©2016 Published in 4th International Symposium on Innovative Technologies in Engineering and Science 3-5 November 2016 (ISITES2016 Alanya/Antalya - Turkey)

Performance Analysis of IP Network Using Two-Way Active Measurement Protocol (TWAMP) and Comparison with ICMP (Ping) Protocol in a Saturated Condition

*[1]Kahraman ZAİM and [2]Asst. Assoc. Dr. Cemal KOÇAK
*[1] Institute of Informatics, Department of Information Systems Gazi University, Turkey
[2] Faculty of Technology, Department of Computer Engineering Gazi University, Turkey

Abstract

The IETF's IP Performance Metrics (IIPM) group looks in to the definition of a Two-Way Active Measurement Protocol (TWAMP), defined in RFC 5357. This protocol can be considered as defining a flexible method for measuring round-trip IP performance between two end devices in a specific network that may be a wired or a wireless IP network supporting the TWAMP protocol. The TWAMP protocol has more precise and accurate results than commonly used protocol ICMP (Ping). In this study, the aim is to compare and analyze the sensitivity and accuracy of the IP network performance for TWAMP and ICMP (Ping) protocols in a saturated traffic condition. According to active measurement method, round-trip delay, jitter and packet loss values, the main criteria of end-to-end IP network performance, are measured. At the end of the real-time test process, TWAMP protocol is to be found more sensitive and convenient than ICMP (Ping) protocol for end-to-end multimedia communication.

Keywords: TWAMP, ICMP (Ping), Performance Measurement of IP Networks, Active Monitoring, Passive Monitoring

1. Introduction

Internet Protocol (IP) networks have become a dominant role for bringing information to users in the worldwide. As IP becomes the transport layer of choice, operators are faced with significant challenges to provide accurate and relevant measurement of IP network performance. That's why, measurement and estimation of performance parameters in IP networks are becoming increasingly important for today's telecommunication operators. There are several reasons to develop efficient and reliable methods in this field. Deployment of the differentiated services in IP networks require effective but also simple methods for measurement of relevant performance parameters to support and verify Service Level Agreements (SLA) with customers. A monitoring system must also support the daily operation, traffic control and planning of an operator's network with timely measurements and estimates. Tools are available such as ICMP Ping/TraceRoute and UDP Echo, but these provide limited value in the context of performance as they typically lack precision or accuracy. Performance testing is the key element of service delivery in telecom networks. Because of the recent high usage of video and voice applications in IP networks, telecom operators are forced to measure performance of their IP networks sensitively. That's why, Two-Way Active Measurement Protocol (TWAMP), is the latest IP performance measurement protocol that is recently used for end-to-end multimedia communicion.

In literature, the measurement of IP network performance with TWAMP protocol cases have remained as more theoretical bases and there are a few real-time protocol analysis. Generally, it is possible to see many analysis about the ICMP (Ping) protocol.

*Corresponding author: Address: Institute of Informatics, Department of Information Systems Gazi University, 06000, Ankara TURKEY. E-mail address: kahramanzaim@hotmail.com Phone: +903123165808

At Backstrom's thesis, which was made in 2009, One-Way Active Measurement Protocol (OWAMP), TWAMP, ICMP (Ping) and some special simulators were used to measure the end-to-end IP network performance and the results were compared [1]. It was also mentioned about the active measurement method. At the end of the studies, it was proved that is how important to measure the IP network performance metrics with TWAMP protocol. Soumyalath, Rakesh and Manjunath have a work that measured the performance of the wireless IP network with TWAMP protocol and the results were evaluated [2]. This study is used for WIFI and 3G, and by using TWAMP-Client and TWAMP-Server embedded applications to mobile phone, TWAMP protocol tests were performed and the results were compared. H-Log QoS Telecom Company has a whitepaper [3] that describes the advantages of TWAMP protocol and compares the measurable Key Performance Indicators (KPIs) and their accuracy with TWAMP, OWAMP and ICMP (Ping) protocols.

In this study, end-to-end performance metrics of IP network are measured with the TWAMP and widely used protocol ICMP (Ping) and then their results are compared. For the measurement of the IP performance metrics, probe devices have been placed to different two end points in a IP network. While tests are running on the recommended topology, one of the probe connection of the router's bandwith is being limited, that is the test link is saturated. Here, the main goal is to see the accuracy and sensitivity of performance measurements of the TWAMP and ICMP (Ping) protocols in a saturated link. The most important IP performance metrics such as round-trip delay, jitter and packet loss values are measured and analysed in the process. 64-byte sample test packets with Best Effort, Video and Voice traffic classes are used in the study as well.

