ID 527

Network Infrastructure Monitoring Tool for Small and Medium Scale Enterprises

HPAI Pathirana#, VB Godagama, HKSH Premadasa and RLW Koggalage

University of Vocational Technology, Sri Lanka

#asanka.pathirana@gmail.com

Abstract— Modern SMEs utilize some form of computer network to accommodate both internal employees and external customers. Hence, managing the network infrastructure is crucial for SMEs. Network infrastructure monitoring is utterly important for network management, to attend to any critical situation as preventive measures for corrections. Eventually, a hassle-free network is introduced, assuring 24x7 availability. As a result, some form of a network infrastructure monitoring tool (NIMT) is an essential element for SMEs, despite the fact that commercially available high-end NIMTs are not affordable in any situation. On the other hand, many SMEs do not consider incorporating an NIMT with priority, since they can still survive with the primary business process, although there are significant interruptions of the network infrastructure. Nevertheless, the involvement of ICT experts is essential on either a full-time or part-time basis to operate high-end NIMT, due to the complexity to deploy and maintain it. As a result, "How to introduce comprehensive, user-friendly, affordable and maintainable NIMT for SMEs?" is the research question. In our methodology, the literature is evaluated for understanding the unique requirements of network management, and the available NIMTs are analysed under eight specific functionalities. Subsequently the design is finalized, focusing on the requirements of SMEs and the system development is based on python, whereas the operating system is Linux. More importantly, the user interface is based on PHP, while the database is on MariaDB. This all-in-one NIMT solution can be used by anyone for essential network analysis. Moreover, SMEs shall benefit from this solution in an effective manner, with neither extra software license cost nor the involvement of ICT experts.

Keywords: utilising network, network monitoring, all-in-one

I. INTRODUCTION

In the present day industry, the network management is crucial, and this include provisioning, maintaining, administrating and operation of the network infrastructure. The network management ensures resources in the network are available for users in an efficient and effective manner improving the quality of service. As the name implies, the NIMTs monitor network traffic and workstation/server performance. Moreover, those are not an all-in-one solution, so the user has to get add-on platforms, such as OS, DBMS software, web server software, hardware, etc., to effectively implement the platform for NIMTs, and it discourages users to adopt the NIMTs at the SMEs. Further, there is an extra cost with such add-on platforms, and it is further discouraged. Nevertheless, those add-on platforms must be deployed in a dedicated physical infrastructure (desktop or server) for installation and configuration on software-based NIMTs. Moreover, it is essential to have a knowledgeable person to install, configure and maintain such a system in a company, otherwise it is essential to recruit someone considering the long-run requirement. Due to those essential extra expenses, the use of NIMT is not motivated, and this has been identified as the background for the research problem of "How to introduce comprehensive, user-friendly, affordable and maintainable NIMT for SMEs?"

With the growing demand to adopt IT into the business everywhere, workstations, laptops, and servers are used by many organizations. Eventually, businesses highly rely on those devices, and the availability of them to access those devices is essential for smooth operations. However, the slowness and breakdowns situations of network infrastructure are

interrupted on the smooth operation of the business process of SMEs. Therefore preventive and corrective maintenance and resource management are highly important. For network infrastructure maintenance and resource management, monitoring network infrastructure in real-time is the best way to maintain infrastructure uptime at the required level. Eventually, this indirectly influences positively on productivity and profit of the SME. The proposed NIMT is not only a software solution to monitor the network infrastructure but it comprises the relevant hardware infrastructure as an all-in-one solution. The following objectives are achieved in the project as the solution for the research problem.

i. To provide an all-in-one solution catering to the basic requirement for network infrastructure monitoring.
ii. To improve the efficiency and effectiveness of the network infrastructure in SMEs.
iii. To assure the utilization of the available hardware.
iv. To reduce the cost of network infrastructure management for SMEs.
v. To develop an affordable network infrastructure monitoring solution for SMEs.
vi. To improve the business process of the SMEs indirectly.

