Evaluation Study for Analysis of Quality of Service in the Internet

SABIHA F.JAWAD
NADA TH.AHMED

AL-Mustanseryah University
computer science dept.

ABSTRACT

In this paper, IP header packet system is used to be capable of supporting performance assurance service in the Internet to apply the properties of QoS and enhancement Internet service, and to find some parameters of QoS and adaptive QoS routing .Since the IP header packet can find the packet which belongs to one of reserved resource reservation Setup Protocol. Then we find the properties of QoS (maximum and minimum delay, jitter delay, source and destination address of each flow, capture time for each packet, and QoS that are made to find performance assurance service work in the internet.

Key Words: Quality of service,IP, Computer Network monitoring, performance assurance, Differentiation Services

الخلاصة

في السنوات الأخيرة ارتبطت الحضارة العالمية بشكل كبير وواسع في عالم تكنولوجيا المعلومات والاتصالات، واليوم أصبحت الشبكة العالمية الإنترنيت الأوسع للمعلومات.

وبسبب زيادة عدد المستخدمين ، مما أدى إلى وجوب تطوير وتحسين نوعية الخدمات المقدمة في هذه الشبكة، لذلك كان مفهوم Quality of Service (QoS) من خلال بناء هيكلية جديدة (تأكيد الخدمات Integrate Service (IntServ) و تمييز الخدمات Differentiate Service (DiffServ) والبروتوكولات)، وذلك لجعل الإنترنيت الحالي قادراً على حمل أحجام كبيرة من الـ Traffic، وان تزداد عدد الـ IP مختلفة كمصادر للمرور لمتطلبات العمل . أي يصبح أداء الإنترنيت بأقل وقت ممكن وبأفضل خدمة ودون ضياع الحزم (Packets) .

إن هدف البحث هو الوصول إلى ضمان أداء الخدمات في شبكة الإنترنيت ، من خلال توظيف خصائص الـ QoS في الإنترنيت ، ومن خلال بناء نظام الـ IP header packet لتحليل المعلومات الداخلة لإيجاد خصائص المتغيرات لـ QoS ،التأخير والوقت المستغرق لكل حزمة . من خلال ذلك يمكننا معرفة تلك الخصائص وضمان الأداء مع تلك المحددات من المصدر إلى الهدف .

1-Introduction

The Internet has grown very fast and only- provides best-afforded service that represents the simplest type of service, where traffic source is processed as quickly as possible and customers want many of new applications and different requirements that make it.

Enhancement of Internet is to find technologies. Standards and to find architectures which make for resource allocation in the Internet and enough for each application .This architecture is integrated services (IntServ), Differentiated services (DiffServ), all multiprotocol, and label switching ,all this are under the term of Quality of Service (QoS), they provide enhancement and performance assurances services to the Internet .

Although the Internet now runs faster and is increasing in size, its basic architecture remains unchanged from its early days. The Internet still operates as datagram network, where each packet is delivered individually through the network [1]. Growing usage and diversity of applications on the Internet make quality of service (QoS) an increasingly critical issue, especially in the E-commerce realm.

Quality of service has been one of the principal topics of research and development in packet networks for many years [2].

As long as the sum of the bandwidth of the increases links exceeds the minimum capacity of a network, QoS can be offered only in one of two ways: either by predicting the traffic and engineering the network to make violations of the committed QoS sufficiently unlikely or by restricting the total amount of traffic competing for the same resources. In many cases, the network capacity is effectively partitioned by packet prioritization, so that higher-priority traffic is largely unaffected by lower-priority traffic.

QoS can be defined in various ways, most of which are equivalent or complimentary. It is the ability of network element (e.g. an application, host or router) to have some degree of assurance that its traffic and service requirements can be satisfied [3]. It describes the assurance of sufficiently low delay and packet loss for certain types of applications or traffic [4]. The provision of QoS in a network, especially one as large as the global internet, is not a trivial matter. The cooperation of all network layers from top-to-bottom (i.e. layer one to layer seven of the ISO-OSI model) in addition to every network element from end-to-end (i.e. from sender to receiver) is required.

QoS generally describes the assurance of sufficiently low delay and packet loss for certain types of applications or traffic. QoS can be described qualitatively (relative) or quantitatively (absolute). Relative QoS definitions relate the treatment received by a class of packets to some other class of packets, while absolute definitions provide metrics such as delay or loss, either as bounds or as statistical indications.