The organisation of this paper is as follows. The TWAMP and its architecture are described in Section 2. The performance monitoring methods are described in Section 3. Next, the meaning of IP Differentiated Services Code Point (DSCP) is described in Section 4. The test topology and evaluation of the test results are described in Section 5. Finally, the concluding remarks are mentioned in Section 7.

2. Twamp

TWAMP is a new generation technology that measures the QoS (Quality of Service) KPIs between any two points of IP Network. The Internet Engineering Task Force (IETF)'s working group on IP Performance and Metrics developed RFC-5357 TWAMP protocol [4]. The TWAMP protocol is a standard-based and effective performance monitoring process that expands upon the OWAMP specification defined in RFC-4656 with the addition of the performance measurement of round-trip and two-way metrics for IP based networks. This means that TWAMP is based on the OWAMP protocol and their architectures are very similar. The TWAMP measurement architecture is usually comprised of two hosts with specific roles, and this allows for some protocol simplifications, making it an attractive alternative in some circumstances. This protocol delivers a flexible method for accurately measuring unidirectional and round-trip performance between two TWAMP-supported endpoints, regardless of device type or vendor [1]. Unlike the OWAMP protocol, synchronization of clocks of hosts participating in protocol is not required to obtain two way metrics namely round-trip time, jitter and packet loss [2].

TWAMP protocol consists of two inter-related protocols: The TWAMP-Control and the TWAMP-Test protocols. The TWAMP-Control protocol is responsible to initiate, start and stop

the test sessions whereas TWAMP-Test protocol is used to exchange of the packets within the two TWAMP entities. The architecture of the TWAMP protocol is shown in Figure 1 [1-3].

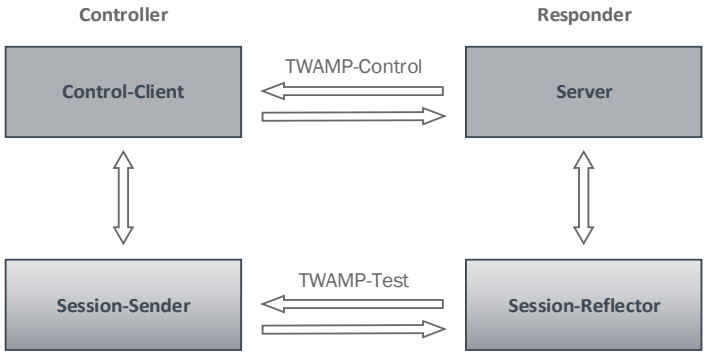

Figure 1. TWAMP Architecture

The role of the Control-Client and Session-Sender are implemented in one host referred to as "Controller", and the roles of Server and Session-Reflector are implemented in another host referred to as "Responder". This architecture supports a full-TWAMP standard. In the full-TWAMP protocol, the Client initiates the TCP-based negotiation by connecting to the TWAMP port on the Server, which is 862 by default. The Server responds with some information about its characteristics, especially its authentication level, and a negotiation of the test follows. If the negotiation is successful, the test itself starts, again the Client initiates the test by generating UDP test traffic towards the port number that was specified by the Server. The Server responds to each UDP packet using a precise test methodology that involves exchanging timestamps. At the end of the test, the Client computes the measurements which can then be reported [4].

2.1. Twamp-Control

The TWAMP-Control protocol initiates, starts, and stops test sessions and to fetch their results that allows the two end points to initialize a performance monitoring session [2]. This protocol consists of two sub-components: "Control-Client" and "Server". The Control-Client is a network node that starts and stops TWAMP-Test sessions. And the Server is a network node, which facilitates one or more test sessions. The role of the server is similar to OWAMP, it configures the test end points. All metrics are obtained, analyzed and published by Session-Sender only [6]. This protocol runs over TCP port number 862 by defult and is used to initiate and control measurement sessions. The sequence of commands are as "request-session", "start-session" and "stop-session" but unlike, the connection setup exchanges, the TWAMP-Control commands can be sent multiple times. However, the messages cannot occur out of sequence although multiple request-session commands can be sent before a session-start command [6].

