SNMP Performance Measurements Using Open Source Software

Evangelos Logaras, Vassilios Voutsas, Christos Kaitatzis, Sotirios K.Goudos and Christos F. Kalialakis
Radiocommunications Laboratory, Physics Department,
Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece
elogaras@physics.auth.gr

***Abstract*— SNMP (Simple Network Management Protocol) is widely used in the network management of IP networks. The contributions of this work are twofold. First, a setup for SNMP performance measurements is introduced using an open source software approach. In the proposed implementation, the Net-SNMP and Wireshark software tools have been utilized. Measurements for several SNMP commands have been carried out in a wired and a wireless indoor environment. Secondly, the setup can be readily introduced as a laboratory exercise that can help students to understand SNMP in an engaging way.**

Keywords—SNMP; Open Source Software; Network Management; Laboratory training

I. INTRODUCTION

Network Management Systems (NMS) are fundamental in the operation of today's complex networks. There are two trends for NMS implementation; company offered systems vs. open software. In this work, open source software components are used which are most suitable for experimentation and academic research. This is also in line with recent research approaches for NMS in general [1].

The domination of the TCP/IP stack followed the Internet growth and the gradual transformation of wireless network systems into IP with the introduction of the IMS (IP Multimedia Subsystem) [2]. IMS testbeds have been implemented using open software components [3]-[4]. The open source approach can also be utilized as a practical educational aid for courses on network management [5].

SNMP is the network management protocol of choice for IP networks. SNMP has evolved from version 1 to the current version 3 which is backward compatible. Version 3 has stronger security characteristics using authentication [6]. Secure Socket Shell (SSH) is also a popular security enhancement that can be used with SNMP [7].

Actual measurements studies on the performance of SNMP [8] are relatively few in comparison. In principle, the performance can be measured in three levels; packet, kernel and application [9]. For performance measurements at the packet level, some kind of protocol packet observation is required. Such observation is feasible with packet sniffers as explained in Section II. In Section III indicative results are given that compare SNMP performance for different versions.

II. MEASUREMENT SETUP

The measurement setup is shown in Fig.1.

The SNMP manager and agents are implemented using Net-SNMP [10]. The required packet sniffing is performed on a separate machine using the Wireshark software [11]. The Wireshark software has an inherent capability to filter SNMP traffic.

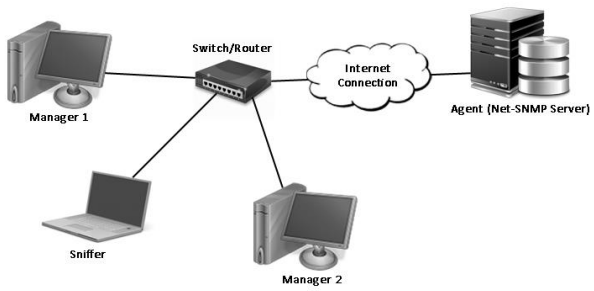

Fig. 1 Setup for SNMP performance measurement

SNMP operates in a client-server fashion. The use of Net-SNMP server simplifies the setup but other standalone SNMP servers can be also used. Two protocol modes of operation are included in SNMP; the request/response mode and the traps mechanism. The request/response commands were used in this work. As a performance metric, response delays have been chosen [9].

III. RESULTS

SNMP commands have been sent across the network and responses were collected. Several scenarios have been tried in both wired and Wi-Fi environments. The performance of the same command in different SNMP versions (v.2, v.3) has been investigated. Repeated transmissions are used in order to establish reasonable statistics. No significant differences were observed in the case of capacity variation. This is due to the small size of SNMP commands (see Table I). The sizes in Table I were measured with Wireshark.

TABLE I. SNMP COMMANDS TESTED

Ref.	*Command Name*	*Manager to Agent (Size in Bytes)*	*Agent Response (Size in Bytes)*
1	get(v.2)	87	91
2	get(v.3 auth)	273	333
3	getnext(v.2)	87	142
4	getnext(v.3 auth)	272	333
5	bulkget(v.2)	87	391
6	bulkget(v.3 auth)	272	602
7	walk(v.2)	174	233
8	walk(v.3 auth)	443	560
9	bulkwalk(v.2)	174	482

Considerable differences in response were found under different traffic scenarios. Ping times are utilized as a crude metric of traffic load. Response times are measured via Wireshark. Results are shown for request/response type commands in Fig.2-Fig.5. It can be seen that the authentication feature in version 3 carries a significant time response penalty; almost double the time compared to the no authenticated version 2. Similar conclusions were reached in [12].

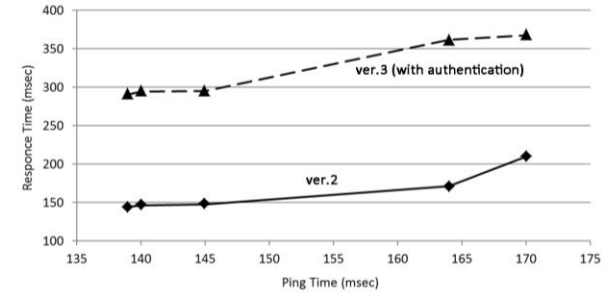

Fig. 2 Performance of command `get` in v.2 and v.3 for different traffic scenarios indicated by ping times.

