Performance Measurement of IP Networks using Two-Way Active Measurement Protocol

Cemal KOCAK
Department of Computer Engineering
Gazi University
Ankara, Turkey
ccckocak@gazi.edu.tr

Kahraman ZAIM
Department of Information Systems
Gazi University
Ankara, Turkey
kahramanzaim@gmail.com

***Abstract*— The use of real-time multimedia applications in IP networks is continuously increasing with the services provided by the evolving internet infrastructure. Providing Quality of Service (QoS) is important for service providers in terms of real-time voice and video services to meet users' expectations. For this reason, QoS parameters such as network latency, jitter and packet loss must be accurately and precisely measured. The widely used PING protocol for measuring the specified parameters do not give accurate and precise results at the desired level. In this study, it is proposed to use Two-Way Active Measurement Protocol (TWAMP) for measuring the QoS parameters of the IP network. TWAMP is the latest method to fully deliver performance metrics for IP network infrastructure. According to the active measurement method, round trip delay, jitter and packet loss parameters between two end nodes were measured with TWAMP and PING protocols and analyzed by comparing values. As a result of the study, it has been shown that TWAMP protocol recommended for multimedia communication is suitable for measuring service quality of IP Networks.**

Keywords—TWAMP; performance measurement of IP networks; active measurement method; passive measurement method; PING; differentiated service code point

I. INTRODUCTION

Quality of Service (QoS) is a concept that has gained importance after data and voice traffic are widely used on IP networks. Service Quality is a broad term used to describe the overall service experience that a user or application receives from the network. The main purpose of service quality is to enable the most efficient use of existing bandwidth. In this context, in order for internet service providers to provide end-to-end quality of service in the IP network, it is necessary to ensure that the network components intervene steadily in the data flow through the network. In addition, when services are being designed, the service has shown high performance and measurement of quality parameters has become an indispensable requirement. Round-Trip Delay (RTD), Jitter and Packet Loss parameters are critical in ensuring the QoS required and providing a successful end-to-end service. Service providers have gone one-step further give the realization values of service quality parameters as commitments to customers and create a value-added space in intense competition environment. For this reason, service providers need to measure service quality parameters with specific methods [1, 2].

The most common measurement method used to measure service quality parameters is PING protocol. PING is supported by almost all systems and uses the Internet Control Message Protocol (ICMP) for packet delivery. Although PING protocol is a commonly used measurement protocol, it can be limited on devices or completely rejected incoming packets. This shows that measurement method is limited [2].

Two-Way Active Measurement Protocol (TWAMP) is a next-generation standard that supports layer-3 protocols of the OSI reference model and is used to measure IP network performance values between any two devices. Measuring IP network performance is gaining in importance every day in the name of measuring the service quality of IP services offered by Internet service providers or network operators and giving SLA (Service Level Agreement) commitments to customers. Today, because of the importance of multimedia services such as Voice and Video, it requires more precise measurement of IP network performance values of any service providers. Because of the fact that video and voice packets are transmitted in real time, and they are quickly affected by problems in the network, it has become necessary to monitor performance metrics extensively and continuously from end-to-end. The latest technology introduced for these metrics and which has recently been widely used is the TWAMP protocol [3].

In the literature, there is a few real-time application study related to the use of TWAMP protocol to measure IP network performance values for multimedia services.

Zaim and Kocak had a study in 2016 that they compared the PING and TWAMP protocol performance results in order to see the accuracy and sensitivity of the protocols in a saturated IP network condition. They have proved that TWAMP protocol had more accurate and sensitive results than PING protocol in limited bandwidth, especially for packet loss parameters [2]. In the thesis study of Backström in 2009, performance measurements of IP network were made between two points for OWAMP (One Way Active Measurement Protocol), TWAMP and PING with some special simulators and the values were compared [4]. At the end of the study, it had been proven how important TWAMP application is to measure network performance metrics. In

978-1-5090-6332-1/17/$31.00 ©2017 IEEE

the study conducted by Soumyalatha and colleagues, the performance of the IP Wireless network was measured by TWAMP protocol and the results were evaluated. For this study, tests were performed with TWAMP Client and Server applications installed on mobile phones using WIFI and 3G, and the results of performance metrics were compared [5].

