Semiconductor Optoelectronics
ISSN: 1001-5868

DESIGN AND IMPLEMENTATION OF NETWORK PERFORMANCE MANAGEMENT SERVER USING SMART SCALABLE SNMP

Rajaram Jatothu
Department of Computer Science and Engineering, Pallavi Engineering College, Hyderabad, Telangana, India. Email id: drjrajaram81@gmail.com

Nethravathi PS
Associate Dean, Institute of Engineering and Technology, Srinivas University , Surathkal, Mangalore, India. Email: nethrakumar590@gmail.com

ABSTRACT: Due to the development of several kinds of gadgets in today's digital era leads to traffic growth and increases the number of internet services over the network. The efforts have been made since decades for making a Simple Network Management Protocol mostly called as SNMP. The network management plays a vital role in improving the network unit utilization ratio, troubleshooting fault and optimizing the performance of network, positioning, ensuring network service quality and security. This paper provides design and implementation of Network Performance Management server using smart and scalable SNMP. Firstly a smart and scalable SNMP is designed that has a hierarchical and decentralized paradigm. The objective of testing this presented approach isdetermining the devices availability. Experiments are conducted repeatedly for computing the time of processing. The processing time will be controlled under a moderate amount due to inclusion of sub-NMS (Network Management Station) cluster. The results exhibit that the framework has better performance in scalability and timeliness.

KEYWORDS: TCP traffic, SNMP (Simple Network Management Protocol), Network management, scalability and availability.

I. INTRODUCTION

During vehicle test the test IP network undertaking the information interactions between the command center and remote measurement equipments [1]. Due to most complex vehicle test the test IP network required to be managed the nodes and the data is much larger and network system stability and security is very high and real-time requirement. For determining the availability of services, conditions of network, downtime and uptime maximum monitoring system is utilized [1]. One of the Management system functions is network monitoring that can be useful for analyzing either network is possibly sufficient for usage or extra capacity is required. Today the SNMP is utilized as a management protocol by huge majority of legacy networks [2]. The first version of SNMP was introduced in 90's (RFC 1157), after that its adoption has been growing. The SNMP contains SNMP manager or NMS (Network Management Station). The network conditions like down or up status of monitoring network

device should be monitored instead of traffic load of network [3]. Simplicity and stateless nature is the major advantages of SNMP. The information about management is stored in MIBs (Management Information Bases) [4] and its elements can be identified through standardized OIDs (Object identifiers) [5]. The manager of SNMP polls the agents at monitored devices through OIDs and obtains required values (for example via a switch interface given). The SNMP utilizes User Defined Protocol (UDP) as an underlying protocol for sending the queries and receives relevant replies that are also stateless; hence simplicity is also provided at transport layer. The SNP management station (server process) and SNMP station (client process) are adopted by SNMP protocol for realizing the asynchronous response and request and for monitoring the equipments of network. Installation of SNMP proxy stations on each network node is its basic principle for collecting the corresponding data which can be collected through the process of management on servers by SNMP protocol. This SNMP protocol contains four parts: network management protocol, MIBs, Management station (MS) and proxy station.

SNMP is working based on the working agent/end management approach; the computer which is running the NMS is basically a network management work station [6]. The agent is a process which works over a management station and network device for getting the working status of network equipment and performance via inquires of agencies. The agent can be responsible to handle and respond to the requests from MS and reports the main events to MS. The MS will receive the trap message send from agent. The trap message is a message transmitted to management end from the agents who has vital relations among network states and local. First the management system analyzes the information from Trap dataand then events will judged and will monitor the network interface working status for achieving communication linemonitoring network in real-time that will implementing the understanding the line status purpose in real time. The networking management system monitors the devicesthat enable SNMP protocol which is a central nervous system in the entire network and here expert databases are saved [7]. Firstly the SNMP works in centralized way that can't assure scalability and timeliness. The real SNMP paradigm contains one "manager" is there and is known as NMS and several managed devices (includes switches, routers and modems). Only modest number of devices is available in LAN (Local Area Network) and centralized SNMP works fine in case of managing the classical network components. If the managed network scale grows (usually this is in IoT, because of wide spreading transducer nodes) then the sequential responses/requests processing time can be unbearable and centralized technique fails. Secondly the actual SNMP is not smart enough [8]. The SNMP lacks potential to the analysis of data because of its simple structure. Only thing that it does is reporting the collecting data mechanically as what they are, and highest level of data is not extracted.To address these issues, a smart and scalable SNMP will be designed. A hierarchical and decentralized paradigm to new SNMP will be devised for achieving scalability and timeliness. The remaining of this work is organized as:Literature survey is introduced in Section II. Section III includes architecture and implementation process of described method. Section IV includes the results analysis and eventually section V concludes the research.

