PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

COMPREHENSIVE REVIEW OF BANDWIDTH USAGE ANALYSIS WITH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) IN FSKM LABORATORY

BALQIS AINI MUHAMMAD BAKHIT
College of Computing, Informatics and Mathematics
UiTM Melaka, Campus Jasin, Melaka
2022340777@student.uitm.edu.my

MOHD AZAHARI MOHD YUSOF*
College of Computing, Informatics and Mathematics
UiTM Melaka, Campus Jasin, Melaka
azahariyusof@uitm.edu.my

ALYA GEOGIANA BUJA
College of Computing, Informatics and Mathematics
UiTM Melaka, Campus Jasin, Melaka
geogiana@uitm.edu.my

Article Info

Received: March 2025
Accepted: September 2025
Available Online:November 2025

Abstract

This project focuses on improving network management and monitoring in all educational institutions by focusing on FSKM laboratory. Network monitoring is very important in educational institutions as it ensures connectivity runs well, helps in a successful use of bandwidth for better performance and online learning tools. Therefore, this paper aims to discuss the lack of comprehensive data concerning network performance. The main objectives are monitoring bandwidth usage using SNMP, visualizing performance metrics through PRTG, Zabbix, and Nagios, and analyzing traffic patterns to identify network inefficiencies. The methodology involved the use of Wi-Fi networks (UiTM WiFi STUDENT), implementing of SNMP agents on the devices, configuration of network monitoring tools, and collecting real-time data over three weeks. The collected results showed that Nagios gave consistent and reliable monitoring with no packet loss, Zabbix illustrated low latency with efficient resource usage, while PRTG offered user-friendly interfaces but showed limitations under high traffic. These findings define the strengths and weaknesses of each tool, highlighting the need to select suitable tools based on network requirements. In addition, this research shows how SNMP-based monitoring allows for better bandwidth, improvement of performance, and stable connectivity within educational environments.

Keywords: Network monitoring tools, network performance, PRTG, Zabbix, Nagios, SNMP, bandwidth usage

INTRODUCTION

Managing networks is important to make sure that people working or studying in an institution can access online resources quickly and easily. Education facilities mostly use network infrastructure to enable operational, research, and educational activities in this digital era. Staff and students need strong network connectivity to get involved in online learning, access online resources, collaborate on projects, and interact smoothly. A well-managed network infrastructure is required in supporting these educational initiatives.

Effective bandwidth is one of the most important aspects of network management in educational institutions (Keah Hui et al., 2020). Next, to meet the increasing demands of research projects, online examinations, multimedia content, and virtual classrooms, managing the network's ability to transport data is important. Students require a consistent, fast network connection to use the latest technologies for teaching and learning processes, like cloud-based software, tools for real-time communication, and video streaming.

This project aims to analyze the issues, improvements, and experiences related to the usage of bandwidth and network management in the FSKM laboratory. By focusing on these learning environments, the research aims to offer valuable insights that can improve network efficiency and enhance the use of resources to satisfy the increasing demands of educational institutions. The aim of this study is to provide more data and generate valuable results through increased network efficiency and improved use of resources. Therefore, the expectations are consistently increased when educational institutions are satisfied.

LITERATURE REVIEW

Bandwidth Usage Analysis

Bandwidth usage analysis is an important part of network management, especially in implementation like educational institutions where the need for data is considerable. For example, it is carried out with such purposes as ensuring network of bandwidth used and addressing various data transfer and network productivity problems.

In educational institutions, interactive learning environments, and online research are common. The ideal bandwidth control is important to maintain a stable and productive environment for educational purposes (Paredes & Hernandez, 2018). Since the FSKM laboratory has requirements and many data is transmitted over the network, one needs to

analyze bandwidth use as well as manage it. Network connections should be connected in the FSKM laboratory which enables numerous kinds of controlled the computers research.

Bandwidth is a serious factor in determining the speed and performance of the internet that refers to the network's ability to transmit data. Ensuring effective use of bandwidth allows staff and students' requirements to be met on the network thereby supporting effective learning, especially in educational institutions. Institutions can maintain a dependable and effective network infrastructure by minimizing bandwidth usage and monitoring it with tools like SNMP (Da Costa & Mesquita, 2022).

Simple Network Management Protocol (SNMP)

SNMP is a common application layer protocol to manage devices on IP networks. It enables network administrators to monitor and control network devices, collect performance data, and handle issues. SNMP, which operates through a system of agents and managers, simplifies the effort of reorganizing network management and allows for real-time monitoring to ensure security, stability, and availability. The protocol supports different versions, improving on security and functionality, with SNMPv3 providing more secure features, including strong authentication and encryption. Regardless of its ease of use, comprehensive monitoring features, and wide device coverage, SNMP has certain limitations, including security weaknesses in older versions and lack of ability to handle errors. To effectively monitor and optimize network performance, network administrators must understand both its strengths and limitations.