In this study, IP network performance between the two points was measured with the active measurement method, TWAMP, and the results were compared with the PING protocol, which is the widely used active measurement method. 64-byte test packets have been used with Best Effort, Voice and Video traffic classes during the measurement. At the end of the study, Wireshark [6] outputs of the tests made with TWAMP and PING protocols were taken and the important parameters in the outputs were evaluated. For the measurements made using the proposed protocols, probe devices in the IP network were placed at two nodes and virtual test packets were sent by probes from one point to the other.

In the second part of the study, the definitions of TWAMP Protocol, Performance Measurement Methods and Differentiated Services Code Point (DSCP) are explained. In section 3, the test topology and details used for the TWAMP and PING protocols are discussed, and the results of the measurements of the study and the statistics of the comparative data are also included. Verification of traffic classes used in tests is provided with Wireshark screen output as well. In the fourth and last section, the results of the study are evaluated and recommendations are given.

II. Definitions

A. *Twamp*

TWAMP is the next generation IP performance measurement protocol documented by the IETF IP Performance Metrics (IPPM) working group in October 2008 [7, 8]. Two-way IP performance metrics can be obtained with this protocol. TWAMP delivers a flexible method for accurately measuring unidirectional and round-trip performance between two TWAMP-supported endpoints, regardless of device type or vendor. The architecture is based on OWAMP and that adds two-way or round-trip measurement capabilities. IP network can be a wired or wireless network [9, 10, 11].

The TWAMP protocol consists of two protocols, TWAMP-Control and TWAMP-Test, which are associated with each other. In practice, the Control-Client and Session-Sender roles are implemented as "Controller" on a single host while the Server and Session-Reflector roles are implemented as "Responder" on the other host. This model supports the Full-TWAMP protocol architecture. Fig.1 shows the architecture of TWAMP protocol [2, 4, 7, 12, 13].

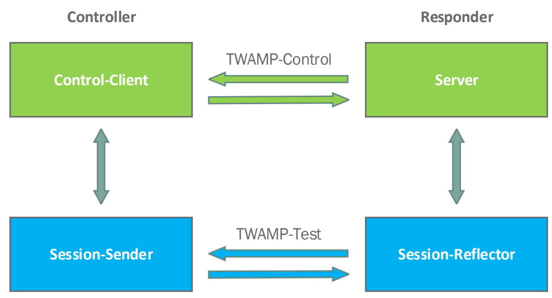


Fig. 1. TWAMP Architecture

1) *Twamp-Control*

This protocol triggers, starts, and stops test sessions. There are two subcomponents of TWAMP-Control protocol; "Control-Client" and "Server". Control-Client is the network node that initiates and stops the TWAMP-Test sessions. Server is a network node that manages one or more test sessions. It has the ability to configure endpoints per session [5]. The TCP protocol is used to establish the session, and the preferred port is 862 by default [7, 13].

2) *Twamp-Test*

This protocol allows the exchange of test packets to compute performance metrics between two points within a network. UDP protocol is used for sending test packets. The TWAMP-Test protocol has three modes: Unauthenticated, Authenticated and Encrypted [7, 12]. There are two subcomponents of the protocol; "Session-Sender" and "Session-Reflector". The Session-Sender is the network node that receives the message or information of the test packets sent and received by the Session-Reflector during the test. It also collects and records information communicated by the Session-Reflector to measure two-way metrics [5]. Session-Reflector is a network node that reflects test packets sent by Session-Sender. No packet information is collected in this section [2, 7, 13].

B. *Performance Measurement Methods*

The methods used to measure and monitor the performance of IP networks are generally divided into two main groups. These are active measurement and passive measurement methods [14, 15]. Passive measurement method is listening the real traffic and transferring, analyzing and interpreting the packets to a different place. The results obtained in this measurement are completely indicative of the end user experience and the measurement results give much more accurate results. However, it is important that the size of the listening and mirroring traffic is very large and the storage space is seriously needed. In addition, the measurement method is considered to be a less preferred method because of the data size as well as the attainment of private information or the violation of confidentiality [16]. In the Active Measurement Method, used in the study, the analysis of the virtual traffic generated by the traffic generators and the obtaining of the IP performance values are mentioned [11, 17]. Unlike the passive measurement method, the measurement scenario needs to be well planned because it occupies an extra bandwidth in a normal traffic flow. In order to perform performance measurements with active measurement method, storage area is not needed in very large capacities. Also, because there is no specific information in the contents of the test packages, it does not pose a problem in terms of confidentiality principle. All test packets are completely virtual. The well-known and commonly used IP performance measurement protocol is PING [17].