2.2. Twamp-Test

The TWAMP-test protocol exchange test packets between two network nodes used to obtain metrics. This protocol consists of two sub-components: "Session-Sender" and "Session-Reflector". The Session-Sender is a network node, which sends test packets to the Session-Reflector and receives test packets from Session-Reflector, during test sessions [2]. In the

TWAMP architecture, the session-sender is able to receive measurement data and to communicate the results back to the control-client. Session-Reflector reflects test packets sent by Session-Sender, as part of test session. Unlike the Session-Receiver, it does not collect any information from the test packets as round-trip delay information is available only after the reflected test packet has been received by the Session-Sender [7]. The TWAMP-Test runs over UDP and exchanges TWAMP-Test packets between Session-Sender and Session-Reflector. The Session-Sender and the Session-Reflector will use the same UDP port to send and receive packets. These packets include timestamp fields that contain the instant of packet egress and ingress. In addition, each packet includes an error-estimate that indicates the synchronization skew of the sender with an external time source. The packet includes a Sequence Number as well [6]. In the TWAMP-Test protocol, there are three types of modes: Unauthenticated, Authenticated ve Encrypted [4].

3. Performance Monitoring Methods

The performance of an IP network has vital importance to both the service providers and the customers. Performance can be measured with parameters such as delay, jitter and packet loss [8]. Traditionally, there are two methods of IP network performance measurement, which are active monitoring and passive monitoring methods. The passive monitoring method obtains the current status of the network by capturing the packet. This monitoring allows watching what is occurring on a live system without actually sending out data to replicate what customers are doing on the systems. This monitoring method can monitor the network status without additional traffic. In this monitoring method, data is gathered by passively listening to network traffic such as by using link splitters or hubs to duplicate a link's real-time traffic or by monitoring buffers in routers. This method usually produces only highly aggregated data and thus provide only little information on the network state or traffic behavior [9].

The active monitoring method which is focused on this article obtains the current status of the network by setting up the test machine at the any points. Active measurements generate special probe packets that are sent over the network to the available capacity of a network path or the response time of an application. Here, a probe packet is an artificial packet that can be any type depending on the information wanted from the measurement. A simple example of a probe packet could be a small UDP packet that contains only a timestamp and little or no payload at all. Unlike passive measurements, active measurements generate additional network traffic so they may possibly disturb the normal traffic flow. This is why active measurements have to be carefully planned before execution [7].

The Active measurements do not require huge amounts of storage space and system load is very low because the amount of generated and analyzed traffic is small compared to passive monitoring method. Also, when using active probing, there are no privacy issues since the data used does not contain any private information. When it comes to accuracy of measurements, passive methods are often more accurate. For example packet loss can be measured very accurately by monitoring router buffers along the network path. Also, available bandwidth can be accurately measured by monitoring link usage on routers. Both above mentioned measurements are difficult to do accurately with active probing [7]. The mechanism of Active and Passive monitoring is listed on Table 1.

Table 1. Performance Montoring Mechanism

Monitoring Method	Mechanism
Active Monitoring	▪ Generate test traffic periodically or on-demand ▪ Measure performance of test packet or response
Passive Monitoring	▪ Capture the traffic by mirroring or splitting ▪ Analyze the captured packets

The well known active measurement tools is probably Ping which is built in and generally by supported most operating systems. It is often used for determining if a host is properly connected to the network as well as the round-trip time to that host. Ping uses the ICMP packets contain a sequence number, and by timestamping when packets are sent and replies are received, the round-trip time can be calculated. Depending on the implementation, the number of lost packets and duplicates is reported. Although Ping is widely used, it is a bad way to measure performance metrics. ICMP packets are often treated differently than for example UDP packets, and may be rate limited in a router. Many devices also refuse to reply to an incoming echo request for security reasons [1].

4. The IP Differentiated Services Code Point (DSCP)

Differentiated services or DiffServ (DS) is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks [10]. DS increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. The DS architecture defines the DiffServ field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing. Based on the Differantaited Services Code Point (DSCP) or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way [11].

The six most significant bits of the DiffServ field is called as DSCP. The last two Currently Unused (CU) bits in the DiffServ field were not defined within the DiffServ field architecture; these are now used as Explicit Congestion Notification (ECN) bits [11]. Routers at the edge of the network classify the packets and mark them with either the IP Precedence or DSCP value in a DS network. Other network devices in the core that support Diffserv use the DSCP value in the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment. In Figure 2, there is a review of the ToS byte and the DSCP fields defined by RFC 791 [12].