Simple Network Management Protocol (SNMP) is an application layer and widely used protocol for managing devices on Internet Protocol (IP) networks (Metropolia, 2021). It enables network administrators to monitor and control network devices, gather performance data, and detect address issues. SNMP is fundamental in network management due to its standardized communication protocols, which facilitate the exchange of management information between network devices. SNMP operates through a system of agents and managers, where agents collect data from devices and managers compile and analyze this information (Matthew et al., n.d.). In addition, SNMP-based network monitoring systems can find applications in almost any field where networked devices and infrastructure require monitoring, management, and optimization. The utilization of the SNMP approach in network monitoring systems simplifies the task of network administrators in centrally managing the

network. This approach enables real-time monitoring of computer networks, ensuring their continuous security, stability, and availability to meet users' demands (Alhilali et al., 2023).

Mechanisms of SNMP

SNMP allows to monitor bandwidth usage, identify peak usage times, and detect unusual patterns that can detect network issues. It is particularly useful for bandwidth usage analysis. It gives network administrators real-time monitoring of network traffic. In the FSKM laboratory, SNMP tools can visualize data trends, helping to manage and optimize network resources effectively (Amit Kore et al., 2019).

SNMP provides network management tools with the ability to gather information about network performance and configure network device metrics as part of device control. Network traffic data is not processed or analyzed by SNMP on its own. So, it provides a communication interface that uses network management systems to gather data needed for analyzing network performance. In addition, SNMP is one of the key components in monitoring tools for network performance. With SNMP, different network devices' agent objects may notify the events of the management to get network information.

SNMPv1, SNMPv2, and SNMPv3 are the three main versions of the Simple Network Management Protocol (SNMP). Basic SNMP operations like Get, GetNext, Set, and Trap were included in the 1988 release of SNMPv1, the first version of the protocol. Its security was limited, though, as it lacked encryption and authentication and did not respond to requests that contained errors of any kind (Bibbs & Matt, 2006). To improve data retrieval and communication between management systems, SNMPv2, which was first released in 1993, kept the same basic functions while adding more features like GetBulk and Inform. Besides that, it also provided for partial responses in situations where some of the request features were invalid and standardized the syntax to use for trap messages. Even though SNMPv2 upgraded the security, different implementations by different vendors resulted in inconsistencies.

With the introduction of the view-based access control model (VACM) and the user-based security model (USM) in SNMPv3, which was introduced in 2002, these security concerns were fully resolved. Network administration is more secure with these models' strong authentication, encryption, and access control. Thus, can safely and remotely update SNMP agent configurations. SNMPv3 message formats are more complex, separating security-related

data to provide better accuracy and ease (Bibbs & Matt, 2006). Table 1 shows the comparison of SNMP versions based on the features.

Table 1: Comparison of SNMP Versions

Features	SNMPv1	SNMPv2	SNMPv3
Protocol Operations	Get, GetNext, Set, Trap	Get, GetNext, Set, Trap, GetBulk, Inform	Same as SNMPv2 (Get, GetNext, Set, Trap, GetBulk, Inform)
Response to Invalid Requests	No response if any part is invalid	Provides partial results if the part is invalid	Same as SNMPv2
Security	Minimal, no authentication or encryption	Improved but inconsistent across variants	User-based Security Model (USM), enhanced security
Access Control	None	Limited and inconsistent	View-based Access Control Model (VACM)

Network Monitoring

The review of network monitoring to analyze bandwidth usage in the FSKM laboratory. Network monitoring solutions like PRTG, Zabbix, and Nagios explain in advance for monitoring purposes. By comparing the features of network monitoring tools and addressing identified problems statement. Also, understanding the importance of network monitoring tools.

Network monitoring involves utilizing hardware and software systems to continuously monitor the condition of network devices and services to guarantee security, integrity, and optimal performance (Peter et al., n.d.). It includes keeping an eye on both the services that are provided by the hardware, such as computers, routers, bridges, hubs, and other physical network components, and the software that runs on them. A Local Area Network (LAN) performance depends on this ongoing monitoring, which allows network administrators to identify and fix possible issues before they have an impact on operations (A Hamid et al., 2017).

There are multiple monitoring tools in the industry, some of them commercial, which means that a license needs to be purchased to use the product, such as SolarWinds, PRTG, and

ManageEngine. The other options are open-source platforms, which are Nagios and Zabbix (Hrín et al., 2019). These tools monitor critical metrics, including response time, availability, uptime, consistency, and reliability. Monitoring systems diagnose network faults and provide performance data by comparing the current state of the network to an internal model of its expected performance (Faris et al., 2023). This helps in identifying errors and potential issues that could disrupt network services (Amit Kore et al., 2019).

Analyzing bandwidth usage in the FSKM laboratory with the Simple Network Management Protocol (SNMP) is particularly important. SNMP is a protocol widely used for network monitoring, allowing for the collection and organization of information about managed devices on IP networks and for modifying that information to change device behavior (Matthew et al., n.d.). In the FSKM laboratory, system admins may use SNMP to address network resources as well as implement real-time monitoring. It is a guarantee of high bandwidth use, it prevents delays, and it makes sure that the network's performance is the same all through.

Comparison of Network Monitoring Tools

This section provides a comparison between three different network monitoring tools as presented in Table 2. In terms of these features used, PRTG, Zabbix, and Nagios each offer unique strengths and weaknesses. PRTG is widely recognized for its easy-to-use interface and setup tools, which enable even people without technical expertise to use it. Without a demand for in-depth networking knowledge, users may add devices for monitoring, set up alarms, and easily move through monitoring settings according to the platform's graphical user interface (GUI). However, Nagios has a more difficult process of learning and usually requires technical knowledge for users to configure and set up (Amit Kore et al., 2019). Zabbix is suited for users of all skill levels due to a combination of an easy-to-use web interface and simple navigation.