PING is a widely used active performance measurement method. It is supported by almost all systems. It uses ICMP protocol to send packets. ICMP packets contain a sequence number, and RTD time is calculated by adding time information to the packets sent and received [18]. PING is a protocol that can be limited on devices and incoming packets may be rejected and not sent. This indicates that the measurement method is limited [4]. The active measurement tool to be considered in this study is TWAMP protocol, which have been developed as new generation IP performance measurement systems.

C. Differentiated Services Code Point (DSCP)

DSCP is an IPv4 packet area that allows different levels of service assignment to network traffic. On the network, each packet on the router is marked with a DSCP code, and the packets for the service level corresponding to the code are parsed and sent. In Fig.2, there is an indication of the DSCP bits in the Type of Service (ToS) field in an IPv4 packet [19].

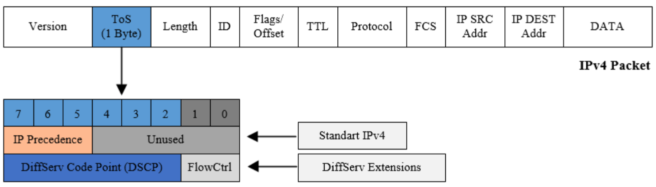


Fig. 2. IPv4 - ToS Byte and DSCP Bits

ToS field is the second field in the IPv4 packet. The first three bits of ToS byte are referred to as IP Presedence bits. Likewise, the first six bits of ToS byte are called DSCP bits. With these 6 bits, the QoS of the packet is determined. QoS is an important application after the networks have been used for audio and video transmission besides data traffic. The main purpose in QoS applications is to enable the most efficient bandwidth usage [20, 21, 22]. Table I shows the traffic classes and their corresponding DSCP bit values.

TABLE I. DSCP BITS AND CORRESPONDING TRAFFIC CLASSES

Traffic	**DSCP PHB (per-hop behavior)**	**DSCP Decimal**
Best Effort	BE	0
Video	AF41	34
Voice	EF	46

The Best Effort (DSCP0) traffic class shown in Table I is defined as a situation in which QoS is not present and operates with the "who-in-power" or first-in first-out (FIFO). If the packets such as FTP, internet, mail etc. are configured in this traffic class, they are sent on the same conditions when they arrive on the router. So there is no information on whether these packets reach the other side. It is likely to be large losses when they are transmitted with priority packets. Assured Forwarding - DSCP34 (Guaranteed Transmission) traffic class is used for other traffic that needs to be prioritized within normal traffic. It is used for sending video packets. The Expedited Forwarding – DSCP46 (Accelerated Transmission) traffic class is typically used to carry real-time voice packets. In a real network, it is the highest priority value that can be given under normal circumstances. [21].

III. ANALYSIS AND EVALUTION OF THE TEST RESULTS

The study was conducted between probe devices that support virtual traffic generation and active measurement methods such as TWAMP and PING protocols are directly connected to the two routers in the IP test network. Fig.3 shows the topology of the study.

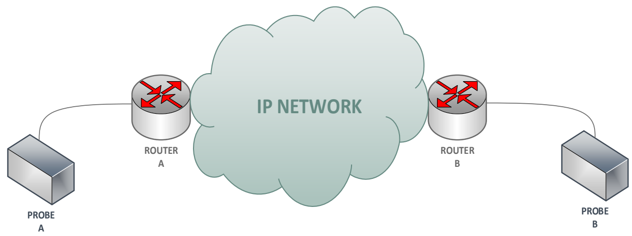


Fig. 3. Test Topology

According to TWAMP protocol architecture mentioned in section 2; the probe (controller) sends TWAMP test packets to Probe B (responder), and Probe B reflects packets. There is a delay of 50 ms between each packet transmission. The parameter values used in the tests performed for the TWAMP and PING measurement methods are given in Table II.

