

TRAFFIC DELAY CONTROL OF WRED QUEUES WITHIN COMMUNICATION NETWORK NODES

Codruț Mitroi¹

Abstract

End-to-end traffic delay control within actual communication networks represents a very important goal for an administrator, due to the direct influence on service quality of service level, which is delivered to users. The difficulty of a maximal end-to-end delay prediction is related especially to the random traffic behaviour within waiting queues belonging to network nodes.

The aim of this paper is to present a delay control proposal for the data traffic within a queue wherein is activated a weighted random early detection (WRED) congestion avoidance mechanism.

Keywords: packet delay, delay control, WRED mechanism, congestion avoidance

Introduction

Quality of service (QoS) is a main concept in present communication networks, being characterized by certain typical QoS parameters: delay, delay variation (called also sometimes jitter), information (packet) loss percent and bandwidth [1], [2].

QoS assurance aim is to offer an end-to-end approach, no matter if users belong to the same LAN or they receive services from one or more service providers. For that purpose, the mechanisms, which are specific to the QoS operational plan, especially those designated to congestion management must assure maximal values for previous presented parameters, according to the specific service requirements.

The delay represents the time period, which is necessary for an information packet to travel from the source to the receiver. Characteristic delay is additive, his total value representing a sum of all delays introduced by various network elements along the transmission path between source and destination. The main problem which appears in networks services delivery is related to the possibility of end-to-end delay value prediction between service's source and destination (user).

The work is organized as follows: section 2 presents an estimation method for network end-to-end delay, in section 3 it is described a delay control procedure for waiting queues, which has activated a weighted random early detection (WRED) mechanism. Section 4 validates the proposed procedure within a testing environment. Finally, section 5 emphasize the main conclusion.

¹ PhD Candidate, Control and Computers Faculty, University POLITEHNICA of Bucharest, engineer, Advanced Technologies Institute, e-mail: cmitroius@yahoo.com

2. Network End-To-End Delay Estimation

The main delay components, which are characterized by the place where they appear within the network or by the influence that they have on the total delay value, are illustrated in figure 1 and presented as follows [3]:

- i. Processing delay (D_p) is represented by the speed wherewith network node process specific informations, which are included within data packet, like packet destination, packet's particular treatment mode according to certain flags (TOS, DSCP, EXP) or the reaction mode regarding possible transmission errors signalling. Delay value depends greatly on architectural model complexity, which characterise the traffic and also processing speed of node's command modules (processor, memory), the last one being affected by traffic level. Processing delay is not the same for packets, which belong to different traffic profiles, and represents a combination between a deterministic (D_{pd}) and a stochastic (D_{ps}) magnitude.
- ii. Propagation delay (D_c) is related on the links between network nodes, being represented by the speed wherewith bits are transmitted on this links. Practically, his value is given by transmission medium propagation speed (optical fiber, metallic cables, radio or satellite links). Generally speaking the value introduced by this kind of delay is constant, exception are the transatlantic or satellite connections with higher delay values, due to the distance.
- iii. Transmission or serialized delay (D_t) represents the time period, which is involved in packet transmission on the network node's output interface. His value is generally speaking constant, being inversely proportional with output interface bandwidth.
- iv. Queuing delay (D_q) represents the time needed to output a packet from waiting queues. His value is determined by implementation mode of congestion avoidance mechanisms and also by output interface bandwidth within network node, having a major stochastic nature due the interaction of all packets, which enter in the queue.

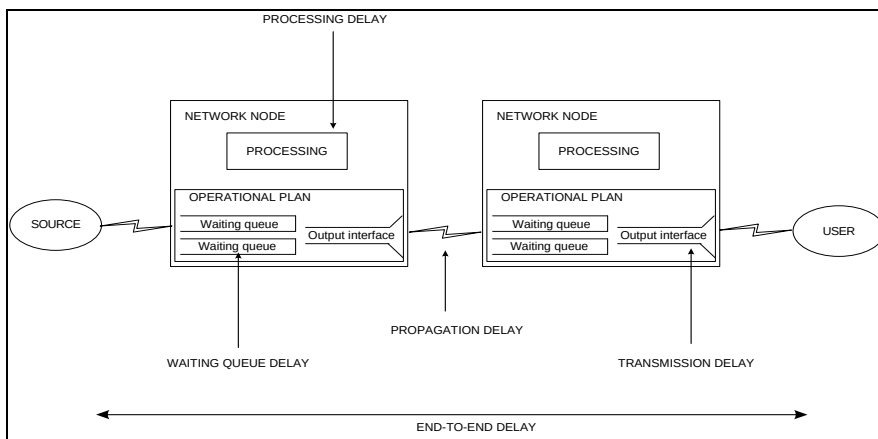


Figure 1: End-to-end delay components

Thus, end-to-end delay could be expressed as a sum of all previous presented components, being characterized by a deterministic and a stochastic component, according to equations (3.1.) and (3.2.):

$$D_{ete} = \underbrace{(D_{c_{ete}} + D_{pd_{ete}} + D_{t_{ete}})}_{\text{deterministic end-to-end delay}} + \underbrace{(D_{ps_{ete}} + D_{q_{ete}})}_{\text{stochastic end-to-end delay}} \quad (3.2.)$$