Next, PRTG is scalable enough for small- to medium-sized networks in terms of design. It has sufficient monitoring capabilities for these kinds of settings, but when used in larger networks with many devices, it might run into issues. Nagios is adaptable and appropriate for medium-sized networks because it provides a large amount of customization, which lets users customize monitoring configurations to meet the needs. Scalability represents where Zabbix performs well, providing excellent monitoring features that can easily manage large operations.

Organizations with wide network environments use it because of its architecture, which is built to facilitate distributed monitoring across complex network infrastructures (Manohar, 2020).

Data virtualization features that PRTG provides configure it separately and make network data visualization and analysis possible for users. Network performance metrics, bandwidth usage, and device health status are all shown in real-time through the platform's configurable interfaces. When looking for relevant data for maintenance and improvement, network engineers and network administrators will find this tool valuable (Jani et al., 2018). Nagios can display data in simple ways, but without additional plugins or modifications, its capabilities could be limited. Zabbix, like PRTG, supports data virtualization, allowing users to perform in-depth analysis and gain insights from network data, making it suitable for advanced monitoring and analysis requirements.

PRTG is recommended for reporting capabilities, providing full functionality with interfaces and templates that can be customized (Rahman et al., 2019). Monitoring and analyzing network behavior periodically is made simpler by the ability of users to generate comprehensive findings on historical data, alert notifications, and network performance patterns (Matthew et al., n.d.). Although users may have to spend time manually configuring Nagios to suit reporting requirements, the tool also offers customized reporting options. Users can create reports on network health, availability, and performance metrics with Zabbix's comprehensive analysis features, which include customizable templates. Also, the reporting features are valuable for generating insights and sharing key network data.

Table 2: Comparison Features of Network Monitoring Tools

Features	PRTG	Zabbix	Nagios
Ease of use	User-friendly interface, intuitive setup wizards	The steeper learning curve requires technical skill	Intuitive web interface, easy navigation
Scalability	Scalable for small to medium-sized networks	Scalable, suitable for medium-sized networks	Highly scalable, suitable for large deployments
Data virtualization	Offers data virtualization capabilities	Limited data virtualization options	Supports data virtualization for better analysis

Reporting	Comprehensive reporting with customizable dashboards	Customizable reporting, but requires configuration	Robust reporting features with customizable templates

Comparison of Solutions Provided by PRTG, Zabbix, and Nagios based on Identified Issues

PRTG is reliable for real-time bandwidth monitoring (Faris et al., 2023). Also, PRTG provides comprehensive data on various network aspects, supported by real-time readings and an intuitive interface (Fathima & Devi, 2024). In addition, Zabbix offers robust monitoring capabilities. Its detailed data collection allows for source code modifications, enhancing data comprehensiveness, which is beneficial useful for users (Chen & Li, 2024). Nagios, while flexible and capable of monitoring various systems through its use of plugins (Metropolia, 2021). Each tool can perform highly affected by the quality of setup and configuration. Table 3 shows a comparison of solutions provided by PRTG, Zabbix, and Nagios based on the identified problems for this project.

Table 3: Comparison of Solutions Providing by PRTG, Zabbix, and Nagios Based on Identified Problems

Network Monitoring Tools	**Problem Statement 1: Inconsistent monitoring of bandwidth usage**	**Problem Statement 2: Lack of comprehensive data**
PRTG	PRTG offers reliable real-time bandwidth monitoring.	PRTG provides comprehensive data on various network aspects, supported by real-time readings and an intuitive interface.
Zabbix	Zabbix provides robust monitoring capabilities with detailed data collection.	Zabbix is known for detailed data collection and allows source code modifications to enhance data comprehensiveness, benefiting those with coding skills.
Nagios	Nagios uses plugins for monitoring, which requires proper configuration to ensure consistency.	Nagios is very flexible and can monitor anything users need, but it requires specific scripts for each unique system

Related Works

This showed significant insights into many aspects of bandwidth management and Internet use in educational institutions in all the related research papers. It provides a comparison of the criteria of the related works.

Designing an Adaptive Bandwidth Management for Higher Education Institutions (Paredes & Hernandez, 2018)

The purpose of this paper is to create effective methods for controlling university Internet bandwidth. It highlights the need for a comprehensive plan that involves user education, technological solutions, and policy enforcement. According to the survey, institutions that do not have enough bandwidth management experience issues, including poor Internet access, which interferes with their ability to do research and teach classes. The article makes the argument that implementing monitoring tools, acceptable use policies (AUP), and quality of service (QoS) measures in a well-balanced approach is necessary compared to simply improving bandwidth. For the setup to be effective, everyone must be involved, including students, lecturers, and computer technicians. While protecting privacy and encouraging responsible use, effective bandwidth management should prioritize academic activities, maximize resource utilization, and create an environment that supports the institution of educational goals.