QoS guarantees can be made either over an aggregate of communication associations or for an individual group of packet delineated in time, this is often called a "flow", QoS is assured by reserving resources, primarily bandwidth and sometimes buffer space [5].

In this paper, IP header packet system is used to be capable of supporting performance assurance service in the Internet to apply the properties of QoS and enhancement Internet service, and to find some parameters of QoS and adaptive QoS routing.

2- Components of (QoS)

QoS has two components:

a- Performance assurance.

Service requirements are application-specific. For example, an audio program would be sensitive to round-trip delay; a bulk file transfer application is more sensitive to the average transmission rate or the total amount of time for transferring the data. The following common parameters have been widely used to describe QoS requirements [1]:

1- Minimum bandwidth: The minimum amount of bandwidth required by an application flow. The time interval for measuring bandwidth should also be specified since different measurement intervals may yield different results.

2- Delay: The delay requirement can be specified as the average delay or worst-case delay. The delay a packet experiences has three components: -

i- Propagation delay: is caused by the speed of light, and so is a function of distance.

ii- Transmission delay : is the time to send a packet .

iii- queuing delay: can be related to bandwidth requirement .

3- Delay jitter: a delay jitter requirement specifies the maximum difference between the largest and smallest delays that packets experience. In any case, the delay jitter should not be larger than the worst-case transmission and queuing delay.

4- Loss rate: is the ratio of lost packets and total packets transmitted. Packet losses in the internet are often caused by congestion, and such losses can be prevented by allocating sufficient bandwidth and buffers for traffic flows.

b- Differentiation Services(Diffserv)

Differentiated services main goals are for service differentiation in IP networks that are both scalable and manageable. Tthese goals can be achieved by providing local service differentiation for large aggregates of traffic.

Diffserv operates by packet tagging which involves setting bits in the header of a packet. The Ipv4 Type-of-Service (ToS) octet currently goes unused and so Diffserv redefines it as the DS byte [6]. Only the first 6 bits are used and are referred to as the DSCP (Differentiated Service Code Point) field. The DSCP specifies a Per-Hop Behavior (PHB) used to forward the packet at each router (i.e. of PHBs include priority dropping and priority scheduling). The DSCP for a packet is set by the end-host or the first-hop router according to the service quality the packet is required and entitled to receive.

3- QoS Architectures

The growing need to support more enhanced services in the internet than the traditional best effort service can provide, has already been established. Architectures for providing service differentiation in the internet have sparked extensive research in the last few years. There are two fundamentally different approaches for QoS architectures [7]:

1- Iintegrate service (IntServ) approach.
2-Differentiated Service (DiffServ) approach.

Comparison between IntServ and DiffServ

IntServ and DiffServ have been designed with different goals ,Table (1) summarizes the traits of each. At the boundary of the network the IntServ requests are mapped onto the underlying capabilities of the DiffServ network, aspects of the mapping include:-

1-selecting an appropriate PHB or a set of PHBs for the requested services .
2-performing appropriate policing at the edge of the DiffServ network exporting IntServ parameters from the DiffServ network.

4- IP Packet Header QoS

In packet processing a router must examine every incoming packet and then decide if the packet belongs to one of the reserved (RSVP) flows, the header fields are :

1- ***version***: There are two versions for QOS version (4) and version (6). In our developed system we assumed to use version (4).
2-***header length***:32-bit word forming the header there are two types of header length 5 and 6.
3- ***total length*** : 16 bits total length size of datagram (header+ data) RSVP protocol used total length measuring massage size in bytes. This includes the variable length objects (the flow).

4- ***ID*** : The parameter "id " consists of two numerical fields one identifying the service associated with the parameter the (service – number) and the other identifying the parameter itself the < parameter- number> the textual form service-number , parameter-number:-

a- service number(1) is reserved to indicate the default value, a parameter value is identified by the id < 1, parameter-umber>
b- service numbers 2 through 254 are allocated to individual services for example guarantee service is allocated number(2) controlled load service number 5 .
c- parameter number in the range (1 through 127) are reserved for general parameters that apply to all services.
d- parameter numbers in the range (128 through 254) should be used for parameters specification to a particular service .