TABLE II. SAMPLING SCENARIO

# of Test Sampling	120.000
Delay between Two Consecutive Test Packet (ms)	50
Test Packet Size (byte)	64

It was determined that RTD values did not change with respect to traffic class for TWAMP and PING protocols according to tests performed with 64-byte packet size. Fig.4 shows the RTD values obtained according to the protocols and the traffic class.

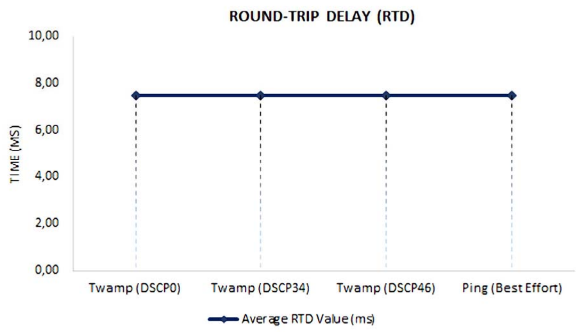


Fig. 4. RTD Values according to TWAMP and PING Protocols

It has been determined that the Jitter values did not differ much with respect to traffic class for TWAMP and PING protocols compared to tests with 64-byte packet size. Fig.5 shows the Jitter values obtained according to the protocols and the traffic class.

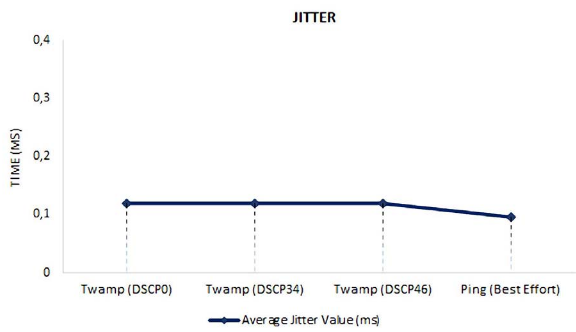


Fig. 5. Jitter Values according to TWAMP and PING Protocols

Fig.6 shows the packet loss values obtained according to protocols and traffic classes. Packet loss values are different according to traffic classes and both TWAMP and PING protocols. The losses of Video (DSCP34) and Voice (DSCP46) test packets with high traffic priority are less than those of Best Effort (DSCP0) traffic class test packets. In addition, when compared between protocols, the lower packet loss rate in tests with TWAMP protocol indicates that these two protocols measure more healthily and precisely than the PING protocol.

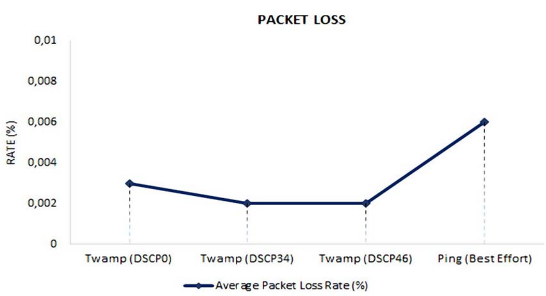


Fig. 6. Packet Loss Values according to TWAMP and PING Protocols

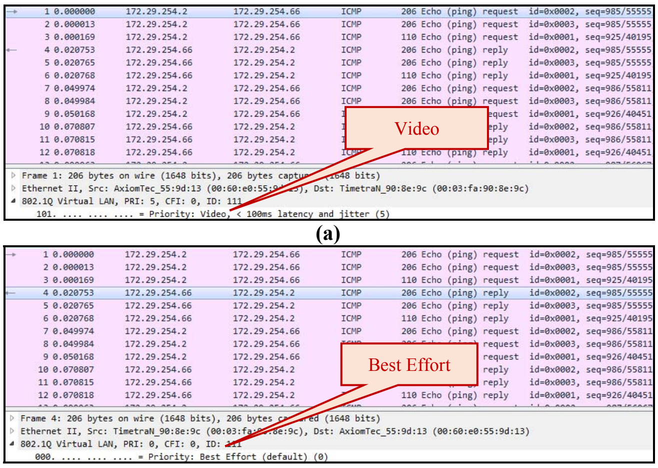
In the wireshark screenshots shown in Fig.7, it is seen that the PING test packets sent in Best Effort traffic class are also answered with Best Effort traffic class.