Internet Data Traffic Analysis for Identifying Usage Trends on Each Day of The Week in a University (Adekitan & Awosope, 2019)

This article focuses on analyzing Internet data traffic within Covenant University, Nigeria, over a year to uncover daily usage patterns. The purpose of the study is to provide insights into bandwidth usage trends, supporting network management optimization and improving service quality. The load placed on network resources because of increasing internet usage is the problem highlighted in educational institutions, which need effective bandwidth management. The review shows that there are high Internet usage patterns on certain days. Thursdays and Mondays saw the highest upload and download traffic, respectively. These findings can help in devising better network management strategies and ensuring balanced bandwidth used.

Internet Usage among University Students in Nigeria: A Case Study (Sawyerr-George & Agina-Obu, 2023)

For this article, provides a comprehensive examination of how university students in Nigeria engage with the Internet, focusing on both usage patterns and the challenges they face. The study aimed to collect data on internet use among students by using a large population of respondents who were interviewed or surveyed to gather more information about them. It has been found that most of the time students utilize this gadget on social networking sites or for entertainment purposes. However, apart from socializing there is so much academic information which is searched by many students while browsing through different web pages. The study finds a few important issues that prevent students from using the Internet effectively, regardless of their high levels of involvement. In Nigerian colleges, the poor Internet infrastructure is one of the main issues. The students complained about regular connectivity issues and slower Internet speeds, which seriously affected their ability to do online activities, especially academic ones. The high cost of Internet connection is one of the challenges, which makes it challenging for students to pay for dependable and common Internet connectivity. So, the current network infrastructure needs to improve, which requires more money to be spent on more reliable network systems and increased bandwidth inside the colleges for educational purposes.

METHODOLOGY

This chapter explains the process that was used in the completion of this project. Other than that, the project methodology looked over the methodology's phases which include the activities, deliverables, and objectives. There will be a study of the methods used to find, select, process, and analyze information that refers to research methodology. This methodology for a research paper helps to determine the effectiveness and reliability of research.

Project Methodology Framework

The methods and phases required to achieve the project's objective are explained in the project methodology framework. The phases start with gathering information, tool selection, implementation of SNMP, data collection and analysis, and documentation. Also, creating the flowchart and logical diagrams for the test bed's methodology. This structured approach ensures the monitoring of network performance issues in the FSKM laboratory. It has also been

mentioned that the framework consists of five phases. These phases are important to ensure that the project can be conducted specifically and figure 1 illustrates the project process.

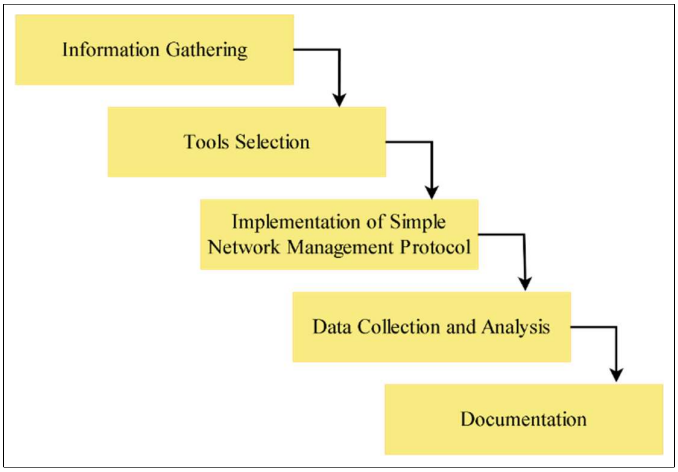

Figure 1: Project Methodology Framework

Project Methodology Flowchart

The project methodology flowchart process, from information gathering to documentation. It starts by connecting Wi-Fi student networks and installing three different network monitoring tools while configuring using SNMP. Data is analyzed to identify potential issues in network performance and the results are documented. Figure 2 shows the flowchart illustrating how each phase of the project will be executed.

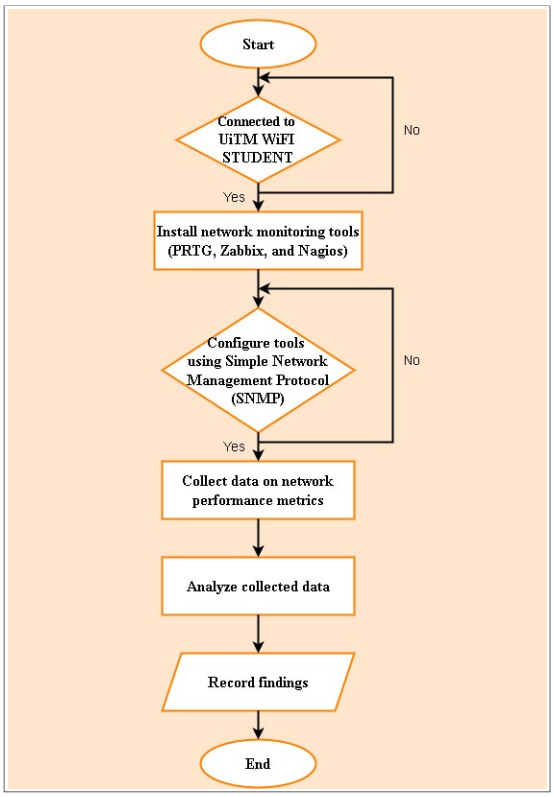

Figure 2: Flowchart

FSKM Laboratory Network Test Bed Diagram

The illustration of the network configuration, including SNMP agents and the connectivity of monitoring tools has been developed in a logical diagram. It enhances the thought of the network architecture and implementation approach. Network monitoring tools are installed, and SNMP is used in the FSKM laboratory. The tools are used to analyze and monitor bandwidth usage, latency, and packet loss. Figure 3 below shows the logical diagram of the test bed design, which represents the system architecture for this project.