In the case of deterministic delay it could be estimated the maximum associated value, taking into consideration that at the beginning network design phase, the administrator has the information about the network topology (number of involved network nodes, transmission medium type, bandwidth requirements for the services delivered to the users). Practically, deterministic delay measured between service source and user it will be equal with the sum between deterministic delay values, which are introduced by each network node and the sum of delays, associated to the links between nodes, according to equation (3.3.):

$$D_{ete-det} = \sum_{i=1}^n (D_{ruter_i} + D_{c_i}) \quad (3.3.)$$

In case of a p bits packet, equation (3.3.) will be reformulated as equation (3.4.) [4]:

$$D_{ete-det}(p) = \sum_{i=1}^n \left(\frac{p}{C_i} + D_{c_i} \right) = p \sum_{i=1}^n \frac{1}{C_i} + \sum_{i=1}^n D_{c_i} \quad (3.4.)$$

where C_i represents the output interface bandwidth of network node i .

There many approaches regarding the queue delay estimation, one of this models consider the stochastic delay as a sum of delays due to each network node [5], according equation (3.5.):

$$D_{ete-stoh} = \sum_{i=1}^n (D_{q_i} + D_{ps_i}) \quad (3.5.)$$

Taking into consideration that stochastic delay produced by waiting queues D_q is caused by variable traffic values, which is present within network nodes, the proposed model is based on two distributed functions F and G , which correspond to the periods with or without traffic. When there is traffic, the measuring packet (probe) will be maintained in the queue until it could be outputed. In the other case, the probe will get through the queue without delay. The resulted value it will be completed by stochastic value resulted from packet processing.

It will be considered the two sequences $X1, X2, \dots$, representing the periods without traffic, respectively $Y1, Y2, \dots$, when the acces is blocked, as being independently (figure 2).

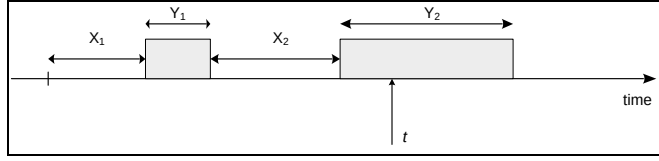


Figure 2: Alternance mode of queue opening/closing [5]

In this condition, the stochastic delay value $D_q(t)$ could be expressed according equation (3.6.):

$$D_q(t) = 0, \text{ if } \sum_{i=1}^{N(t)} (X_i + Y_i) < t < \sum_{i=1}^{N(t)} (X_i + Y_i) + X_{N(t)+1} \quad (3.6.)$$

$$D_q(t) = \sum_{i=1}^{N(t)+1} (X_i + Y_i) - t, \text{ if } \sum_{i=1}^{N(t)} (X_i + Y_i) + X_{N(t)+1} < t < \sum_{i=1}^{N(t)+1} (X_i + Y_i)$$

Equation (3.6.) points a direct proportionality between the two time periods μF and μG and the probability that stochastic delay introduced by waiting queue is zero, which conducts to a significant dependability of stochastic delay towards traffic behavior within queues.

Processing delay value estimation is subject of many articles and studies, one of them presents a processing cost approach [6]. This regards the number of used instructions, respectively the number of memory accesses needed for single packet processing.

Finally, the processing delay per network node could be expressed according to equation (3.7.) as a sum of the two subsequent delays:

$$t_a(l) = t_{p_a}(l) + t_{m_a}(l) = \frac{\alpha_a + \beta_a \times l}{f} + (\gamma_a + \delta_a \times l \times t_{mem}) \quad (3.7.)$$

There are also some limitation of the above presented model, the case of data flows is one of them, because the packets processing is inequal distributed (for example, in the case of HTTP services, the major part of processing is done in the initial URL transmitting moment). At the same time, this model cannot be applied in case of supplementary processing resources, like e.g. coprocessors or hardware accelerators.