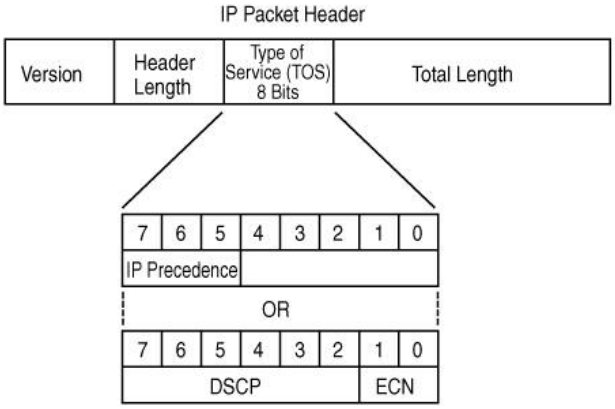

Figure 2. IPv4 Packet Header – ToS and DSCP Review

Best-Effort - DSCP0 traffic class delivery describes a network service in which the network does not provide any guarantees that data is delivered or that a user is given a guaranteed quality of service level or a certain priority. In a best-effort network, all users obtain best-effort service that obtain unspecified variable bit rate and delivery time, depending on the current traffic load. It can be contrasted with reliable delivery, which can be built on top of best-effort delivery [13].

Assured Forwarding– DSCP34 behaviour 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. The AF behavior group defines four separate AF classes where all have the same priority. Within each class, packets are given a drop precedence (high, medium or low, where higher precedence means more dropping). The combination of classes and drop precedence yields twelve separate DSCP encodings from AF11 through AF43 [14].

Expedited Forwaring–DSCP46 behaviour has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for especially voice and other realtime 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 [15]. The DSCP bits and its comparison of the traffic classes are shown in Table 2.

Table 2. DSCP Bits and Comparison of the Traffic Classes

Traffic	DSCP PHB (per-hop behavior)	DSCP Decimal
Bronze-Data (Best Effort)	BE	0
Silver-Data (app1)	AF11	10
Silver-Data (app2)	AF12	12
Silver-Data (app3)	AF13	14
Gold-Data (app1)	AF21	18
Gold-Data (app2)	AF22	20
Gold-Data (app3)	AF23	22
Voice-Control	AF31	26
	AF32	28
	AF33	30
Video	AF41	34
	AF42	36
	AF43	38
Voice	EF	46

5. Test Topology and Evoluation of the Test Results

The test topology is infrustructured between two routers to where ICMP (Ping) and TWAMP protocols supported probes are diretly connected. The probes have capability to generate virtual traffic and the test procedure is focused on the active monitoring method. Recommended test topology is shown at Figure 4.

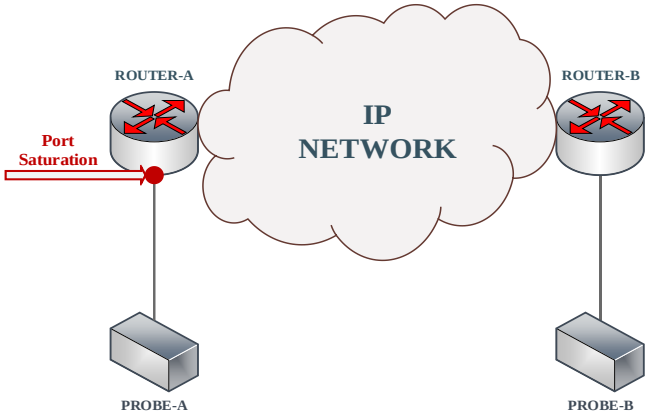

Figure 4. Test Topology

In this study, the main goal is to measure the end-to-end performance metrics of IP network by using TWAMP and ICMP (Ping) protocols with a saturated port condition, see the affects of saturation to the monitoring methods and compare the performance results.

As mentioned at the second part of the article, Probe A sends the test packets to Probe B and then Probe B reflects them. The time interval between two consequtive packets is set to 50 miliseconds (ms). The sampling parameters for TWAMP and ICMP (Ping) methods that is used in the study is shown in Table 3.

Table 3. Sampling Scenario of the Test

Number of Test Samples	60.000
Delay between packets (ms)	50
Size of the Test Packets (bytes)	64

According to test results that is performed with 64-byte probe test packets, the Round-Trip Delay values are almost same for TWAMP and ICMP (Ping) protocols, but values are very high because of the port saturation on test topology. That's why, the amount of the test traffic capasity is more than saturated port bandwith value, the Round-Trip Delay values are higher than it should be. The comparision of the Round-Trip Delay Values for TWAMP and ICMP (Ping) Protocol Test Results are shown at Figure 5.