II. BACKGROUND

The background of the solution focuses on evaluating the purpose of the network monitoring tool, and the sources for the literature are from peer-reviewed journals. Nevertheless, the available similar products in the market are also evaluated next as per Table 1 for a clear understanding of the requirement to have an affordable device to cater to the requirements of SMEs.

A. Literature Review

Managing network infrastructure is a critical process of modern IT-related enterprises (Ferraiolo, Kuhn, and Hu, 2008; Liu, 2021; Jovanovic, Markovic, Popovic, and Jovanovic, 2010; Verma, 2002), and this includes provisioning, administrating, operating, and maintaining of the network. Further, network infrastructure management ensures resources in the network are available to users in an efficient manner and consumed efficiently by users (Ferraiolo, Kuhn, and Hu, 2008). Eventually, proper management of network resource increase quality of service.

Network provisioning involves providing equipment, services, or software to employees or ICT professionals (Ferraiolo, Kuhn, and Hu, 2008). Once the authenticated user requests for different services/resources, then authorization is taken place to grant relevant privileges, so the access control is managed effectively by considering the assigned privileges through the automated process to control the operations towards specific resource requirement(s).

Network administrating carries out a wide range of operational tasks that ensure smooth and efficient performance of an enterprise network (Verma, 2002), and policy-based initiatives are encouraged for network management to simplify the complexity of dealing with multiple users. The absence of a minimum level of network administration is always problematic for the smooth operation of the network environment for anyone other than operating smaller networks.

Network operation focusing on the hassle-free best functionality of the network (Svoboda, Ghafir, and Prenosil, 2015), and monitoring the network, pre-emptively identifying and solving the issues are main tasks. Among them, monitoring the network is a significant component for network operation for having proactive measures for remedial actions, otherwise, it is not guaranteed to comply with 24x7 service requirements.

Network maintenance mainly includes corrective and preventive maintenance to adopt the evolvement of the technologies adequately (Liu, 2021), so updates and bug fixes to device software, and reviews of security policies are important to incorporate within the scope of the corrective maintenance. Even intermediate devices such as L2-switches, L3-switches, and routers should be upgraded in a timely manner to assure the smooth functioning of the network.

B. Evaluation of Tools

Among the available similar tools, few tools are considered based on purposive sampling to evaluate as in Table 1 focusing the specific requirements of the SMEs, and relevant product specifications are used for this analysis over the 8 different factors listed below.

1) Hardware Utilization Monitoring: hardware utilization is utterly important to observe over 24x7 otherwise the availability of the servers/services can be interrupted. Addressing such a situation all the following tools have been provided some way of communication with network administrator/team via email, text, a dashboard in the industry.

2) Network Utilization Monitoring(NUM): NUM is also important for the medium and large-scale industries where complex networking infrastructures are available. However, SMEs are not comprised of such networking infrastructures. As a result, the comprehensive NUM is not essential for SMEs by considering the requirement, despite there is average use of NUM in some situations.

3) Internal Session Detail Monitoring(ISDM): The number of connections that each computer maintains with some other computer can be captured through this feature with the details of the sessions. It is useful for recognizing the suspicious computer which is having an unpredictable connection with either internal or external device(s) because it can be due to internal/external threats. This feature is available by default only with the first option, and it is not affordable for SMEs.

4) Alerting and Reporting: This is the primary option for any monitoring tool having prompt notification in the pre-defined critical situation via email, text, mobile app, and dashboard, etc. In SMEs, at least the minimum level of these features should be incorporated to assure prompt responses due to any situation.

5) Device Discovering: The availability of the nodes of the networks are captured via SNMP or client application focusing the traffic towards the well-known ports such as HTTP, SSH, SMTP, DNS, ICMP, etc. However, it is not comprised as a basic feature for some cases, whereas it is possible to incorporate it through additional services.

6) Additional License Software Required: The basic version is not adequated in many cases to deploy the monitoring tools due to the requirement of the supplementary operating systems or application software. With that, it is further difficult to afford for SMEs.