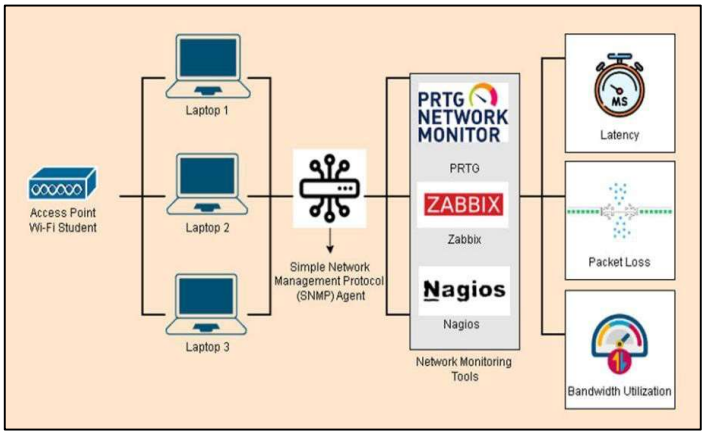

Figure 3: Test Bed Diagram

The processes for this outline to ensure that all project objectives were met according to plan. Each phase has its timeline with specific milestones to track progress and make sure the schedule is followed. The testing phase verified the achievement of project objectives. Data gathering and documentation across all phases are important for setting up the project report. In summary, the methodology supports project planning, ensuring a comprehensive and successful implementation within the stated timeline.

RESULT AND DISCUSSION

The results and analysis of the network monitoring tools used in the FSKM laboratory are presented in this chapter, focusing on PRTG, Zabbix, and Nagios. Besides that, it explains the setup process and analyzes the tools performance over three weeks of monitoring.

Result

The results summarize the monitoring of network performance at the FSKM laboratory using PRTG, Zabbix, and Nagios over a period of three weeks. The data was collected during peak and off-peak hours across different levels and sessions. It showed differences in bandwidth, latency, and packet loss among the tools. The discussion evaluated the performance of the three tools a week, level, sessions, and benchmark. Each tool had its strengths and weaknesses. Nagios consistently provided stable and reliable results, Zabbix was effective in environments with limited resources, and PRTG showed potential for improvement during periods of high network traffic.

Experiment: Network Monitoring Tools by Week

Based on Table 4, Nagios showed the highest bandwidth, 1.09Mbps with no packet loss, while PRTG has the highest latency, 13.28ms. Zabbix recorded the lowest bandwidth, 0.07Mbps, with no packet loss for the first week monitoring. In week 2, Nagios again collected the highest bandwidth, 1.17Mbps, but showed a higher latency, 6.20ms. For PRTG, it recorded the lowest bandwidth, 0.09Mbps, and had the highest packet loss, 0.44%. In week 3, Nagios maintained a stable performance with a bandwidth of 1.08Mbps, while PRTG had the highest latency, 14.50ms. The minimal bandwidth is 0.004Mbps, collected by Zabbix with no packet loss.

Table 4: Network Monitoring Tools: Average by Week

Week	Tools								
	PRTG			Zabbix			Nagios		
	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)
1	0.34	13.28	0.17	0.070	0.94	0.00	1.09	3.60	0.00
2	0.09	16.17	0.44	0.080	1.53	0.28	1.17	6.20	0.00
3	0.18	14.50	0.22	0.004	0.98	0.00	1.08	3.90	0.00

Experiment: Network Monitoring Tools by Level

Based on Table 5 below, at level 1, Nagios carried the highest bandwidth, 1.12Mbps and 0% for packet loss. However, PRTG had a higher latency, 10.17ms, and packet loss, 0.33%. Zabbix showed low usage of bandwidth with 0.04Mbps. Next, at level 2, Nagios maintained the stability of bandwidth with 1.12Mbps. Zabbix displayed the lowest packet loss, 0.16%, while PRTG illustrated higher latency 14.72ms. At level 3, Nagios's performance worked consistently with 1.11Mbps. PRTG recorded the lowest bandwidth, 0.13Mbps and highest latency, 19.78ms.

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 3 [November, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

Table 5: Network Monitoring Tools: Average by Level

Level	Tools								
	PRTG			Zabbix			Nagios		
	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)
1	0.25	10.17	0.33	0.04	1.12	0.12	1.12	4.81	0.00
2	0.24	14.72	0.33	0.03	1.14	0.16	1.12	5.37	0.00
3	0.13	19.78	0.17	0.09	1.20	0.00	1.11	3.59	0.00

Experiment: Network Monitoring Tools by Sessions

During the morning session, Table 6 showed Nagios had the highest bandwidth, 1.15Mbps with no packet loss, but PRTG had higher latency, 18.93ms. For Zabbix, this tool required minimal bandwidth, 0.02Mbps. Next, during the evening session, Nagios also showed a consistent bandwidth which is 1.08Mbps with no packet loss. PRTG had the lowest bandwidth, 0.06Mbps and lower latency, 10.85ms.