(a)

(b)

Fig. 7. Wireshark Screenshots according to PING Protocol with Best Effort Traffic Class a) Sent b) Received

In the wireshark screenshots shown in Fig.8, PING test packets sent in Video traffic class are also answered with Best Effort traffic class. This means that the Video packets sent are evaluated and answered with the same priority as the packets in the traffic class with data, mail and etc. regardless of the traffic class.

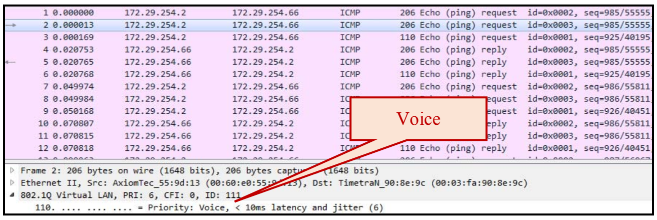


(a)

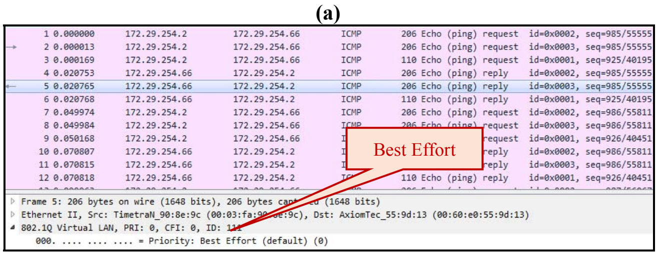
(b)

Fig. 8. Wireshark Screenshots according to PING Protocol with Video Traffic Class a) Sent b) Received

In the wireshark screenshots shown in Fig.9, PING test packets sent in Voice traffic class are also answered with Best Effort traffic class. This means that the Voice packets sent are evaluated and answered with the same priority as the packets in the traffic class with data, mail and etc. regardless of the traffic class.



(a)

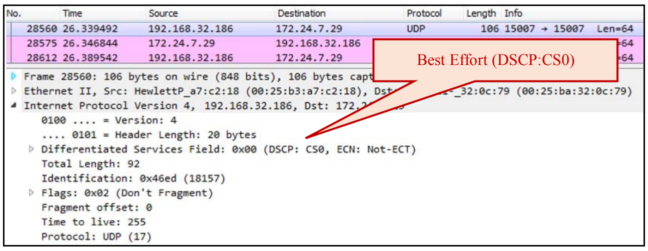


(b)

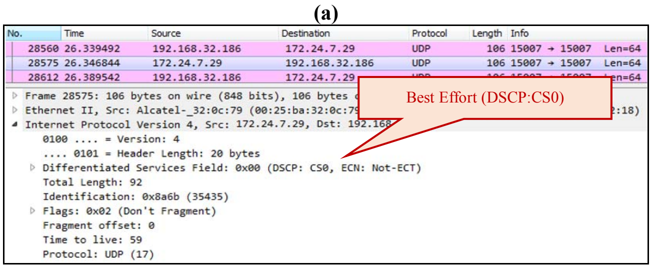
Fig. 9. Wireshark Screenshots according to PING Protocol with Voice Traffic Class a) Sent b) Received

Fig.10, Fig.11 and Fig.12 show the protocol stages of the TWAMP-Test role which is one of the subcomponents of the TWAMP protocol. In the TWAMP-Test step, it is seen that UDP ports are used for exchanging the test packets.

Details of the UDP test packets sent with Best Effort traffic class are shown in the wireshark screenshots in Fig.9. The test packet sent in Best Effort (DSCP: CS0) traffic class was also answered with the packet stamped with Best Effort (DSCP: CS0) traffic class.



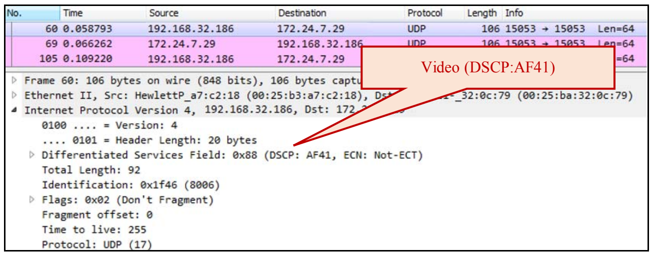
(a)