3. Delay Control Within Waiting Queues Dedicated To Data Traffic

Data traffic is processed into weighted random early detection (WRED) waiting queues, which represents an improvement of RED algorithm through a packet drop differentiation according to some specific parameters, like e.g. DSCP field. RED algorithm, described for the first time in 1993 by Sally Floyd and Van Jakobson [7], is based on the following sequence:

Initialization

```

 $q_{med} = 0$ 
count = 1
end
for each packet arrival
  calculate the new average queue size " $q_{med}$ "
  if the queue is nonempty
     $q_{med}(t) = (1-w_q) \cdot q_{med}(t-1) + w_q \cdot q_i(t)$ 
  else
     $m = f(time - q\_time)$ 
     $q_{med}(t) = (1-w_q)^m \cdot q_{med}(t-1)$ 
  end
  if  $th_{min} \leq q_{med} \leq th_{max}$ 
    increment count
    calculate probability " $p_a$ "
     $p_b = max_p \cdot (q_{med} - th_{min}) / (th_{max} - th_{min})$ 
     $p_a = p_b / (1 - count \cdot p_b)$ 
    end
    with probability " $p_a$ "
      mark the arriving packet
      count = 0
    end
  end
  else if  $th_{max} \leq q_{med}$ 
    mark the arriving packet
    count = 0
  end
  else
    count = -1
  end
end
end
when queue becomes empty
   $q\_time = time$ 
end

```

variables:

$q_{med}(t)$ mean queue length

q_time starting time of queue packet accumulation

count number of packets accumulated after the last marked packet

Fixed parameters:

w_q queue weighted factor

th_{min} minimum packet dropping threshold value

th_{max} maximum packet dropping threshold value

max_p maximum value of probability p_b

Other parameters:

q_i queue instantaneous length value

p_a packet marking probability

time current time

$f(t)$ a linear time function

The analysis of previous sequence leads to the conclusion that they are two instances through which queue „flexibility“ could be controlled, this shows the capacity to absorb

some traffic bursts. First of all, illustrated by equation (3.8.) refers to the computing of mean queue length q_{med} according to the instantaneous queue length q_i :

$$q_{med}(t) = (1 - w_q) \cdot q_{med}(t-1) + w_q \cdot q_i(t) = (1 - \frac{1}{2^n}) \cdot q_{med}(t-1) + \frac{1}{2^n} \cdot q_i(t) \quad (3.8.)$$

where parameter n represent an exponential weighted factor dependent of packets length and interface speed. As we can see, n value growing will conduct to an accentuated approach of mean queue length to the instantaneous queue length, that will act bursts absorbtion, whereas n value decrease will act queue limitation towards mean value. This behavior is illustrated in figure 3 [8], where the instantaneous queue length present a strong packet bursts characteristic within 3-4 sec. time interval, instead mean queue length dynamic is reduced in the first monitorized period and negligible in the second.

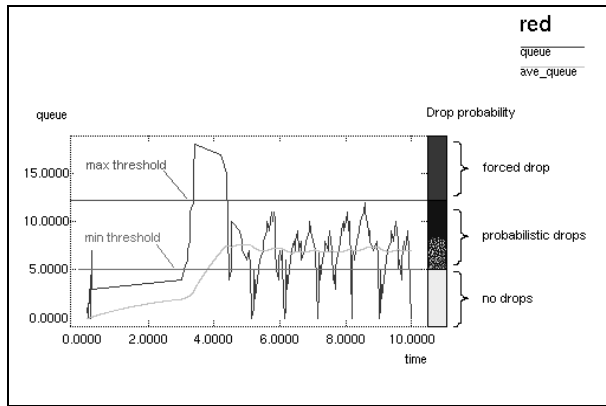


Figure 3: Queue behavior in the presence of RED [8]

The second instance refers to the computing of packet marking probability p_a in order to drop the packet, according equation (3.9.), whereby results an explicit dependability towards mean queue length:

$$p_a = \frac{\max_p \cdot \frac{q_{med} - th_{min}}{th_{max} - th_{min}}}{1 - count \cdot \frac{q_{med} - th_{min}}{th_{max} - th_{min}}} \quad (3.9.)$$

Concluding the previous presented aspects, it could be perform a strong control of WRED queues behavior, and thus a control of network nodes traffic delay through the following three parameters setting:

- weighted factor value n – through this parameter it could be set the mean queue length behavior, thus implicit traffic bursts capacity, directly proportional with packet delay within queue;
- packet drop maximum threshold value th_{max} – it serves to the setting of the maximum packet delay within queue;
- maximum packet marking probability max_p – through this parameter it could be set the packet drop aggressivity and thus the delay value within queue.

Based on mentioned facts, below is proposed a control procedure for data traffic within WRED queues, in order to obtain a maximum benefit regarding the ratio between maximum assumed delay and dropped packets percent, procedure consisting of three steps optimisation algorithm:

- identifying the optimum value of weighted factor, which assures enough flexibility for traffic bursts absorbtion;
- limiting the maximum queue length through an identification of optimum packet drop maximum threshold value, in order to assure the assumed delay;
- and finally identifying the optimum value of packet marking probability, in order to assure the assumed delay for the situations characterized by an excessive traffic volume.