Table 6: Network Monitoring Tools: Average by Sessions

Sessions	Tools								
	PRTG			Zabbix			Nagios		
	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)
Morning	0.38	18.93	0.37	0.02	1.28	0.19	1.15	5.50	0.00
Evening	0.06	10.85	0.19	0.08	1.02	0.00	1.08	3.59	0.00

Experiment: Network Monitoring Tools Based on Benchmark

During peak hours, Nagios recorded the highest bandwidth, 1.16Mbps with no packet loss, while PRTG showed higher latency, 16.42ms and highest packet loss at 0.31%. Zabbix maintained minimal bandwidth use (0.07Mbps) but behaved better with low latency (1.22ms). During off-peak hours, Nagios maintained the highest bandwidth at 1.07Mbps, while PRTG recorded the lowest at 0.07Mbps but improved with the lowest latency of 2.67ms. All tools showed 0.00% packet loss, ensuring stable performance. Nagios proved consistently strong in bandwidth, Zabbix in latency, and PRTG showed better results off-peak. Table 7 below displayed the collected data based on the benchmark.

Table 7: Network Monitoring Tools Based on Benchmark

Benchmark	Tools								
	PRTG			Zabbix			Nagios		
	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)	Bandwidth (Mbps)	Latency (ms)	Packet Loss (%)
Peak hour	0.21	16.42	0.31	0.07	1.22	0.00	1.16	3.70	0.00
Off-peak hour	0.07	2.67	0.00	0.004	1.03	0.00	1.07	5.60	0.00

Discussion

The discussion evaluated the performance of the three tools a week, level, sessions, and benchmark. Each tool had its strengths and weaknesses. Nagios consistently provided stable and reliable results, Zabbix was effective in environments with limited resources, and PRTG showed potential for improvement during periods of high network traffic.

Comprehensive Comparison of Performance Metrics

The figures below show the detailed performance comparison of PRTG, Zabbix, and Nagios in terms of bandwidth usage, latency, and packet loss. This clearly shows that there are

different ways each manages network resources for the efficiency in monitoring network performance.

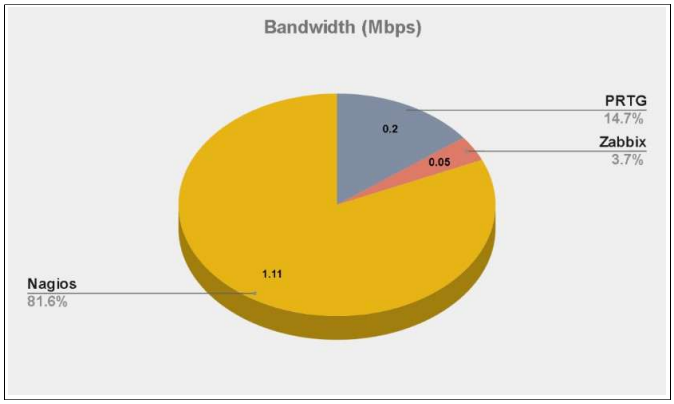

Figure 4: Pie Chart Bandwidth Usage

Among the three tools, Nagios records the highest bandwidth usage, resulting in 81.6% (1.11 Mbps), providing its regular processes of data collection and the complex monitoring configurations. Also, this tool has real-time and detailed data even if there are high monitoring activities using a lot of network bandwidth. This is why Nagios is not the ideal option for limited bandwidth. In terms of data management, PRTG is in the middle between Zabbix and Nagios, using 14.7% (0.2 Mbps) to show an attractive monitoring capability that does not use the network too much. Zabbix is the most effective than other selected tools, requiring a small amount of bandwidth at 3.7% (0.05 Mbps). Zabbix transfers less data because of its simple and organized design, which is useful for network with limited bandwidth. The main advantage is the tool works well even with low bandwidth, making it a good choice for institutions that have limited network usage.

Additionally, to improve bandwidth usage, Nagios can remain operational under incident-based monitoring, whereby data is collected only during unusual activities and not continuous monitoring of the network. PRTG may require further enhancement of the time established for data collection to avoid issues between comprehensive monitoring and network efficiency.