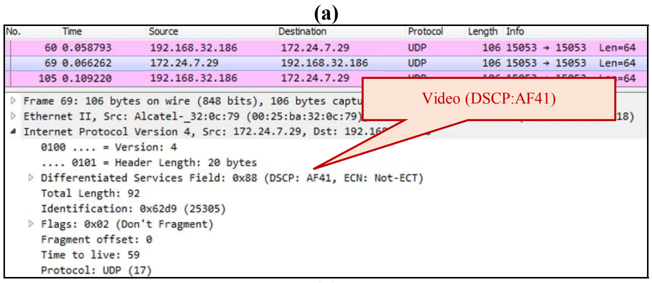
(b)

Fig. 10. Wireshark Screenshots for UDP Test Packets in TWAMP Protocol with Best Effort (DSCP:CS0) Traffic Class a) Sent b) Received

In the wireshark screenshots shown in Fig.10, details of the UDP test packets sent with Video traffic class are available. The test packet sent with Video (DSCP:AF41) traffic class was also answered with same traffic class stamped with Video (DSCP:AF41) traffic class. This indicates that, unlike the PING protocol, the TWAMP protocol is more accurate and sensitive for IP performance measurements in real-time multimedia applications.



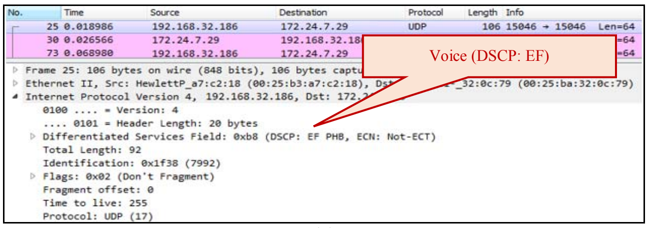
(a)



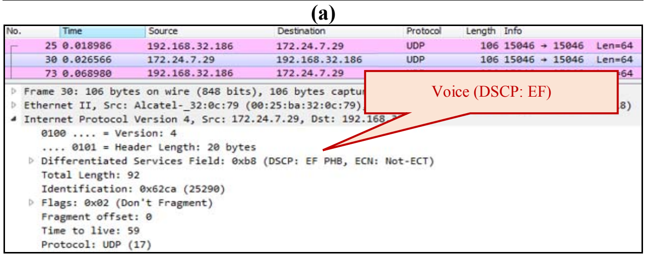
(b)

Fig. 11. Wireshark Screenshots for UDP Test Packets in TWAMP Protocol with Video (DSCP: AF41) Traffic Class a) Sent b) Received

In the wireshark screenshots shown in Fig.11, details of the UDP test packets sent with Voice traffic class are available. The test packet sent with Voice (DSCP: EF) traffic class was also answered with same traffic class stamped with Voice (DSCP: EF) traffic class. This indicates that, unlike the PING protocol, the TWAMP protocol is more accurate and sensitive for IP performance measurements in real-time multimedia applications.



(a)



(b)

Fig. 12. Wireshark Screenshots for UDP Test Packets in TWAMP Protocol with Voice (DSCP: EF) Traffic Class a) Sent b) Received

IV. RESULTS AND RECOMMENDATIONS

With the spread of applications in the IP world and the importance of performance measurements, TWAMP protocol has been widely used recently. TWAMP is the latest technology implemented to give service providers a complete visibility on the performance of their IP-based network infrastructure.

In this study, the performance values such as RTD, Jitter and Packet Loss were measured between two points in IP network according to TWAMP protocol which is one of the active measurement methods. In addition, measurements were made at the same time by using a widely used active measurement method, PING protocol, and then values were compared with TWAMP protocol. Best Effort, Video and Voice traffic classes were also taken into consideration. As a result of measurement and comparison, RTD and Jitter values are almost same for all three traffic types in all traffic classes. However, the Packet Loss value in the PING protocol is higher than the TWAMP protocol. In order to analyze and verify the results, packets details belonging to TWAMP and PING protocols were taken as Wireshark outputs. In the test runs, it is seen that the answers to the test packets sent to the other side with PING Protocol in Best Effort, Voice and Video traffic classes are Best Effort in all cases. However, the answers given to the test packets sent to the other side with TWAMP protocol in the Best Effort, Voice and Video traffic classes in is based on the traffic class being sent. This suggests that TWAMP protocol should be used in performance measurement of IP network.