II. LITERATURE SURVEY

Paulo Roberto da Paz Ferraz Santos et. al. [9] evaluated NETCONF(Network Configuration)

Protocol, SNMP and RWS (RESTful Web Services) for virtualization Management of Router. For achieving high scalability, management interoperability and good performance they developed, demonstrated and compared to other management interfaces to the physical routers which host the virtual ones. The obtained results demonstrated that the Simple Network Management Protocol (SNMP)interface is suitable to smallerNetwork Virtual *Interface (NVE)*with no strict security necessaries and NETCONF is the good selection for composing a management interface for deploying in many realistic cases in which major concerns are scalability and security. Rendon et al. [10] described a model that allows any Administrator of Virtual Infrastructure for adoption, customization and combining the previous monitoring tool to enhance network monitoring and system tasks in virtualized fields. They utilized RWS for developing the Virtual Node Wrappers. While this work has presented an extensible and flexible system and is mainly focused over monitoring and won't support Virtual Nodes configuration (e.g., creation of VR). Arman Roohi et. al. [11] presented a real-time monitoring technique for dynamic data for reducing the cost and complexity basing on the management of network. In this approach a SNMP protocol is utilized for collecting the data to initiate the interactions between specific data center and equipment. An WBEM (Web Based Enterprise Management) is desirable for transferring the protocols such as SNMP and to manually enter the original data for later authenticity with real time data. Hopefully this work encourages the companies to try alternative solution for the issues while managing the equipments in data center.

Han Yan et. al. [12] discussed the study over

Topology discovery algorithm of network based on SNMP and ICMP (*Internet Control Message Protocol*)protocols that utilize single visual tool for data visualization. Air and 3D technology has been utilized widely due to development of graphic processing technologyandWeb technology. However the network topology visualization point should includes many functions of modern network management for truly realizing the research technology value.Daitx et al. [13] has presented a network virtualization management interface basing on SNMP, extended the VRMIB module for allowing the binding of flexible interface. Certain common management operations are utilized for evaluating the presented interface performance of virtualization platforms includes VMWare and XenServer. Further they demonstrated that the performance of SNMP largely dependent on virtualization domain and other management protocols are not investigated. They utilized Virtual Reality Management Information Bases (VR-MIB) as a data model. Jürgen Schönwälder et. al. [14] described how security protocols are above transport layer and below application protocols are utilized for securing SNMP. These protocols take the merits of previously implementedvital management architectures which can be utilized in other network managements. The major contribution can be a detailed prototype implementation performance analysis, compared the SNMPv3 performance over DTLS (Datagram Transport Layer Security), TLS(*Transport Layer Security*), Secure Shell Protocol (*SSH*) with other SNMP versions. In addition the differences among several options are discussed for securing the SNMP and providing guidelines to choose solutions for implementing or deploying. You-Sun Hwang et. al. [15] presented a model that contains a SNMP agent, BS (Base Station) manager and GUI (Graphic User Interface). TheSNMP agent to Manger communicates through a model basing extensible Trap feature of SNMP. The agents of SNMP are utilized for managing the Broadband Wireless Access (BWA)

network elements and communicate with the manager of BS through SNMPProtocol Data unit (PDU). The fault management and configuration management functions are provided by the BS manager.

III. DESIGN OF NETWORK PERFORMANCE MANAGEMENT USING SMART SCALABLE SNMP

The work flow of implementation of Network Performance Management server using smart and scalable SNMP is represented in below Fig. 1.