7) Price: The NIMT is usually expensive aline with the available features. Although it is not considered with priority by SMEs due to the non-value addition for their business process SMEs should consider adopting some form of NIMT by considering uninterrupted networking facilities to streamline business processes.

8) Hardware: Almost all of the NIMTs are software-based implementation and it is required to adopt hardware to deploy NIMT which is not practical in SMEs because there is no strong technical workforce in most of the cases.

Table 1: Evolution of Available Tools

Option of the tool	Solar Winds Network Performance Monitor	Paessler PRTG Network Monitor	Manage Engine OpManager	Zabbix	Nagios XI
Hardware Utilization Monitoring	Yes	Yes	Yes	Yes	Yes
Network Utilization Monitoring	Yes	Yes	Yes	Yes	Yes
Internal Session Detail Monitoring	Yes	No	No	No	No
Alerting and Reporting	Yes	Yes	Yes	Yes	Yes
Device Discovering	Yes	Yes	Yes	No	Yes

Additional License Software Required	Yes	Yes	Yes	No	No
Price (USD)	2,675	1600	16,495	0	1,995
Hardware	No	No	No	No	No

III. METHODOLOGY AND EXPERIMENT DESIGN

A. Methodolgy

In this research, relevant literature is considered under the requirement gathering, and the present-day related tools are evaluated for catering to the requirement of the SMEs. As a result, the main factors to monitor for evaluating the exact requirement to develop NIMT are identified as details of an enterprise network infrastructure, hardware system requirements, and software requirements.

Then, the design is introduced as a block diagram incorporating the required elements as the initial phase, and that is revised accordingly throughout the development phase. The coding is mainly based on Python and there is comprehensive testing based on identified test cases before the deployment. The physical implementation of the NIMT is assured to use at the SMEs.

The overall objective of this methodology is to introduce cost-effective monitoring tool which targets the requirement of the SMEs, and it focuses mainly to introduce an all-in-one solution for the convenient monitoring process.

B. Experiment Design

To represent experiment design, the Figure 1 illustrates how the experment steps are carried out step by step as described in the methodology. The each step represents its pupose and involvement during the experiment.

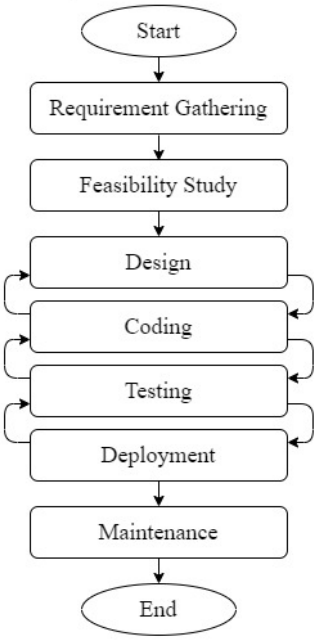


Figure 1: Flowchart of the Experiment

IV. IMPLIMENTATION AND TESING

A. Implementaion

The implementation is focused on five different elements for the solution as shown in Figure 2, and those are client application, server application, hardware device, web interface, and database. The client and server applications are developed with Python, and the web console is developed by using PHP. The database is introduced using MariaDB, and the deployment server is the Apache server.

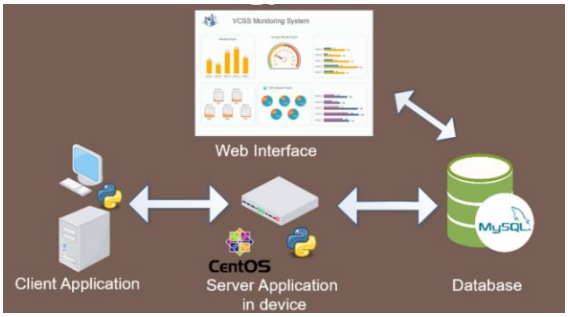


Figure 2: Solution Architecture

To introduce a prototype of the rack-mountable device, Fujitsu laptop motherboard with the processor, cooling system, RAM, and SATA hard disk are used in order to maintain low power consumption and size of one rack unit. Further, the CentOS operating system in CLI is selected due to the free license and minimum utilization of system hardware to install developed server applications. Finally, the solution development is

based on an iterative method that moves step by step in a linear fashion.

