Proceeding of ICMR 8(1), 25-34

Implementation of Adaptable Network Monitoring Using MRTG

Fania[1*], Abdul Habir[2]

[1]Faculty of Engineering, Universitas Serambi Mekkah, Aceh, Indonesia
[2]Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Malaysia

*Corresponding Author: faniausm@gmail.com

Abstract. *Having optimal network traffic management is a key element in building a reliable network infrastructure, especially for organizations that rely on connectivity to carry out their business activities. Various software is available, such as Solarwinds or PRTG, which provide full monitoring functionality, easy to use display, sophisticated analysis and advanced reporting capabilities. However, high costs are an obstacle for some organizations to do so. In these circumstances, the Multi-Router Traffic Guard (MRTG) provides a more affordable and effective solution based on open-source network monitoring needs. MRTG is a software package that provides an abstraction view of network traffic. Using the Simple Network Management Protocol (SNMP), MRTG collects data from network devices such as routers and switches and can monitor real-time network performance. Through SNMP, you can automatically get information about network usage, device status, and other statistics about the network. The purpose of this study is to examine the use of MRTG and assess its performance as an open-source solution for monitoring network traffic. The study was performed in stages, starting with installing and configuring MRTG and SNMP on Linux, then collecting SNMP network traffic data, and presenting the results in a graphical representation. The final stage is to assess the accuracy of the resulting data and the overall performance of the system. The result showed that MRTG can capture traffic on a network and help administrators detect problems more quickly and respond more effectively.*

Keywords: *Network, Monitoring, MRTG*

1. Introduction

The rapid technological developments in this digital age have made digital networks become an essential requirement for organizations. Network systems are needed to support the different activities and to facilitate information exchange within and outside the organization (Mahrivi & Nasution, 2024). This high dependence on networks means that even minor disruption can cause serious problems, such as problems with connectivity, reduced system performance and security threats, including data breaches and cyber-attacks. An efficient network monitoring system is therefore needed to enable administrators to continuously monitor the state of the network, detect problems at an early stage and maintain the stability, reliability and optimum performance of the network (Rizqi et al., 2025).

Network monitoring is the activity of collecting and analyzing data related to network conditions and then presenting it in the form of reports that can be used as a basis for decision making by administrators. In general, network monitoring is used to determine the performance of the computer network used by users, including data traffic and connection stability (Sidqi & Nathasia, 2021). The main purpose of network monitoring is to ensure that all network services and activities can run properly, stably, and without interruption while the network is in use (Manapa et al., 2020).

The importance of effective network monitoring can be clearly seen through real-life events, such as the ransomware attack that occurred at the National Data Center or Pusat Data Nasional (PDN) on June 20, 2024. As a result of the attack, various government services, including administrative systems and immigration services, were disrupted and had to be temporarily suspended (Sembiring & Pattihahuan, 2024). Since the PDN functions as an integrated data center that is interconnected and shared by central and regional government agencies, this incident posed a serious threat to the security of public and government data.

The network monitoring system monitors network connections in real time and periodically. The monitored network devices can be adjusted according to their needs and level of importance. As shown in Table 1, comparison of the common software for network monitoring.

Tabel 1. Comparison of Network Monitoring Tools

Reference	Software	Pros	Cons
(Siaulhak & Muis, 2025)	Nagios	Free license with limited function, with low to moderate system requirements	Complex configuration
(Najma & Octaviana, 2024)	PRTG	Easy to use, visually appealing, and with moderate system requirements	Limited free sensors
(Litha et al., 2023)	SolarWinds	Comprehensive features, detailed notifications, with moderate to high system requirements	High cost due to the use of a modular system
(Nendi & Maulana, 2024)	MRTG	Completely free, very lightweight and stable for simple traffic, with low system requirements	Focused on traffic monitoring, lacking a modern GUI

The selection of network monitoring tools needs to consider the requirements and the administrator's capability to manage it (Utami et al., 2026). Based on the above table, this study selected the Multi Router Traffic Grapher (MRTG) on the basis of its suitability for small and medium infrastructure that often have limited budgets but still needing a reliable network monitoring system.

MRTG is open-source software developed by Tobias Oetiker in 1995 to monitor network traffic using Simple Network Management Protocol (SNMP) (Putra et al., 2025). SNMP is used to monitor and manage network devices, both centrally and remotely, by collecting information about the condition and status of network devices (Aritonang & Simanullang, 2025). MRTG collects incoming and outgoing traffic data from network devices such as routers and switches, then displays it in the form of web-based graphs that are updated periodically. MRTG is written in Perl and utilizes SNMP utilities such as *snmpget* and *snmpwalk*. MRTG settings are stored in a configuration file with the .cfg extension. Traffic data is recorded in bytes per second, stored in log files, and displayed in graphs that are typically updated every five minutes (Nurhidayat & Sulistyo, 2023).

The MRTG web page displays information on the maximum, average, and current values of network traffic (Defit, 2022). MRTG can be used to monitor various protocols and network interfaces, and can be combined with external scripts to support network management. Networks monitored with SNMP consist of several main components, namely the Network Management System (NMS), SNMP Agent on network devices, Management Information Base (MIB), and Object Identifier (OID) (Husein & Gunawan, 2023). Communication between the SNMP Manager and Agent is carried out through several types of messages, as shown in Table 2.