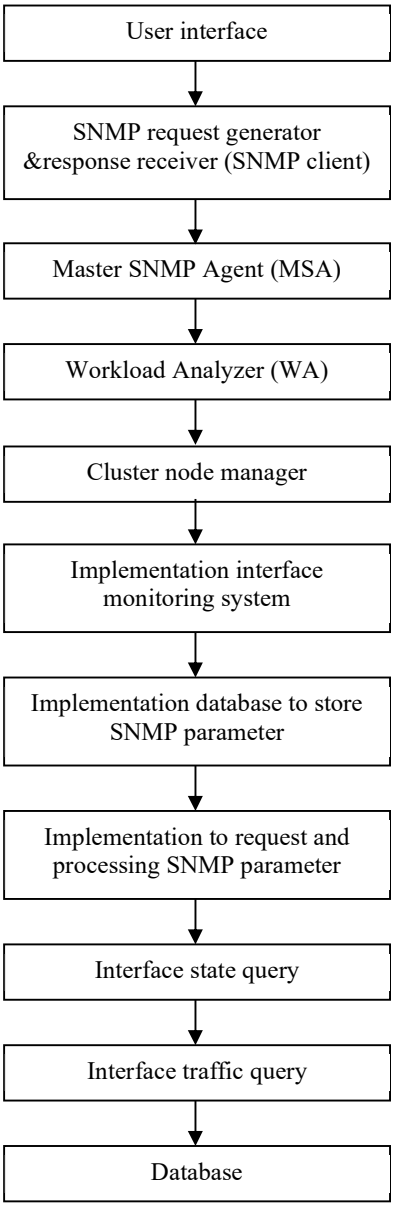


Fig. 1: WORKFLOW OF NETWORK PERFORMANCE MANAGEMENT USING SMART AND SCALABLE SNMP

The network management has the ability of monitoring, controlling and planning the components and resources of computer networks and systems. Various kinds of network

managements are security management, accounting, configuration management and fault management. Decentralized and hierarchical paradigm will be devised for new SNMP that contains 3 layers: managed devices, sub-NMS cluster and central NMS.
The presented central NMS is the topmost layer, with this the administrators interacts directly.Central NMS includes the processing steps as SNMP request generator, Master SNMP Agent (MSA), Workload Analyzer (WA) and cluster coordinator. The central node is placed to be compatible with earlier architectures and the internal functions redesigned thoroughly. A user interface is provided to administrators by central NMS for sending the requests, receiving the responses and to make decisions manually. The administrators will send the requests of SNMP through the user interface and in the same manner they manage the networks ofTransfer Control Protocol/ Internet Protocol (TCP/IP). The results will provided based on utilized algorithm that can be pre-defined in MIB files.

Cluster node manager and SNMP client are contained with sub-NMS. An SNMP client is there for every sub-NMS and is responsible to undergoing interactions includes sending the SNMP requests and receiving the responses of SNMP. Thus the timeliness and scalability can be ensured in terms of communication. Hence this architecture is allowed for performing the distributed big data analysis.

First the administrators sent an 'SNMP GET' request while calling the SNMP client's Application Programming Interface (API) through user interface. The OID is a request message fields that specifies that which content is requested and indicates which algorithm is to be utilized. Then the message is resolved locally through MSA (Master SNMP agent) and analyzed through WA (Workload Analyzer). The WA will split the job of GET into smaller piece of tasks and optimal places (i.e. over which sub-NMS) will be determined for conducting the underlying interactions. Rather, it can search through the algorithms which are available and identifies which is to be utilized. All options and generated commands are sent to CC (Cluster Coordinator), assign a few subsets of task pieces to one who interacts with cluster node manager.

After that the sub-NMSs initiates the underlying interactions with smart transducer networks utilizing common SNMP and collection of data from the regions which are distributed geographically. The implementation of interfaces and polling modules will be performed through open NMS Cacti version 0.8.8b through version 1.8.3 XAMP (cross-platform, Apache, MySQL, PHP and Perl) database contains phpMyAdmin 1.4.12 and PHP 55.11 Apache 2.4.9. The aim of web interface implementation is displaying the monitoring results process if already performed or being performed. All these modules implementations are aiming for finding the agents which are attached between the manager, relation between traffic conditions and agent in graph form in real time. If the process of polling occurs then the based agent who is already appears over the list, the conditions of traffic over the interface can be stored in database. Therefore the network conditions between agents will be plotted over the network map which is made earlier.