B. Testing

A demonstration is carried out in the actual working environment to make sure the practicality of the solution based on identified test cases. The results are obtained from the demonstration exhibits focusing on the adequate requirements of the monitoring system. The evaluation of the system is based on identified requirements to demonstrate its level of performance and ratings. As a result, a comprehensive tool is introduced adhering to the requirements.

V. RESULTS AND DISCUSSION

The Blade monitoring system is an all-in-one device and it has the capability to monitor Windows and Linux hosts. Moreover, the users can start monitoring the network infrastructure by simply connecting the device to the network and configuring the IP of the device and the network range. Further, it is possible to customize the available configurations assuring better security.

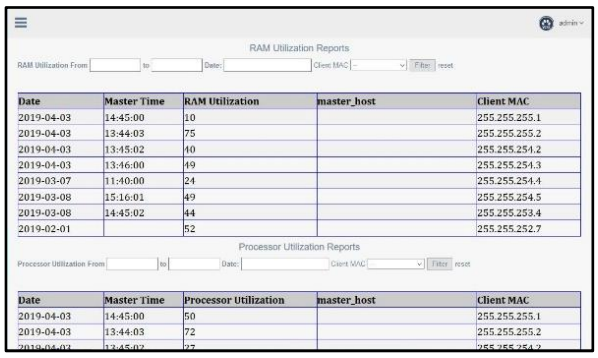
A. The outcome of the Blade NIMT

In the Blade NIMT, authentication and authorization have been implemented as basic functionalities to access the devices. Once the environment is ready, the privileged user is allowed to generate the report and alerts as shown in the following figures for example. On the other hand, a normal user can only view the reports and alerts belonging to an individual as per the assigned authorization.

Among the different approaches to evaluate the present utilization of network as per different diagnostic measures, few of them are illustrated below for sharing some understanding. In Figure 3, the highest utilization of the RAM, the hard disk and the processor of three different devices in the network is illustrated for required involvement. This interface is available for both the administrator and normal user roles.

Figure 3: Dashboard

In Figure 4, the RAM utilization and the processor utilization are retrieved for any device in the network for management purpose, and it is possible to apply filters based on date, time period and MAC.



Date	Master Time	RAM Utilization	master_host	Client MAC
2019-04-03	14:45:00	10		255.255.255.1
2019-04-03	13:44:03	75		255.255.255.2
2019-04-03	13:45:02	40		255.255.254.2
2019-04-03	13:46:00	49		255.255.254.3
2019-03-07	11:40:00	24		255.255.254.4
2019-03-08	15:16:01	49		255.255.254.5
2019-03-08	14:45:02	44		255.255.253.4
2019-02-01		52		255.255.252.7

Date	Master Time	Processor Utilization	master_host	Client MAC
2019-04-03	14:45:00	50		255.255.255.1
2019-04-03	13:44:03	72		255.255.255.2

Figure 4: RAM Utilization and Proccessor Utilization

Similarly, the hard disk utilization is also captured for any device in the network as per Figure 5.

Date	Master Time	Hard Disk Utilization	master_host	Client MAC
2019-04-03	14:45:00	72		255.255.255.1
2019-04-03	13:44:03	68		255.255.255.2
2019-04-03	13:45:02	59		255.255.254.2
2019-04-03	13:46:00	39		255.255.254.3
2019-03-07	11:40:00	45		255.255.254.4
2019-03-08	15:16:01	55		255.255.254.5
2019-03-08	14:45:02	25		255.255.253.4
2019-02-01		12		255.255.252.7

Figure 5: Hard Disk Utilization

Nevertheless, the upload and the download utilization are recorded for required actions as in Figure 6.

Figure 6: Network Traffic Upload and Down load Utilization

In the Figure 7, there is sample email notification which has been generated due to the suspicious downlod from a network node (DESKTOP-2JG20B8).