5- ***time to leave*** : it is used by the sender in the IP header number of network hops .
6- ***protocol*** : service access point which indicates the type of transport packet being carried.
7- ***Checksum*** : RSVP checksum is similar to the ones used in TCP-UPP and IP to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check.
8- ***Source IP address*** : the IP address of the original sender of the packet.
9- ***Destination IP address*** : IP routers currently use a small number of fields in a packet header to market forwarding decisions. All packets that have the same destination network number follow the same path and receive the same treatment (the IP address of the final destination of the packet) .
10- ***Capture time*** : packet-by-packet finishes time for every packet weighted fair **queuing.**
11- ***counter of packet*** : to find the number of packet with selector.
12- ***Packet per sec*** : total per second for the number of packet .
13- ***Maximum buffer*** : to fine the maximum buffer to use the first hop router may have to allocate a buffer for the source larger than the burst size.
14- ***Minimum buffer*** : the packet will be sent from the packet buffer.
15-***Differentiated services*** : DiffServ uses 6 bits in the IP packet header, the Internet standards that define the DiffServ :
0= normal delay
1= low delay
0= normal throughput
1= high throughput
0= normal reliability
1= high reliability

Table (2) shows, the number of minimum and maximum values, and mean for total length, ID, Time to leave, checksum and capture time. This table shows the comparison between three types of protocols (UDP, IGM, and TCP) which are entered in analysis of IP packet header. This comparison is used to test the difference between means of every protocol (Total length, ID, Time to leave, check sum and capture time).

4- Flow Identification

An IP flow is identified by the five fields in the packet header, source IP address, destination IP address, protocol ID, source port, and destination port. To determine if a packet matches an RSVP flow, the flow identification engine must compare the five-tuple of the incoming packet with the five- tuple of all flows in the reservation table. If there is a match, the corresponding reservation state is retrieved from the reservation table and the packet is dispatched to the packet scheduler with the reservation state associated.

A flow can be characterized in many ways; The exact form may depend on what admission control and packet scheduling mechanisms are used. The following parameters are common [8]:-

1- ***Peak rate*** : (the highest rate at which a source can generate traffic), the peak rate is limited by the speed of the hardware devices, for example, we cannot generate packets faster than 10 M bits/ sec over 10 M bits /sec Ethernet. The peak rate can be calculated from the packet size and the spacing between consecutive packets.

2- ***Average rate***: (the average transmission rate over a time interval). The average rate is calculated with a moving time window so that the averaging time interval can start from any point in time.

3- ***Burst size***: (the maximum amount of data that can be injected into the network at the peak rate). It reflects the burstness of the traffic source.

In developed system we assume to use 30 flows.

5- Application

The calculation of finish time can be more clearly explained with arrival-departure curves. Suppose that we have two flows sharing a server equally, so that flow 1 and 2 are both served at a rate of 1/2. figures(1)and (2) are the arrival-departure curves. The dashed line is the arrival process (the amount of data arrived versus time) and each arrow represent the arrival of a packet. The height

of the arrow is the size of the packet. For example in figure (1) packet arrive at t= 1, 2, 3 and 11 with packet size 1, 1, 2, 2, respectively after the arrival of each packet the arrival curve (dashed line) increase by the packet size. The soled line represent the amount if data that have served. During the time interval (0,1) flow 1 is idle and flow 2 sends a packet at time = 0. Therefore the first packet from flow 2 is served at a rate of 1 during interval. At t=1 the first packet from flow 1 arrives, and both flow are backlogged and are served at the rate of
1/2 until t=9. At this time three packet form flow 1 have left the system, and no more packet arrive. During the interval (9,11) flow 2 again is serve at the rate of 1. At t=11, a packet from flow 1 arrives, and by this time all packet from flow 2 are finished. The fourth packet from flow 1 is then served at the full rate of 1 and finished at t=13. Let us look at flow 1 figure (1) the third packet from flow 1 arrives at t=3, and the total amount of arrived data is 4 (dashed line). The soled line indicates that the amount of data that has been served reaches 4 at t=9. Thus the third packet from flow 1 arrives at t=3 and departs at t=9; the total delay it experiences is 6. In fact, the distance between the dashed line and soled line along the (x- axis) is the delay bound for the flow.