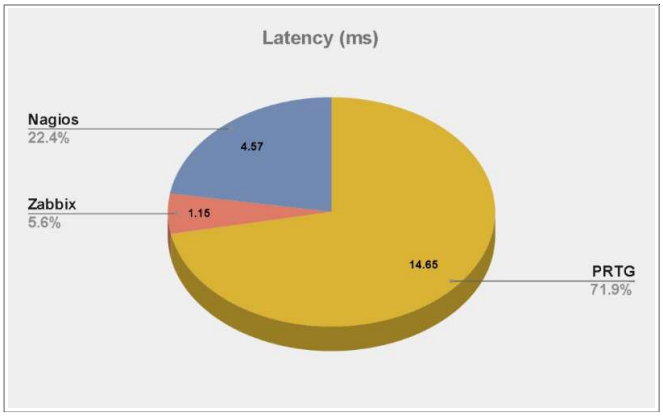

Figure 5: Pie Chart Latency

Figure 5 shows a comprehensive pie chart for latency which measures the responsiveness of the tools, demonstrates that PRTG faces the highest latency at 71.9% (14.65 ms), making it a bit slower. This high latency can be related to PRTG's comprehensive data analysis process, where large quantities of data are processed before updates are provided, causing delays. Network traffic also results in increased latency. Nagios has a normal latency of 22.4% (4.57 ms). Zabbix has the lowest latency of 5.6% (1.15 ms) because it has organized designs and highly effective data analysis tools. Zabbix's networked design allows for faster analysis and transmission, reducing delays and ensuring real-time monitoring capabilities.

To reduce latency, PRTG might set up monitoring sensors across different network areas, which would minimize data usage limitations and improve the performance. Additionally, PRTG could benefit from multiple data analysis, allowing it to handle multiple tasks simultaneously and reduce network traffic.

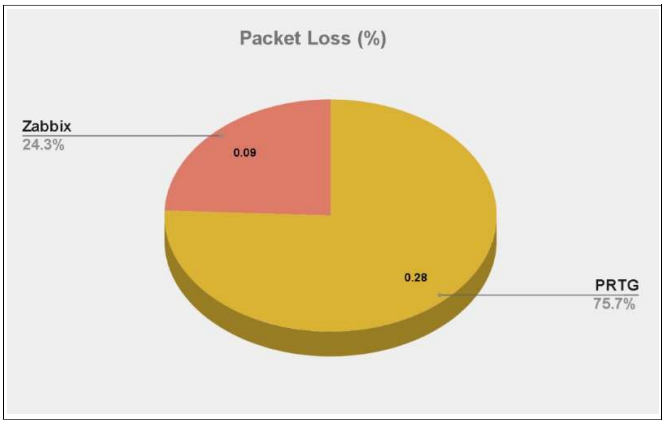

Figure 6: Pie Chart Packet Loss

Next, for figure 6, it illustrates the percentage of data packets loss during transmission. It shows that PRTG performs the worst, with a packet loss rate of 75.7% (0.28%), most likely to be a result of network traffic and ineffective data traffic methods. This high packet loss may affect the accuracy and reliability of the monitoring results. Besides that, the packet loss rate of 24.3% (0.09%) for Zabbix demonstrates better reliability, with displaying the reliable connections and successful data transmission mechanisms.

For Nagios tools constantly record no packet loss, showing its efficient error-handling method that ensures data transfer without loss. With no packet loss in Nagios suggests that it uses reliable data transmission methods to ensure the confidentiality of data. To minimize packet loss, PRTG should consider implementing more reliable transmission protocols, such as TCP, which is more possible to packet loss. Furthermore, network traffic management strategies, such as organizing traffic using Quality of Service (QoS) settings, can help to ensure that monitoring traffic is no interruption.

Nagios offers effective monitoring capabilities, but it has high bandwidth and low latency, making it insufficient for networks with limited bandwidth. PRTG, while maintaining bandwidth usage, has concerns with high latency and packet loss, which limits the effectiveness in high-traffic environments. However, Zabbix proves to be the most efficient solution, with the lowest bandwidth usage, minimal latency, and higher reliability, making it the best option for networks with limited resources.

A few strategies can be implemented to further improve the performance of these tools. Adaptive monitoring techniques, which network activities start monitoring, can reduce usage without affecting the performance. Data compression methods must also be employed to optimize bandwidth usage without affecting the quality of collected data. Organized designs are needed to ensure balanced efficiency, reliability, and responsiveness in different network environments. Finally, upgrades to wireless networking could be provided to further enhance data transmission efficiency and minimize packet loss and latency.

This chapter described how PRTG, Zabbix, and Nagios were implemented and showed how well the tools performed across various scenarios. The network monitoring tools showed clear advantages, showing how important it is according to network needs. For wireless networks, Nagios proved to be the most reliable tool, but Zabbix and PRTG provided alternative features for in-depth analysis and visualization.

The results demonstrated the unique strengths of each network monitoring tool. PRTG come out for its user-friendly interface and data visualization capabilities, but its irregular higher latency and packet loss require further optimization. Zabbix performed well in environments with limited resources, providing consistent monitoring and understanding of user's behavior. The most stable and dependable tool was Nagios, which provided consistent results in any circumstance with no packet loss and low latency.

The comparative analysis highlights the importance of selecting a network monitoring tool that meets specific requirements and conditions. However, all three tools are useful. The choice usually depends on factors such as network size, resource availability, and performance expectations. This study provides valuable insights into the application of SNMP-based monitoring tools for optimizing network performance in learning environments.

Choosing the right network monitoring tool depends on specific network needs and limitations. For comprehensive and detailed monitoring is required without concern for bandwidth usage, Nagios is a suitable network monitoring tool. However, for organizations that require efficient and low-latency monitoring, Zabbix is the most effective choice. Since PRTG is easy to use, it needs to be improved to manage the environment with high traffic. By considering the improvements suggested, these tools can be modified to meet different operational requirements while ensuring network stability and efficiency.