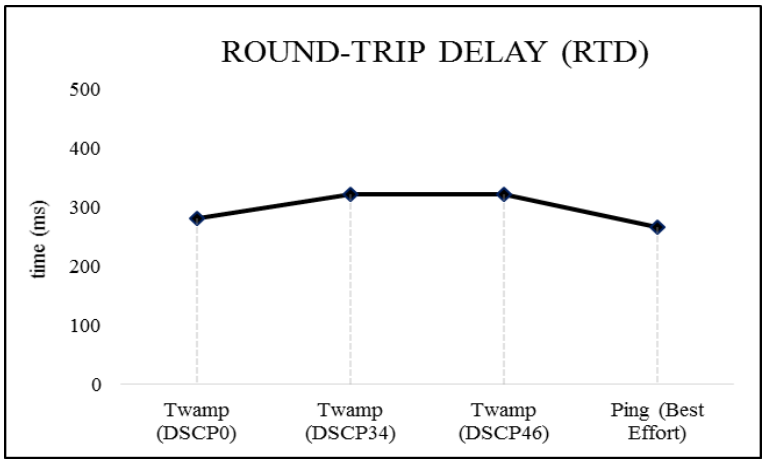

Figure 5. Comparision of the Round-Trip Delay Values for TWAMP and ICMP (Ping) Protocol Test Results

According to test results that is performed with 64-byte probe test packets, the Jitter values are almost same for TWAMP and ICMP (Ping) protocols, but values are very high because of the port saturation on the topology. That's why, the amount of the test traffic capasity is more than saturated port bandwith value, the Jitter values are higher than it should be. Normally, the jitter value is calculated with the consequtive paket delay values, but in this study, since there is a bandwith limit on the line, it is possible to see packet losses or high response time to sent packet. The comparision of the Jitter Values for TWAMP and ICMP (Ping) Protocol Test Results are shown at Figure 6.

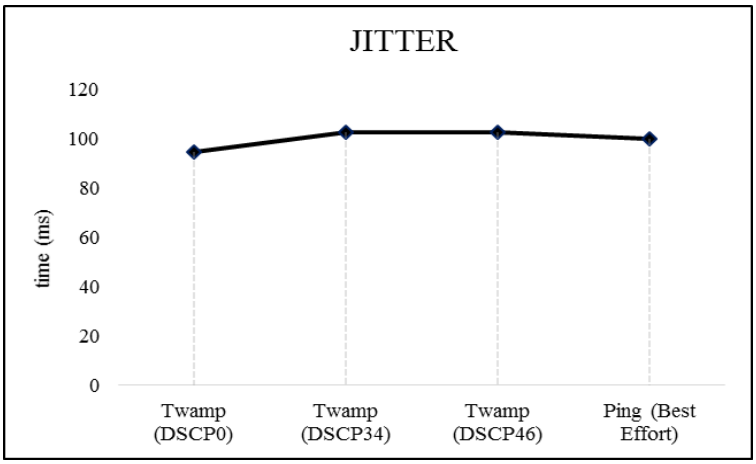

Figure 6. Comparision of the Jitter Values for TWAMP and ICMP (Ping) Protocol Test Results

According to test results that is performed with 64-byte probe test packets, the Packet Loss values are absolutely different for TWAMP and ICMP (Ping) protocols. In terms of the traffic classes, the results seem changeble because of saturation on the test port. The test results for TWAMP (DSCP34) and TWAMP (DSCP46) almost zero, since their traffic classes have higher priority for trasmission and as we know they are called real-time traffics. Unlike The test results for TWAMP (DSCP34) and TWAMP (DSCP46), TWAMP (DSCP0) and Ping (Best Effort) packet loss rate is very high because of their low priority. Actually, the test results are occurred as we predicted

before test procedure. The comparision of the Packet Loss Values for TWAMP and ICMP (Ping) Protocol Test Results are shown at Figure 7.

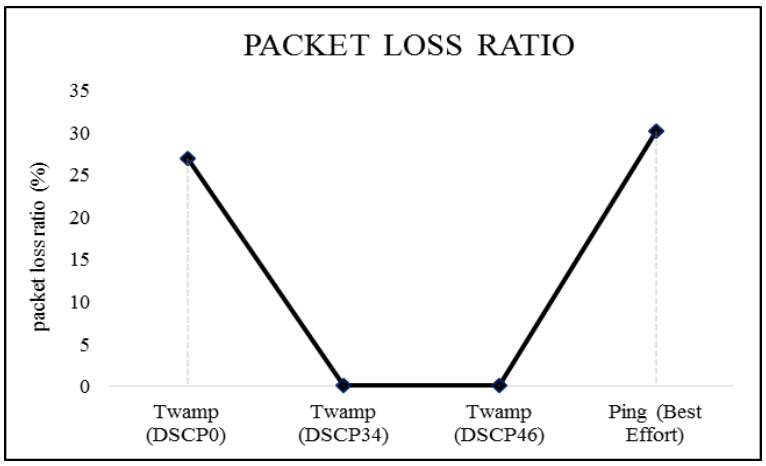

Figure 7. Comparision of the Packet Loss Values for TWAMP and ICMP (Ping) Protocol Test Results