4. Simulation Of The Proposed Delay Control Procedure Within Wred Queues

In order to simulate the proposed delay control algorithm within queues allocated to data traffic, it has been used the testing diagram illustrated in figure 4 [8].

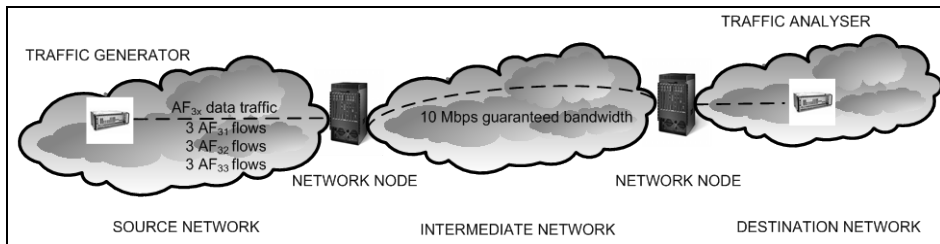


Figure 4: Testing diagram of the proposed delay control algorithm

As it can be seen, there are three networks: a source network, an intermediate network, which serve as a transport network and a destination network. The three networks are connected through two network nodes represented by Cisco 7609 routers and within the intermediate network it was set a 10 Mbps guaranteed bandwidth connexion, which links source and destination networks. The generated traffic in the source network and the measured traffic in the destination network has been simulated with an equipment IXIA model XM, which could operate with multiple traffic patens like TCP, UDP and Internet mix, in order to answer accurately to various simulation requirements. Simulation tests supposed a weighted class-based configuration for the queue scheduling mechanism (CBWFQ) [9], this means each traffic profile has his own bandwidth on network node's output interfaces, according to the following percentage: voice traffic (DSCP EF value) – 1 Mbps, video traffic (DSCP AF₄₁ value) – 1 Mbps, critical data traffic (DSCP AF_{3x} value) – 7,2 Mbps, the rest of bandwidth capacity being reserved for other traffic classes.

Testing sessions purpose is to emphasize the delay control algorithm function mode in case of critical data, which are characterized by AF_{3x} DSCP value. In order to do this, the allocated bandwidth for this class was congested with a supplementary traffic of 1,8 Mbps, allocated on a number of 9 flows (3 for each subclass AF₃₁, AF₃₂, AF₃₃), each of them with

1 Mbps. All flows are characterized by a strongly variable profile, because they contain a great amount of variable bursts. At the receiver module within IXIA equipment was collected the measures of maximum and mean delay values, respectively, packet drop percent value.

Weighted Factor Influence On Maximum Delay Value

First step corresponds to the identification of optimum weighted factor value. The influence of this parameter on delay was established through successive settings of his value for the three AF₃₁ subclass flows. Certain values were configured in the network nodes according to equipment limitation $n=1, 5, 9, 12$ și 16 .

At receiver's end it was measured the maximum and mean delay values for the 9 AF_{3x} flows and also the packet drop percent. Figures 5 and 6 illustrate maximum and mean delay values for the best results obtained ($n=1$ and 5).

In order to decide about the optimum n parameter value, it is useful to emphasize the packet drop percent, which could be extract from the network node's interface (figure 7) and also from IXIA equipment (figure 8).