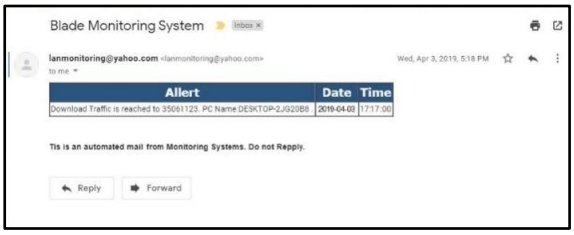


Figure 7: Email Notification Suspicious Download

B. *Evaluating the Blade NIMT*

In Table 2, the new Blade NIMT is also evaluated against the eight different criteria used for evaluating similar tools under section II, and the evaluation is based on the fulfillment of the requirements of SMEs.

Table 2: Evolution of the Blade Monitoring System

Option of the tool	Blade Monitoring System
Hardware Utilization Monitoring	Yes
Network Utilization Monitoring	Yes
Internal Session Detail Monitoring	Yes
Alerting and Reporting	Yes
Device Discovering	Yes
Additional License Software Required	No
Price (USD)	450
Hardware	Yes

1) Hardware Utilization Monitoring: hardware utilization is utterly important to observe over 24x7 otherwise the availability of the servers/services can be interrupted. Addressing such situation all the following tools have been provided some way of communication with network administrator/team via email, text, the dashboard in the industry.

2) Network Utilisation Monitoring (NUM): NUM is also important for the medium and large-scale industries where complex networking infrastructures are available. However, SMEs are not comprised of such networking infrastructures. As a result, the comprehensive NUM is not essential for SMEs by considering the requirement, despite there is average use of NUM in some situations.

3) Internal Session Detail Monitoring (ISDM): The number of connections that each computer maintains with some other computer can be captured through this feature with the details of the sessions. It is useful for recognizing the suspicious computer which is having an unpredictable connection with either internal or external device(s) because it can be due to internal/external threats. This feature is available by default only with the first option, and it is not affordable for the SMEs.

4) Alerting and Reporting: This is the primary option for any monitoring tool for having prompt notification in the pre-defined critical situation via email, text, mobile app, and dashboard, etc. In SMEs, the minimum level of these features should be available.

5) Device Discovering: The nodes of the networks are triggered via SNMP or client application focusing the traffic towards the well-known ports. However, it is not comprised as a basic feature for some cases.

6) Additional License Software Required: The basic version is not adequated in many cases to deploy the monitoring tools due to the requirement of the supplementary operating systems or application software. With that, it is further difficult to afford for SMEs.

7) Price: The NIMT is usually expensive aline with the available features. Although it is not considered with priority by SMEs due to the non-value addition for their business process SMEs should consider adopting some form of NIMT by considering uninterrupted networking facilities to streamline the business process.

8) Hardware: Almost all of the NIMTs are software-based implementation and it is required to adopt hardware to deploy NIMT which is not practical in SMEs because there is no strong technical workforce in most cases. As in Figure 8, the Blade NIMT is an all-in-one solution comprised of both hardware and the software together as one unit.

Figure 8: The Blade NIMT

C. Future Work

In this phase, the Blade NIMT focuses to monitor the hard disk utilization, RAM utilization, and processor utilization, Network bandwidth utilization of session in desktop, laptop, and servers within SMEs and send alerts as email or SMS to identified responsible individuals. Further, it is essential to extend the scope of the tools by monitoring intermediate devices such as switches, routers, firewalls in the next phase. Further, it is required to improve the reports/charts and improve the system coping with the progressive evolvement of the technologies. Nevertheless, the future development is aligned with improving the solution to the next level based on customer feedback to compete with the other competitive tools.