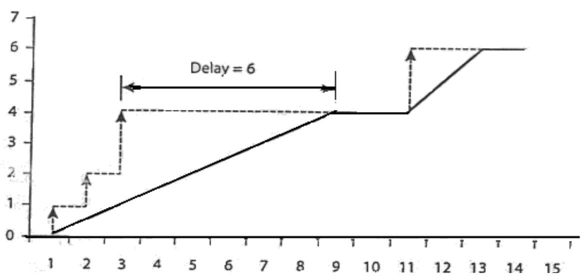

Figure (1) Arrival – departure curve for flow one

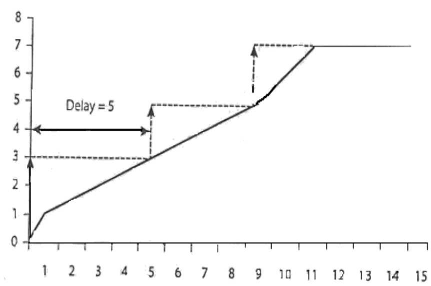

Figure (2) Arrival – departure curve for flow two

6- Conclusion

Growing usage and diversity of applications on the internet make quality of service (QoS) an increasingly critical issue. QoS parameters may also be used for optimizing internal resources.

1. The architecture of the reposed system (IP packet header) has evaluation serves for each application about delay jitter and toss packet, and performance assurances serves in the Internet.

2. Implements (IP packet header) in the Internet which each used have some requirement that make know the type of service and the model is used for each application.

3. The proposed (IP packet header) in the Internet is most important to know where is some problem in the service like that the load traffic, access between the link , the repute for each flaw .Time to live that mean (loss packet)

4. In system (IP header packet can find the most important think the error between each part of (IP packet header) (like protocol TCP .UDP. And can be find limited error and, improvement that's error.

5. In system (IP header packet can fined some parameter for QOS like delay jitter throughput IP source IP destines. to meek know the which part of them is more effected for each serves .

Table (3) shows delay quantity between each flow reality for each application to find the maximum and minimum delay for 50 users. Mean delay realized delay sensitive application on the timely arrival of its packets.

Table (4) shows the difference between maximum delay and minimum delay, and shows jitter time and jitter quantity for each flow.

References

[1] Wang Z., "Internet QoS architectures and mechanisms for quality of service", http://www.objs.com /survey/qoshtm ,2001.
[2] Niklaos Vasition , " Overview of internet QoS and web server QoS " , Department of computer science western on tario university, London, 2000 .
[3] Charly S. , " The need for QoS ", white paper, http://www.qosfoum.com , July, 1999.
[4] Zhao W. and Schulzrinne H.," Internet quality of service ", IEEE,Network, September / October , 1999 .

[5] Weibin Zhao and David Olshefski , " Internet quality of service " , Colmbia University, 2001 .
[6] Nichols K. and Black D. , " Difinition of the Differentiated service field in the IPV4 and IPV6 headers " , RFC 2474, IETF, December , 1998 .

[7] Nichols K. and Zhang L. , " A two-bit Differentiated services architecture for the internet" , RFC 2638,IETF , July 1999 .
[8] Agedal J.Q. ," Quality of service support in develop ment of distributed systems ", PHD thesis Department of Information , University of Oslo, 2001 .