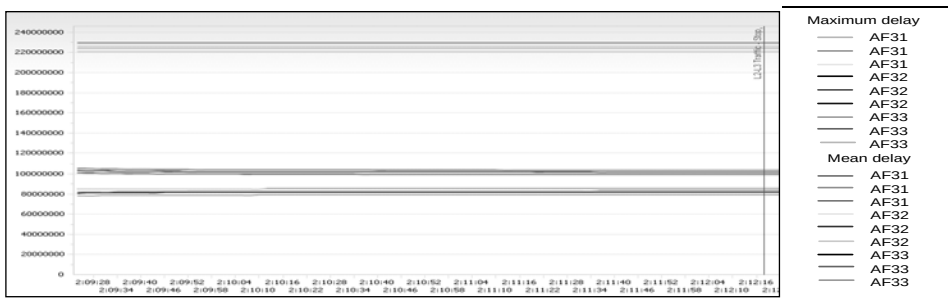


Figure 5: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=1$

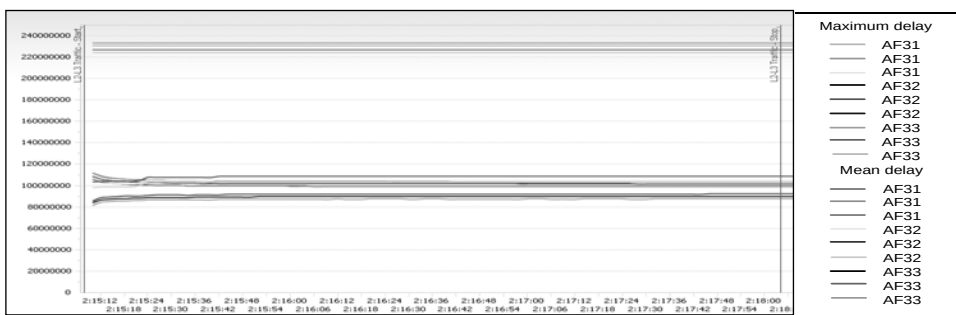


Figure 6: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=5$

dscp	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Mean queue	Maximum thresh	Mark probe
af31	52389/41701644	9741/7753836	0/0	32	32	40	1/10
af32	52400/41710400	6109/4862764	3621/2882316	28	39	40	1/10
af33	52403/41712788	6216/4947936	3511/2794756	24	39	40	1/10

af31	55365/44070540	10288/8189248	5/3980	32	36	40	1/10
af32	55372/44076112	6525/5193900	3761/2993756	28	39	40	1/10
af33	55365/44070540	6663/5303748	3630/2889480	24	39	40	1/10
af31	49502/39403592	5396/4295216	3800/3024800	32	39	40	1/10
af32	49505/39405980	5683/4523668	3510/2793960	28	39	40	1/10
af33	49505/39405980	5872/4674112	3321/2643516	24	39	40	1/10
af31	52365/41682540	4923/3918708	4803/3823188	32	39	40	1/10
af32	52366/41683336	6056/4820576	3669/2920524	28	39	40	1/10
af33	52368/41684928	5955/4740180	3768/2999328	24	39	40	1/10
af31	55962/44545752	14/11144	10384/8265664	32	42	40	1/10
af32	55965/44548140	6566/5226536	3829/3047884	28	39	40	1/10
af33	5961/44544956	6721/5349916	3678/2927688	24	39	40	1/10

Figure 7: Influence of weighted factor variation on packet drop extracted from the node's interface

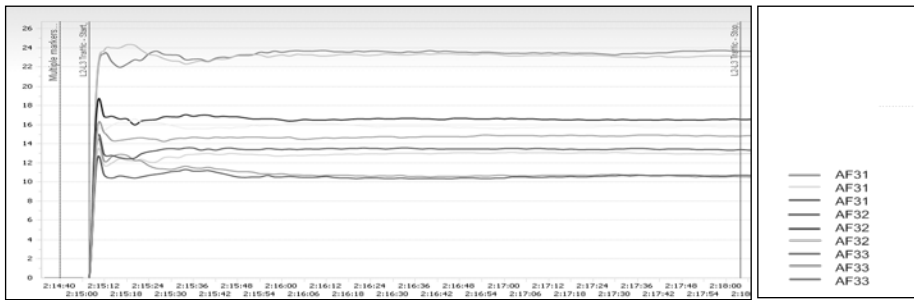


Figure 8: Critical data flows (AF_{3x}) packet loss (%) for $n=5$

Combining the results obtained in the two series of measurements, it could be concluded that the value $n = 5$ is optimum in order to assure a minimum delay together with a minimum packet loss.

Packet Drop Maximum Threshold Influence On Maximum Delay Value

Second test stage corresponds to packet drop maximum threshold setting, taking into consideration the optimum value for the weighted factor, identified in the first stage. For a common reference, value $n = 5$ was configured for all 9 flows belonging to AF_{3x} class, and th_{max} setting will perform for the three AF_{32} subclass flows. Like in the first stage, it was set a large range of th_{max} (40, 80, 160, 320 and 640).

At receiver's end it was measured the maximum and mean delay values for the 9 AF_{3x} flows and also the drop packet percent. Figures 9 and 10 illustrate maximum and mean delay values for the best results obtained ($th_{max} = 80$ and 160).

Optimum value identification for packet drop maximum threshold is obtained through a correlation between minimum delay and minimum packet loss, which can be extracted from network node's interface (figure 11) and also from IXIA equipment (figure 12).