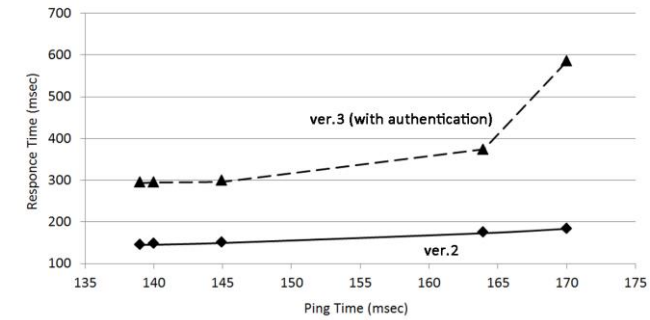

Fig. 3 Performance of command `getnext` in v.2 and v.3 for different traffic scenarios indicated by ping times.

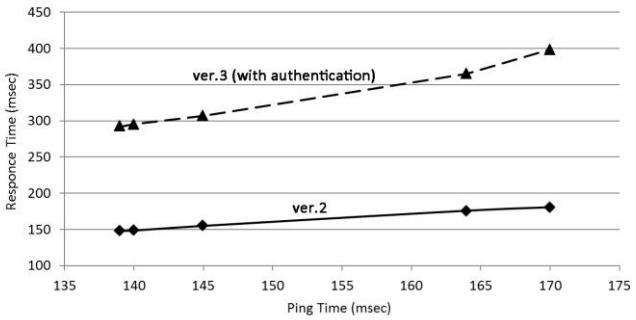

Fig. 4 Performance of command `bulkget` in v.2 and v.3 for different traffic scenarios indicated by ping times.

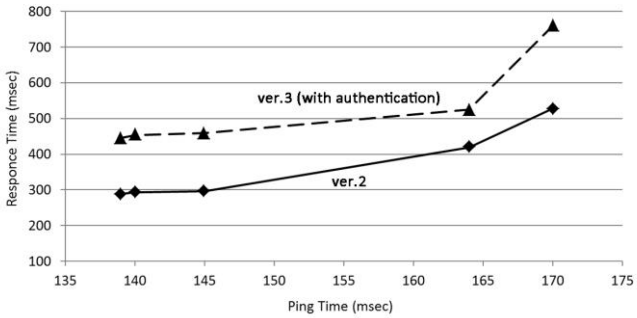

Fig. 5 Performance of command `walk` in v.2 and v.3 for different traffic scenarios indicated by ping times.

IV. CONCLUSIONS

A setup for performance measurements has been presented using open source software (Net-SNMP and Wireshark). The response delay was utilized as a metric. Several request/response commands were tested in a variety of network traffic conditions. It was found that the authentication mechanism in version 3 introduces almost double response time compared to version 2. The setup is scalable and can be readily used as laboratory exercise in a network management course.

REFERENCES

[1] OpenNMS, *The Open Network Management Systems Project*, online at www.opennms.org.

[2] Camarillo, G. and Garcia-Martin, M.A.. *The 3G IP multimedia subsystem: merging the Internet and the cellular worlds*. John Wiley & Sons, 2007.

[3] Segeč, P. and Kovacikova, T. "Implementation of IMS testbeds using open source platforms", *Communications*, 14(2):55-62, 2012

[4] Ling, X. "The Research and Design of IMS Network Management", *Intelligence Computation and Evolutionary Computation*, pp.813-818, Springer Berlin Heidelberg, 2013

[5] Hernandez-Leo, D. ,Bote-Lorenzo, M.L. ,Asensio-Perez, J.I.; Gomez-Sanchez, E.; Villasclaras-Fernandez, E.D.; Jorrin-Abellan, I.M.; Dimitriadis, Y.A., "Free- and Open-Source Software for a Course on Network Management: Authoring and Enactment of Scripts Based on Collaborative Learning Strategies," , *IEEE Transactions on Education*, vol.50, no.4, pp.292-301, Nov. 2007

[6] RFC 3584, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework", Internet Society, 2003.

[7] Marinov, V., and Schönwälder, J., "Performance Analysis of SNMP over SSH." *Large Scale Management of Distributed Systems. Springer Berlin Heidelberg*, 2006, pp. 25-36.

[8] Andrey, L. *et al*. "Survey of SNMP performance analysis studies", *International Journal of Network Management*, 19(6), pp.527-548, 2009.

[9] L.Abdelkader, L.Andrey, and O.Festor. "On delays in management frameworks: Metrics, models and analysis." *Large Scale Management of Distributed Systems*, pp.13-24. Springer Berlin Heidelberg, 2006.

[10] Net-SNMP, Current Release 5.7.2.1, available online at http://www.net-snmp.org).

[11] Wireshark, Stable Release 1.12.3, available online at https://www.wireshark.org.

[12] Corrente, A. and Tura, L., "Security performance analysis of SNMPv3 with respect to SNMPv2c," IEEE/IFIP Network Operations and Management Symposium, 2004. NOMS 2004., vol.1, no., pp.729,742 Vol.1, 23-23 April 2004.