Appendix

Table(1) Comparison between IntServ and DiffServ

Element	IntServ	DiffServ
Granularity of service differentiation	Individual flow	Aggregates of flows
State maintenance in routers (e.g. buffers, scheduling)	Per-flow	Per-aggregate
Packet classification	Several header field (the 5 tuple)	DS byte of IP header
Type of service differentiation	Deterministic or statistical guarantees	Absolute or relative assurances
Admission control	Required	Required only for absolute differentiation
Signaling protocol	Required (RSVP)	Not required for relative schemes absolute schemes need semi-state reservations or broker agents
Coordination	End-to-End	Local(per-hop)
Scalability	Limited by number of flows	Limited by number of classes of service
Network accounting	Based on flow characteristics and QoS requirement	Based on class usage
Net work management	Similar to circuit-switched net-works	Similar to existing IP networks
Interdomain deployment	Multilateral agreements	Bilateral agreements
Type of protocol	IP protocol only	Ip protocol only
Resource allocation to aggregated traffic rather than individual flows	Allocates resources to individual flows, which can run into tens of thousands in a large network.	Resource are allocated to individual classes that represent aggregate traffic.
Traffic policing on the edge and class-based forwarding in the core	Requires all nodes to perform packet classification to identify packets from reserved flows and schedule them with per-flow queuing	Only boundary nodes at the edge of the network classify traffic and mark packets
Define forwarding behaviors not services	Takes the opposite approach	Define forwarded treatments, not end-to-end services.
Guarantee by provisioning rather than reservation	Per-flow reservation lower than in IntServ	Provides ressource assurance through provisioning combined with prioritization
Emphasis on service level agreements rather than reservation Ensure that the SLAs between customers and service providers are honored	Application setup resource reservation on domaned using the RSVP protocol	Ensure that the SLAs between customers and service providers are honored
Focus on a single domain vs.end-to-end	Inherently end-to-end	The deployment of DfServ can be incremental

Table (2) Protocol Descriptive

IP packet	protocol	N	MEAN	MINIMUM	MAXIMUM
TOTAL. LENGTH	**IGM**	34	10179.765	8192	10240
	TCP	942	20521.803	770.0	63490
	UDP	19351	20780.042	3842	60160
	total	20327	20750.344	770.0	63490
ID	**IGM**	34	4776.1765	.00	19744
	TCP	942	29284.475	.00	65352
	UDP	19351	32260.960	.00	65518
	total	20327	32077.051	.00	65518
TIME TO LEAVE	**IGM**	34	1.0000	1.0	1.0
	TCP	942	99.8811	39	242
	UDP	19351	139.2530	1.0	143
	total	20327	137.1972	1.0	242
CHECK SUM	**IGM**	34	51837.500	192.0	64896
	TCP	942	34515.882	29.00	65356
	UDP	19351	32615.979	1.00	65533
	Total	20327	32736.176	1.00	65533
CAPTURE TIME	**IGM**	34	30.08576	1.261	54.759
	TCP	942	23.10156	.003	59.85
	UDP	19351	29.91974	.003	59.999
	Total	20327	29.60405	.003	59.999

Table (3) Delay quantity between requests for each flow number

Number of flow	Number of packet for each flow	Maximum delay	Minimum delay	Mean delay
1.00	105	9	7	7.182692
2.00	254	19	2	2.869565
5.00	32	2211	2	453.4
6.00	326	2329	6	824.0909
7.00	86	22	2	6.625
8.00	16	18	7	12.5
9.00	4	181	2	67.33333
10.00	27	227	2	41.2
11.00	56	35	2	10.16667
12.00	21	630	2	51.53846
13.00	30	65	2	9.461538
15.00	57	212	2	15.26087
16.00	35	5	2	2.6
17.00	7	39	3	18.8
18.00	5	12	3	8.666667
19.00	6	13	2	5.4
20.00	88	18	2	5.428571
21.00	53	384	2	19.41667
22.00	15	6	2	4.428571

23.00	15	16	2	7.375
24.00	29	380	2	39.28571
25.00	13	16	2	6.7
26.00	14	13	2	7.272727
27.00	7	37	3	11.33333
28.00	18	3	2	2.25
29.00	3077	36	2	5.953937
30.00	2798	36	4	6.190561

Table(4) Jitter quantity between requests for each flow number

Number of flow	**Number of packet for each flow**	**Jitter time**	**Jitter quantity**
1.00	105	61.743	2
2.00	254	61.693	17
5.00	32	10.065	2209
6.00	326	14.012	2323
7.00	86	49.505	20
8.00	16	1.653	11
9.00	4	48.383	179
10.00	27	84.785	225
11.00	56	58.609	33
12.00	21	37.629	628
13.00	30	74.887	63
15.00	57	70.946	210
16.00	35	4.868	3
17.00	7	40.984	36
18.00	5	11.507	9
19.00	6	62.272	11
20.00	88	71.717	16
21.00	53	85.647	382
22.00	15	4.676	4
23.00	15	68.231	14
24.00	29	79.636	378
25.00	13	69.744	14
26.00	14	61.422	11
27.00	7	36.967	34
28.00	18	63.595	1
29.00	3077	63.515	34
30.00	2798	63.415	32