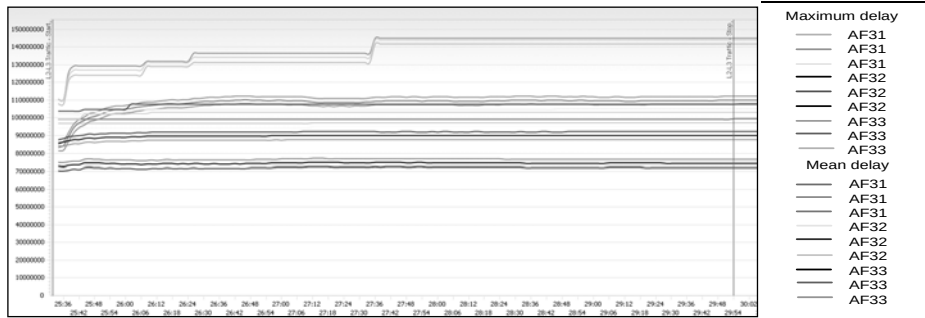


Figure 9: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=5$ and $th_{max}=80$

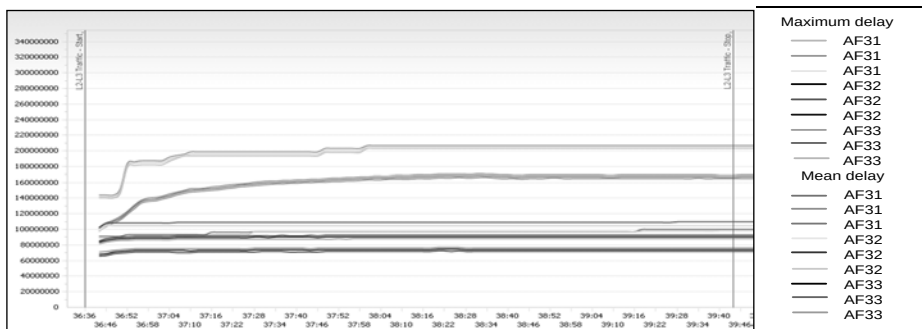


Figure 10: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=5$ and $th_{max}=160$

dscp	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Mean queue	Maximum thresh	Mark probe
af31	55445/44134220	10306/8203576	3/2388	32	35	40	1/10
af32	55443/44132628	10311/8207556	0/0	28	31	40	1/10
af33	55440/44130240	10315/8210740	0/0	24	27	40	1/10
af31	65642/52251032	12211/9719956	0/0	32	35	40	1/10
af32	65649/52256604	12204/9714384	0/0	28	41	80	1/10
af33	65638/52247848	12215/9723140	0/0	24	28	40	1/10
af31	48184/38354464	8951/7124996	0/0	32	36	40	1/10
af32	48210/38375160	8925/7104300	0/0	28	61	160	1/10
af33	48179/38350484	8956/7128976	0/0	24	30	40	1/10
af31	67423/53668708	12536/9978656	6/4776	32	34	40	1/10
af32	67515/53741940	12450/9910200	0/0	28	126	320	1/10
af33	67416/53663136	12549/9989004	0/0	24	28	40	1/10
af31	57349/45649804	10661/8486156	3/2388	32	34	40	1/10
af32	57541/45802636	10472/8335712	0/0	28	225	640	1/10
af33	57346/45647416	10667/8490932	0/0	24	29	40	1/10

Figure 11: Influence of packet drop maximum threshold variation on packet drop extracted from the node's interface

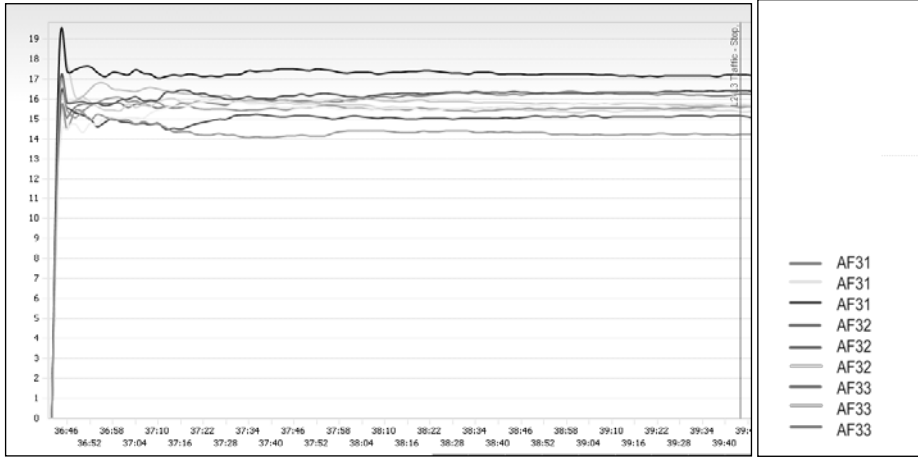


Figure 12: Critical data flows (AF_{3x}) packet loss (%) for $n=5$ and $th_{max}=160$

Based on the correlation, it could be concluded that the optimum configuration for minimum delay and packet loss is $n = 5$ and $th_{max} = 160$.