It is recommended to measure the performance values of multimedia services in fixed and mobile areas using the TWAMP protocol within the framework of the test conducted and the results obtained. In particular, service quality parameters should be measured using TWAMP protocol in LTE (Long Term Evolution) technology where delay, jitter and packet loss parameters are very sensitive and important. It should be taken into consideration that the capacity values of the existing lines should be taken into account when testing scenarios are planned and the CPU and Memory values of the devices to be measured according to the standards should be observed, as well.

REFERENCES

[1] N.V Mnisi., O.J. Oyedapo and A. Kurien, “Active throughput estimation using RTT of differing ICMP packet sizes”, IEEE, 2008.

[2] K. Zaim, C. Kocak, “Performance analysis of IP network using two-way active measurement protocol (TWAMP) and comparison with ICMP (ping) protocol in a saturated condition”, 4th Int. Symp. on Innovative Technologies in Engineering and Science (ISITES-2016), Alanya-Antalya, Turkey, pp.1618-1627, ISSN: 2148-7464, 2016.

[3] H-Log QoS Telecom - White Paper, A Two-Way Active Measurement Protocol.

[4] I. Backström, ”Performans measurement of IP Network using the two-way active measurement protocol”, Master of Science Thesis Stockholm, Royal Institute of Technology, Sweden, 2009.

[5] N. Soumyalatha, R.K. Ambhati, M.R. Kounte., “Performance evaluation of IP wireless networks using two way active measurement protocol”, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013.

[6] https://wiki.wireshark.org/ (online: 01.07.2016).

[7] H. Hedayet, R. Krzanowski, A. Morton, K. Yum, J. Babiarz, “A Two-way active measurement protocol”, RFC-5357, October, 2008

[8] IETF Network Working Group, Ericsson Two-Way Active Measurement Protocol (TWAMP) Value-Added Octets, Request for Comments: 6802 (RFC-6802), November, 2012.

[9] E. Svante, E. Humlegardens, Formerly with Ericsson Research, J. Andreas and F. Christofer, Scalability, Research Area Cloud Technologies Ericsson Research, “Dimensioning of network-capacity measurement system using reflecting servers”, Sweden.

[10] IETF Network Working Group. A One-way Active Measurement Protocol (OWAMP). Request for Comments: 4656 (RFC-4656), Sep. 2006.

[11] Technology & Application Overview Whitepaper - Accedian Networks, “Automated, end-to-end carrier ethernet deployment & monitoring”, April 2009.

[12] Cisco ME 3800X and ME 3600X and ME 3600X-24CX Switch Software Configuration Guide, Chapter 70, IP SLAs TWAMP Responder, July 31, 2014.

[13] H. Saqlain, S. Harpal, “Available bandwidth measurement in 4G networks, Master of Science, Luleå University of Technology Department of Computer Science”, Electrical and Space Engineering, Luleå, Sweden, 2013.

[14] R. M. Ganapathy, “A tool for measuring available network bandwidth in the cloud”, Master’s Degree Project, Stockholm, Sweden, September 24, 2015.

[15] L. Thomas, “A new approach to performance monitoring in IP networks – combining active and passive methods”, KTH IMIT and Ki Consulting, 136 40 Haninge, Sweden.

[16] H.J. Lee, M.S. Kim, J.W. Hong, G.H. Lee, “QoS parameters to network performance metrics mapping for SLA Monitoring”, 2002.

[17] V. Mohan, Y.R.J. Reddy, K. Kalpana, “Active and passive network measurements: A Survey”, Venkat Mohan et al,/(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1372-1385, 2011.

[18] IETF Network Working Group. Internet Control Message Protocol, Request for Comments: 792 (RFC-792), September, 1981.

[19] P. Skurowski, R. W’ojcicki, Z. Jerzak, “Evaluation of IP transmission jitter estimators using one-way active measurement protocol (OWAMP)”, Communication in Computer and Information Science, June 2010.

[20] IETF Network Working Group. Internet Protocol, Request for Comments: 791 (RFC-791), September, 1981.

[21] 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.

[22] CISCO, Cisco Nexus 1000V Quality of Service Configuration Guide, Chapter 6, DSCP and Presedence Values, Release 4.