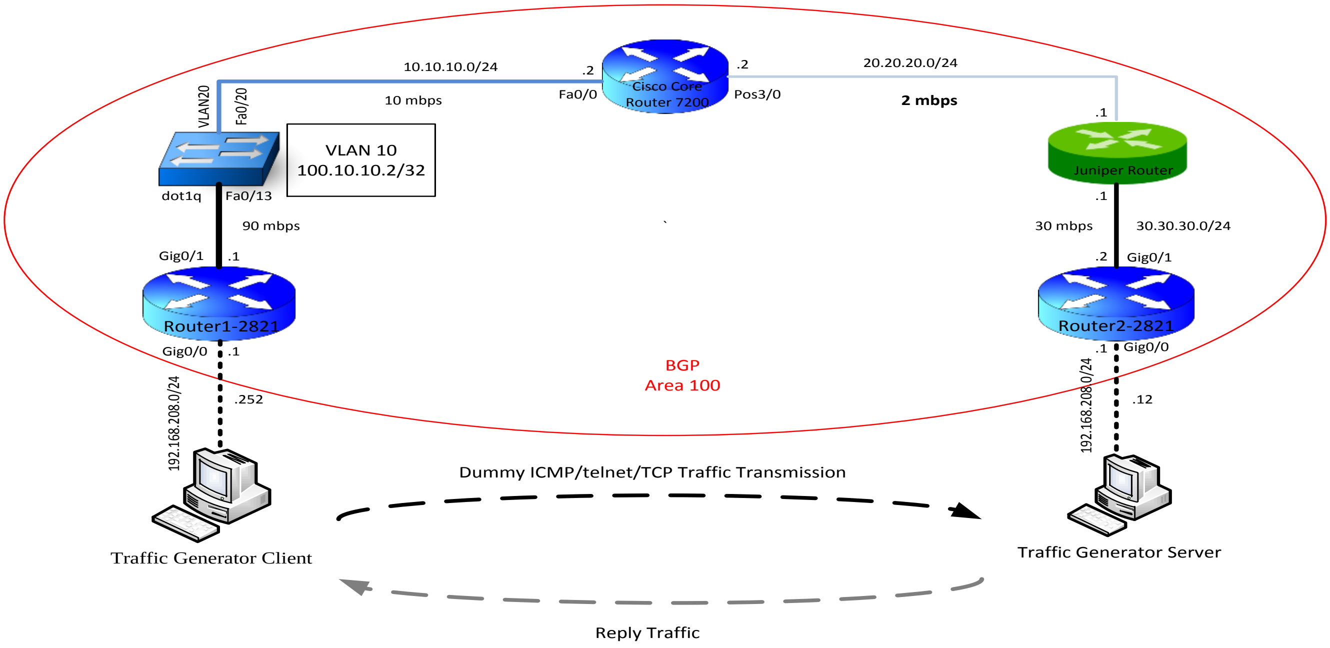

Figure 4. Sample network topology for proposed scenario

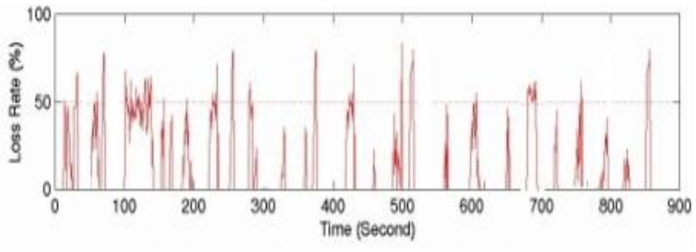

Figure 5. Packet lost before applying DMT

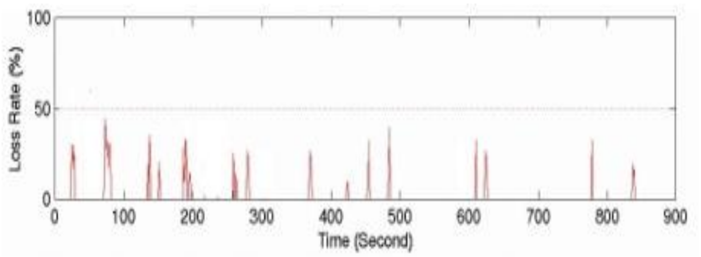

Figure 6. Packet lost after applying DMT

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-199-1