6. Conclusion

TWAMP is the latest technology implemented to give to service providers a complete visibility on the performance of their IP based Network infrastructure. The TWAMP implementation presented in this report has been proven useful for measuring network performance metrics. ICMP (Ping) is a good enough to have some indication regarding IP connectivity of one network equipment and get a rough value of round-trip delay measurement, but this tool cannot be used as a reference. Along with the high correctness of the measurements in the tested environment, the TWAMP implementation must be considered successful, and the TWAMP protocol can be established as a competitive alternative for network performance measurements.

The implementation presented in this work has been evaluated in a saturated IP network by comparing between TWAMP and ICMP (Ping) protocols which are active monitoring methods. The results using this methods are the estimates of round-trip delay, jitter and packet loss between two nodes. During the comparison of the protocols, this three performance metrics are compared in terms of Best Effort, Voice and Video traffic classes. According to test results that is performed with 64-byte probe test packets, the Round-Trip Delay and Jitter values are almost same for TWAMP and ICMP (Ping) protocols, but Packet Loss is not. The Packet Loss results for TWAMP (DSCP34) and TWAMP (DSCP46) almost zero, since their traffic classes have higher priorities than TWAMP (DSCP0) and Ping (Best Effort) protocols. Since TWAMP (DSCP34) and TWAMP (DSCP46) known as real-time traffics, it is important to get lower packet loss value in the saturated condition. This means that TWAMP protocol has accurate and sensitive result for Packet Loss value rather than ICMP (Ping) protocols. This implemantation proves that TWAMP protocol should be used for measurement of IP network performance because of its accuracy and sensitivity.

References

[1] Backstrom I, Performans Measurement of IP Network using the Two-Way Acive Measurement Protokol, Master of Science Thesis, Stockholm, Sweden, 2009
[2] Soumyalatha N. , Rakesh KA ve Manjunath RK, Performance Evaluation of IP Wireless Networks using Two Way Active Measurement Protocol, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013
[3] TWAMP, TWAMP White paper. Access Date: 10.08.2016, http://www.hlog-qostelecom.com/uploads/media/files/twamp---rfc-5357---white-paper---13-08-15.pdf
[4] Hedayat H, Krzanowski R, Morton A, Yum K, Babiarz J, A Two-Way Active Measurement Protocol, RFC-5357, October, 2008
[5] Skurowski1 PL, W´ojcicki1 R, and Jerzak Z, Evaluation of IP transmission jitter estimators using One-Way Active Measurement Protocol (OWAMP), Communication in Computer and Information Science, June 2010
[6] Cisco Nexus 1000V Quality of Service Configuration Guide, DSCP and Presedence Values, Chapter 6, Release 4.0(4) SV1(1)
[7] Mohan V, Janardhan YR, Kalpana K, Active and Passive Network Measurements: A Survey, Venkat Mohan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , pp. 1372-1385, 2011
[8] Hasib M., Schornmans JA, Limitations of Passive & Active Measurement Methots in Packet Networks, Department of Electronic Engineering, Queen Mary, University of London
[9] Lee HJ, Kim MS, Hong JW, Lee GH, "QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring, 2002
[10] IETF Network Working Group. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Request for Comments: 2474 (RFC-2474), Dec. 1998
[11] Cisco, Implementing Quality of Service Policies with DSCP, Feb. 15, 2008. Access Date: 10.08.2016, http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-parking/10103-dscpvalues.html
[12] IETF Network Working Group. Internet Protocol, Request for Comments: 791 (RFC-791), September, 1981
[13] IETF Network Working Group. Comments on the Usefulness of Simple Best-Effort Traffic, Request for Comments: 5290 (RFC-5290), July, 2008
[14] IETF Network Working Group. Assured Forwarding PHB Group, Request for Comments: 3260 (RFC-3260), April, 2002
[15] IETF Network Working Group. An Expedited Forwarding PHB (Per-Hop Behavior), Request for Comments: 3246 (RFC-3246), March, 2002