Maximum Packet Marking Probability Influence On Maximum Delay Value

The last stage will conclude the previous configuration in order to identify an optimum value of maximum packet marking probability value max_p . This value setting is useful in the moments of a supplementary traffic appearance, which doesn't respect a normal profile. Under this condition, until the capacities will be redimensioned, is useful to apply an aggressive packet dropping policy, which will assure a nondiscretionary flow access to queue processing resources.

In order to maintain a common reference, the optimum value obtained in previous stage ($n = 5$, $th_{max} = 160$) was configured for all 9 flows belonging to AF_{3x} class and the max_p setting will be performed for the three AF_{33} subclass flows. It was set a large range for max_p (1, 1/5, 1/10, 1/20 și 1/200).

At receiver's end it was measured the maximum and mean delay values for the 9 AF_{3x} flows and also the drop packet percent. Figures 9 and 10 illustrate maximum and mean delay values for the best results obtained ($max_p = 1$ and 1/5).

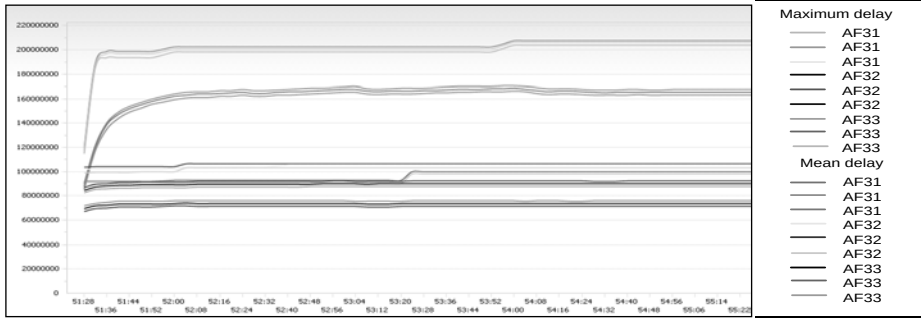


Figure 13: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=5$, $th_{max}=160$ and $max_p=1$

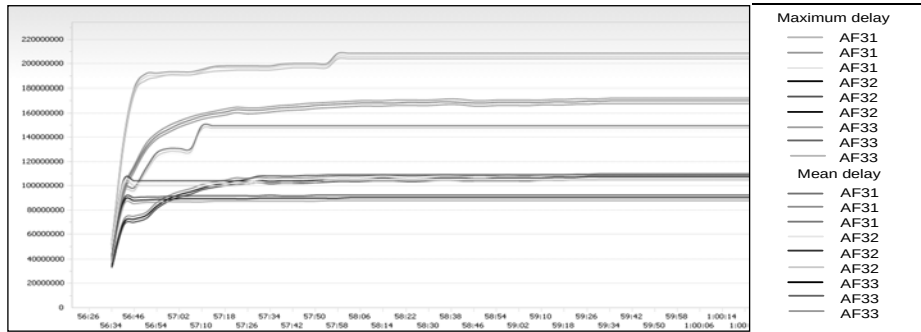


Figure 14: Critical data flows (AF_{3x}) mean and maximum delay (ns) for $n=5$, $th_{max}=160$ and $max_p=1/5$

Identification of optimum value for packet drop maximum threshold is obtained through a correlation between minimum delay and minimum packet loss, which can be extracted from network node's interface (figure 15) and receiver module within IXIA equipment (figure 16).

dscp	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Mean queue	Maximum thresh	Mark probe
af31	67358/53616968	12529/9973084	0/0	32	35	40	1/10
af32	67392/53644032	12495/9946020	0/0	28	69	160	1/10
af33	67354/53613784	12536/9978656	0/0	24	29	160	1/1
af31	45736/36405856	8487/6755652	8/6368	32	35	40	1/10
af32	45772/36434512	8459/6733364	0/0	28	70	160	1/10
af33	45747/36414612	8484/6753264	0/0	24	46	160	1/5
af31	67140/53443440	12489/9941244	0/0	32	36	40	1/10
af32	67173/53469708	12456/9914976	0/0	28	70	160	1/10
af33	67176/53472096	12456/9914976	0/0	24	68	160	1/10
af31	49453/39364588	9188/7313648	0/0	32	35	40	1/10
af32	49484/39389264	9157/7288972	0/0	28	66	160	1/10
af33	49525/39421900	9116/7256336	0/0	24	106	160	1/20
af31	63957/50909772	11891/9465236	4/3184	32	34	40	1/10
af32	63991/50936836	11861/9441356	0/0	28	69	160	1/10

Figure 15: Influence of maximum drop packet probability variation on packet drop extracted from the network node's interface