CONCLUSION

This project evaluated the performance of three network monitoring tools using the Simple Network Management Protocol (SNMP) to analyze bandwidth usage in the FSKM laboratory. The main objective is to determine which is the most suitable tool for ensuring optimal network performance in a learning environment.

Each tool has its own certain benefits. PRTG remained attractive for its simple interface that is easy to understand, and the visualization capabilities that could help with quick insights and detailed information. The only problem with it could not manage network traffic very well, because that displayed high latency and packet loss when there was high traffic. During implementations in FSKM laboratory with low usage of resources, Zabbix would be enough to provide full current patterns analysis that use the tools successfully. Nagios is the most stable tool providing ideal metrics concerning no packet loss and low latency under high network

traffic. This is the most scalable and reliable solution for complex, high-demand network environments with various plugin support.

In general, this study highlights the significance of selected network monitoring tools based on specific requirements such as ease of use, scalability, data virtualization, and reporting. The results show that SNMP-based monitoring is important for reducing bandwidth usage, improving network performance, and maintaining stable activities in the area. These insights can guide network administrators in choosing the most suitable tools to meet institutional needs.

REFERENCES

A Hamid, I. R., Ab Sukor, N. H., Mohd Foozy, C. F., & Abdullah, Z. (2017). NETWORK MONITORING SYSTEM TO DETECT UNAUTHORIZED CONNECTION. *Acta Electronica Malaysia*, *1*(2), 13–16. https://doi.org/10.26480/aem.02.2017.13.16

Adekitan, A. I., & Awosope, C. O. A. (2019). Internet data traffic analysis for identifying usage trends on each day of the week in a university. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(3), 1442–1452. https://doi.org/10.11591/ijeecs.v17.i3.pp1442-1452

Alhilali, A. H., Al Farawn, A., & Mjhool, A. Y. (2023). DESIGN AND IMPLEMENT A REAL-TIME NETWORK TRAFFIC MANAGEMENT SYSTEM USING SNMP PROTOCOL. *Eastern-European Journal of Enterprise Technologies*, *5*(9(125)), 35–44. https://doi.org/10.15587/1729-4061.2023.286528

Amit Kore, P., Bhat, M., Gorana, O., Ghugul, A., & Saha, S. (2019). Survey on Monitoring Of Network Using Open Source Software. *IJRAR19H1190 International Journal of Research and Analytical Reviews*. www.ijrar.org

Bibbs, E., & Matt, B. (2006). *Comparison of SNMP Versions 1, 2 and 3*.

Chen, C., & Li, K. (2024). Fangming Guo Research on Zabbix Monitoring System for Large-scale Smart Campus Network from a Distributed Perspective. In *J. Electrical Systems* (Vol. 20, Issue 10).

Da Costa, E., & Mesquita, S. (2022). Computer Network Management and Monitoring System With SNMP and QoS Approach. In *Journal of Engineering and Science* (Vol. 3, Issue 1). http://tljes.org/index.php/tljes/data

Faris, M., Fuzi, M., Firdaus, M., Mahdzir, M., Hazwam, I., Halim, A., & Ruslan, R. (2023). Performance Analysis of Open-Source Network Monitoring Software in Wireless Network. *Journal of Computing Research and Innovation (JCRINN)*, *8*(2). https://doi.org/10.24191/jcrinn.v8i2.375

Fathima, A., & Devi, G. S. (2024). Enhancing university network management and security: a real-time monitoring, visualization & cyber attack detection approach using Paessler PRTG and Sophos Firewall. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-024-02448-y

Hrín, A., Author Hrín, D., Salmikangas, S., & Assigned by Solteq Oyj, E. (2019). *Transfer of monitoring solution Transfer of monitoring solution Degree programme Information and Communications Technology*.

Keah Hui, L., Machap, K., & Chandrasekaran Arun, K. (2020). Bandwidth Management System to Monitor the Internet Connection. In *Journal of Applied Technology and Innovation* (Vol. 4, Issue 2).

Matthew, A., Khan, H., & Högskoleexamen, A. (n.d.). *Network Monitoring*.

Paredes, R. K., Sison, A. M., Medina, R. P., & Programs, G. (2018). Bandwidth Allocation Mechanism based on Users' Web Usage Patterns for Campus Networks. In *International Journal of Communication Networks and Information Security (IJCNIS)* (Vol. 10, Issue 2).

Peter, M., Mfupa, M., & Uk Employee, M. C. (n.d.). *The International Journal of Multi-Disciplinary Research Network Monitoring System (Net-Mon) The International Journal of Multi-Disciplinary Research*. www.ijmdr.net

Rahman, W., Nguyen, P. T., Rusliyadi, M., Laxmi Lydia, E., & Shankar, K. (2019). Network monitoring tools and techniques uses in the network traffic management system. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 11), 4182–4188. https://doi.org/10.35940/ijrte.B1603.0982S1119

Sawyerr-George, O. E., & Agina-Obu, R. (2023). Internet Usage among University Students in Nigeria: A Case Study. *Asian Journal of Information Science and Technology*, *13*(1), 16–20. https://doi.org/10.51983/ajist-2023.13.1.3411