VI. CONCLUSION

A newly introduced monitoring system provides essential functionalities as per the main requirements of problem identification by considering the requirements of SMEs. Although the commercially available high-end products in the market are performing in a mature manner compared to the Blade NIMT in different aspects, the Blade NIMT fulfill the requirements of the SMEs adequately. Despite some open source tools are available to cater to the same requirement, those have complexities with the installation, configurations, utilization, and maintenance. The choice is always with the customer to make sure whether their requirement is fulfilled with the Blade NIMT because it is available to purchase for an affordable price of USD 450. In that background, the Blade NIMT strongly recommends for the startup companies and SMEs,

REFERENCES

Ferraiolo, D., Kuhn, R. and Hu, V., 2008. Authentication, Authorization, Access Control, and Privilege Management. *Wiley Handbook of Science and Technology for Homeland Security*, pp.1-12.

Jovanovic, N., Markovic, S., Popovic, O. and Jovanovic, Z., 2010. Managing Network Elements in the ComputerNetwork. *International Journal of Computer and Electrical Engineering*, *2*(2), p.316.

Liu, J., 2021, February. Analysis of Computer Network Maintenance Strategy Based on LAN. In *Journal of Physics: Conference Series* (Vol. 1744, No. 3, p. 032131). IOP Publishing.

Svoboda, J., Ghafir, I. and Prenosil, V., 2015. Network monitoring approaches: An overview. *Int J Adv Comput Netw Secur*, *5*(2), pp.88-93.

Verma, D.C., 2002. Simplifying network administration using policy-based management. *IEEE network*, *16*(2), pp.20-26.

ABBREVIATIONS AND SPECIFIC SYMBOLS

CLI – Command Line Interface
DNS – Domain Name Service
HTTP – HyperText Transfer Protocol
NIMT – Network Infrastructure Monitoring Tool
ICT – Information and Communication Technology
ISDM – Internal Session Detail Monitoring
NUM – Network Utilization Monitoring
ICMP – Internet Control Message Protocol
IP – Internet Protocol
PHP – PHP Hypertext Preprocessor
RAM – Random Access Memory
SATA – Serial Attached Technology Architecture
SME – Small and Medium Enterprises
SNMP – Simple Network Management Protocol
SMTP – Simple Mail Transfer Protocol
SMS – Short Message Service
SSH – Secure Shell

ACKNOWLDGMENT

The University of Vocational Technology is the one and only government university catering to the Technical and Vocational Education sector,

and this paper is the outcome of the final year project of the university. University offered different levels of assistance during the project.

AUTHOR BIOGRAPHIES

Eng. H.P.A.I. Pathirana is a senior lecturer at the University of Vocational Technology, and he earned his first degree in the Computer Engineering field from Faculty of Engineering, University of Peradeniya. He has earned his master of Computer Science degree from Flinders University of Australia, and his research interest is in the field of the semantic web, information security, and software engineering.

Mr.V.B. Godagama is a graduate in Bachelor of Technology in Networking Technology at the University of Vocational Technology. He has been working as an Assistant Manager IT in the IT sector for the past three years. His experience in the IT sector over 10 years. He is a researcher in the field of information security.

Mr. H.K.S.H. Premadasa is a graduate in Bachelor of Technology in Networking Technology at the University of Vocational Technology. He has been working as a Network Administrator in the IT sector for passed eight years. He is also a researcher in the field of networking system management.

Dr. Ravindra L. W. Koggalage is the Dean of the Faculty of Engineering Technology, and former Head of Department, Department of Electrical & Electronics Technology at the University of Vocational Technology. He has obtained two Ph.D. degrees in Mechatronics Engineering and Buddhist Studies from Australia and Thailand respectively. He has obtained M.Eng. from the Nanyang Technological University, and M.Sc. from National University of Singapore. His first degree is in computer science & Engineering (hons) from the University of Moratuwa, Sri Lanka. His research interests are ranging from Artificial Intelligence, Human Computer Interfacing, Data Mining and Data Science, Evolutionary Algorithms, Management, Mathematics and Mind Development. He is a certified Project Management Professional, and also internationally known meditation instructor. He has published over 50 international research papers, and nearly 15 books. He is the former Deputy Vice Chancellor-Academic of the Kotelawala Defence University and also held positions such as Chief Technology Officer, Director Projects in industry. He can be contacted by e-mail: koggalage@yahoo.com