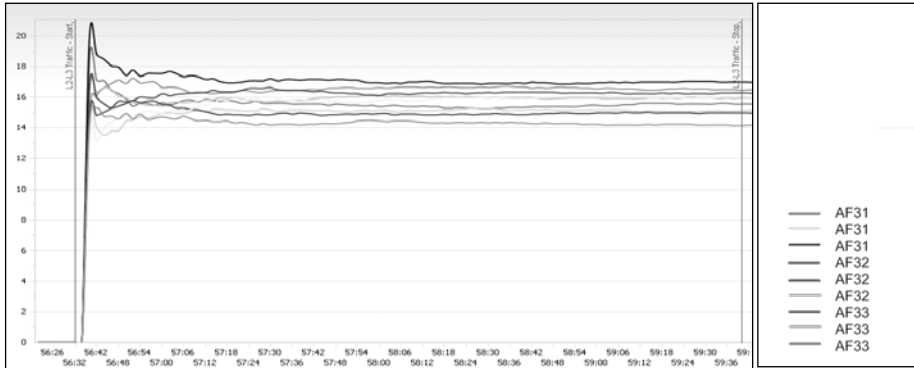


Figure 16: Critical data flows (AF_{3x}) packet loss (%) for $n=5$, $th_{max}=160$ and $max_p=1/5$

Based on the correlation, it can be identified a proper maximum packet drop probability value in the interval $max_p = 1 \div 1/10$, which conducts to a final parameter set of $n = 5$, $th_{max} = 160$ and $max_p = 1, 1/5$ or $1/10$ (the punctual values of max_p are conditioned by the technical limitations of Cisco routers).

Results Evaluation

As a conclusion about the presented results, it could be possible to perform a delay control within waiting queues associated to data traffic through an iterative adjustment of the main three parameters, which determine queue behavior. These are the mean queue length, the packet drop maximum threshold value and the maximum packet drop marking probability. Dimensioning the three parameters must also take into account the packet dropping percent in order to prevent the situation when the maximum delay can be controlled, but the traffic efficiency is very low because of a great number of retransmitted packets, or, in even critical cases, when we can face the situation of global synchronisation for all flows which transit the queue.

Results are conditioned by a preliminary bandwidth calculation for each data service class, in order to assure a ratio between serialisation speed and traffic volume, which could allow an efficient function of proposed control procedure. If not, massive packet accumulation will conduct to an accentuate degradation of data flows (through an adequate packet dropping), so that delay control procedure will be totally inefficent for quality of service level, required by specific traffic.

5. Conclusions

This paper's aim was to present some important aspects regarding the delay control within network nodes. It was denoted that one of the main objective followed in order to assure a maximum quality of service level within networks is the end-to-end delay control for delivered services. In order to perform this control, firstly it must be determined the main

components which influence the total delay value in the network. As it was presented, end-to-end delay could be split in a deterministic and a stochastic component, each of them representing a sum of all values, which influence each network segment (build from network nodes and interlinks).

If in case of deterministic delay it could be assumed a maximal delay value, according an initial network, implemented protocols within network nodes and bandwidth allocation dependent on delivered traffic classes, in case of stochastic delay, dependent almost exclusively on queuing delay, maximum value could be assumed only after a fine adjustment of parameters, which define queue behavior.

On this line, the paper proposes a delay control through a three steps procedure, which aims the adjustment of how the mean queue length follows the instantaneous queue length (first iteration), the packet drop maximum threshold (second iteration) and the maximum packet drop marking probability (third iteration).

In order to validate the proposed procedure, it was built a testing environment, which simulates three networks, a source and destination network linked through an intermediate network serving as transport medium between the two above mentioned networks. Measured values of delay and packet loss percent confirm the functionality of this procedure.

References

1. *ITU-T Recommendation Y 1540*, Internet protocol data communication service – IP packet transfer and availability performance parameters, 2002;
2. *ITU-T Recommendation Y 1541*, Network performance objectives for IP-based services, 2002;
3. *C.J. Bovy, H.T. Metrodimedjo et. al.*, Analysis of end-to-end delay measurements in Internet, Passive and Active Measurement Conference, 2002;
4. B. Y. Choi
5. *G. Hooghiemstra, P.V. Mieghem*, Delay Distributions on Fixed Internet Paths, Technical Report, Delft University of Technology, Information Technology and Systems, 2001;
6. *Ramaswamy Ramaswamy, Ning Weng, Tilman Wolf*, Characterizing Network Processing Delay, Proc. of IEEE Global Communications Conference, 2004, pp. 1629-1634;
7. *S. Floyd and V. Jacobson*, Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, vol. 1, no. 4, Aug. 1993;
8. ***, RED queuing discipline, <http://www.opalsoft.net/qos/DS-26.htm>
9. *Codruț Mitroi, Dragoș Stroescu*, Optimisation of congestion management mechanisms within Customer Equipment node in an Intranet network, in course of issue in U.P.B. Scientific Bulletin, Series C: Electrical Engineering and Computer Science;