In interface state query module, it is required to be initialize the Winsock, SNMP and constructs

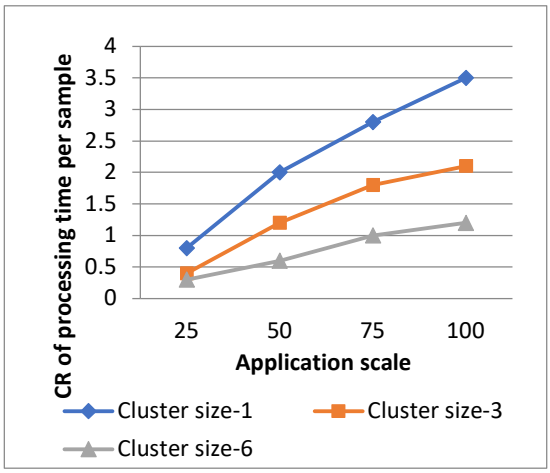
the object of UDP and SNMPaddress. This work will be completed by the function GetPort(CString &ip, CString &community, CString &OID_port). The query of interface traffic will be implemented through SNMP class function like GetNext() function. The result of query can be stored in variable form that is a CStringArray kind variable.

As the interface state and traffic query are completed then the real-time monitored data will transmitted to database as a historical data part. Based on historical data analysis the fault state is divided into various categories for test IP network. Mostly, the job of GET has been completed. While in autonomous system, it can be expected further that the architecture of management is able for acting on the extracted data. As a consequence the manager of the network will find and judges the faults of network in real time and network is maintained in time.

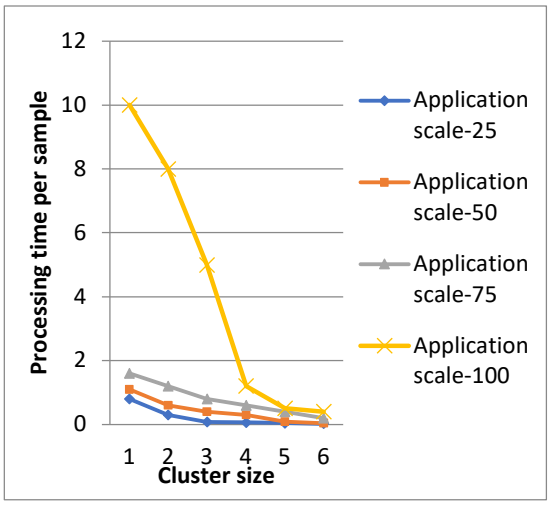
IV. RESULT ANALYSIS

The monitoring system implementation is performed for examining the success levels of function interface and web interface for operating the monitoring system. First the username and password must be entered by the user as an admin. The application will be executed after the successful completion of login process. The first process that should add devices is monitored with the SNMP feature of IP device can be activated thus polling process will be executed for every 5 minutes. As the polling process is going, the agent of SNMP would request the whole information which is monitored through earlier OID,the MIB of every agent and stores the data for database manger which can be shown in admin web monitoring and mapping system of network.All the agents will monitor the interfaces, bandwidth optimization model is applying for observing that which agent utilizes the traffic of UDP and TCP (Transmission Control Protocol) with higher bandwidths. Hence with this data the administrators will find the appropriate bandwidth allocation to each network.

The architecture performance is evaluated in terms of scalability and timeliness. For making the differences more evident the experiments are conducted on much time consumingidentification of job-anomaly, where time of processing is selected as a criteria for evaluation. Size of the cluster (i.e number of sun-NMS) and application scale are two adjustable parameters. If cluster size is set to 1 then the architecture will be considered as classical approximation, centralized architecture and these cases result can be utilized as baseline. Experiments are conducted repeatedly for computing the time of processing and average time consumed per sample is calculated. The results of two perspectives are represented in Fig. 2(a) and 2(b).



(a)



(b)

Fig. 2: AVERAGE PROCESSING TIME PER SAMPLE: (a) CUBE ROOT OF TIME VERSUS APPLICATION SCALE, (b) TIME VERSUS SUB-NMS CLUSTER SIZE

In Fig. 2 (a) the vertical axis represents the processing time CB (Cube Root)($S^{1/3}$) and concluded that the identification of anomaly has cubic complexity with respect to application scale that is unbearable if the monitored application growth is beyond certain scale. This issue is alleviated greatly through the decentralized architecture. From the Fig. 2(b) due to sub-NMS introduction the time ofprocessing will be controlled to moderate value. The obtained results demonstrated that the presented frameworkhas better performance compared to classical architecture in terms of scalability and timeliness.

V. CONCLUSION

In this paper, design and implementation of Network Performance Management server using smart and scalable SNMP is described. In network management the SNMP application is studied deeply andthe test IP network characteristics are analyzed. A test IP (Internet Protocol) network monitoring system is designed based on data base technology and SNMP. It plays a

vital role in network management, includes improving network elements utilization. The SNMP protocol works by requesting the parametervalue basing on OID that will perform it functions. The raw text data is produced by monitoring SNMP, will made the web interfaces much simpler for analysis results. Experiments are performed repeatedly for computing the time of processing. The processing time is controlled to a moderate value due to sub-NMS cluster introduction. The SNMP protocol is utilized for system monitoring that can provide optimal results and is utilized for monitoring the network device which can support SNMP. This work shows a promising direction to big data management. The system is provided to complex network operation real time monitoring meant for network management by the administrator of system discovered the network issues. The results demonstrated that the presented framework has better performance compared to classical architectures in terms of scalability and timeliness.

VI. REFERENCES

[1]Lixia Zhang, Yang Li, Bijie Qiu, Jianliang Zhang, Weiwei Liang, "Design of communication power centralized remote monitoring system based on big data technology", 2021 International Conference on Electronics, Circuits and Information Engineering (ECIE), Year: 2021

[2]Oliver Jukić, Ivan Heđi, Antonio Šarabok, "Fault management API for SNMP agents", 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Year: 2019

[3]Martin Kontšek, Pavel Segeč, Marek Moravčík, Jozef Papán, "Approaches and tools for network protocol modeling", 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), Year: 2019

[4]Muhammad Zeeshan, Mohammad Ziad Siddiqui, Farrukh Bin Rashid, "Design and Testing of SNMP/MIB based IoT Control API", 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Year: 2019

[5]Duo Ding, Minbo Li, Zhu Zhu, "Object Naming Service Supporting Heterogeneous Object Code Identification for IoT System", 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Volume: 01, Year: 2018

[6]Khamdamboy Urunov, Soo-Young Shin, Soo-Hyun Park, "The unique reliable identity system of enabling lightweight device management in NMS mechanism for the U-IoT", 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Year: 2017

[7]Rajaram Jatothu, G. Narasimha, "Enhancement in SNMP services with improved security with the impact of SSH, TLS and DTLS Protocols", 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Year: 2017

[8]Young-Il Kim, So-Jeong Park, Nam-Jun Jung, Moon-Suk Choi, Byung-Seok Park, "Design and implementation of NMS using SNMP for AMI network device monitoring", 2016 IEEE International Conference on Power System Technology (POWERCON), Year: 2016

[9] Paulo Roberto da Paz Ferraz Santos, Rafael Pereira Esteves, Lisandro Zambenedetti Granville, "Evaluating SNMP, NETCONF, and RESTful web services for router virtualization management", 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Year: 2015

[10] O. M. C. Rendon, C. R. P. dos Santos, A. S. Jacobs, and L. Z. Granville, "Monitoring

virtual nodes using mashups," Computer Networks, vol. 64, no. 0, pp. 55 – 70, 2014.
[11] Arman Roohi, Khashayar Raeisifard, Suhaimi Ibrahim, "An application for management and monitoring the data centers based on SNMP", 2014 IEEE Student Conference on Research and Development, Year: 2014
[12] Han Yan, "The study on network topology discovery algorithm based on SNMP protocol and ICMP pr otocol", 2012 IEEE International Conference on Computer Science and Automation Engineering, Year: 2012
[13] F. Daitx, R. Esteves, and L. Granville, "On the use of SNMP as a management interface for virtual networks," in Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on, 2011, pp. 177–184 [Online] Available: http://dx.doi.org/10.1109/INM.2011, 5990689
[14] Jürgen Schönwälder, Vladislav Marinov, "On the Impact of Security Protocols on the Performance of SNMP", IEEE Transactions on Network and Service Management, Volume: 8, Issue: 1, Year: 2011
[15] You-Sun Hwang, Eung-Bae Kim, "The management of the broadband wireless access system with SNMP", 10th International Conference on Telecommunications, 2003. ICT 2003, Year: 2003.