Table 2. Types of SNMP Messages

Message Type	Function
GET	Request from the Manager to the Agent to retrieve the value of a specific parameter
GET-NEXT	Request from the Manager to the Agent to retrieve the next variable value, used to browse table data
GET-RESPONSE	Response from the Agent to the Manager in reply to a request, containing the requested data or operation status
SET	Request from the Manager to the Agent to change a parameter value on the Agent, if permitted
TRAP	Automatic notification from the Agent to the Manager when certain conditions occur, such as a device going offline or experiencing overload

The workflow of MRTG and SNMP can be seen in Figure 1, which shows the process of retrieving data from network devices via SNMP and displaying network traffic information in graphical form by MRTG.

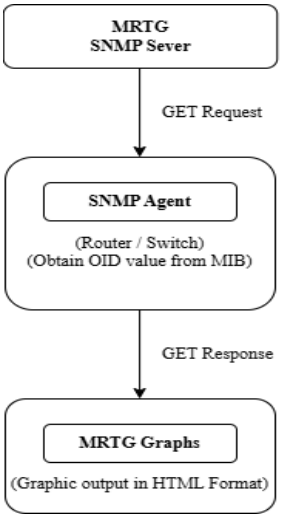

Figure 1. MRTG and SNMP Operation Flow

Based on this workflow, there are three main components in the network monitoring process namely MRTG as an SNMP Server, SNMP Agent, and MRTG graphics module. These three components interact with each other in accordance with the SNMP protocol workflow.

a. MRTG (SNMP Manager) functions to retrieve traffic data by sending SNMP GET commands to network devices.
b. Network devices provide data through MIB and respond to MRTG requests.
c. MRTG graphs stores the collected data in log files and displays it in the form of HTML based graphs that show network traffic.

Overall, MRTG is a network monitoring system that can be used to monitor network conditions. This system is suitable for organizations with limited resources but require structured network monitoring.

2. Method

In this study, the scope is limited to ensure that the discussion is more focused on system design and implementation. The network system used is fully virtualized using

Oracle VM VirtualBox, without discussing the performance of physical computer hardware. Kali Linux is used as a router and gateway with Network Address Translation (NAT) configuration, while the client machines consist of several Windows and Linux operating systems connected to the gateway.

Network monitoring is performed using SNMP-based MRTG software, with a focus on evaluating network traffic history. This study aims to demonstrate that MRTG is capable of capturing network traffic data and displaying it in graphical form, making it a reliable and free alternative solution for network monitoring in small to medium-sized organizations.

2.1 Research Flow

The research stages include system environment preparation, installation and configuration, testing and data collection, and the presentation of monitoring results for analysis. If the system fails to collect data during the testing stage, the process returns to the installation and configuration stage until validation is successful. The flow of the research stages is shown in Figure 2.

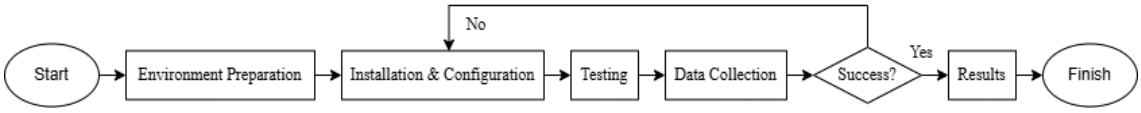

Figure 2. Flow of the Research Stages

2.2 Building Environment

The network diagram in Figure 3 illustrates the system architecture, data flow, and the relationships between components in this study.

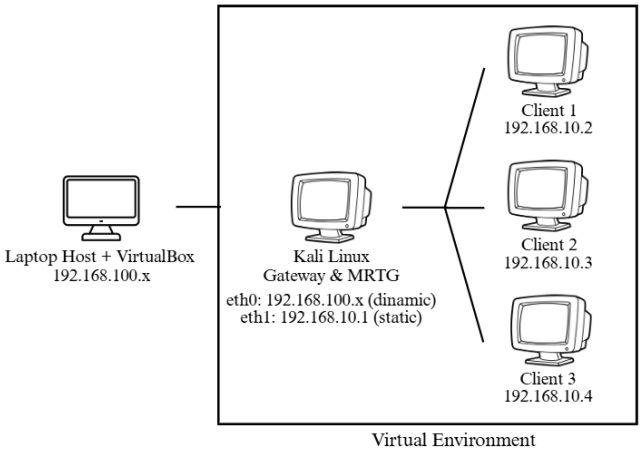

Figure 3. Network Topology Diagram

In the implemented network system, each device is assigned a specific IP address to support communication between devices. The system uses two different network segments, namely a dynamic network on the internet connection side and a static local network on the client side. This configuration directs all client traffic through the gateway, allowing MRTG to perform centralized traffic logging and monitoring. The allocation of IP addresses used in the system is presented in Table 3.

Table 3. Network IP Address Configuration

System Component	Role	IP Address	Description
Router and Gateway	eth0 (NAT)	Automatic (DHCP)	Used to obtain internet connectivity from the host system
Router and Gateway	eth1 (Local Gateway)	192.168.10.1	Functions as the local network gateway and the main path for all client traffic
Clients	Virtual Machine	192.168.10.2 192.168.10.3 192.168.10.4	Connected to the local gateway for network access

2.3 System Installation and Configuration

The installation process is carried out in a virtual environment consisting of several virtual machines. The installation includes MRTG, SNMP services, an Apache web server, including several other supporting tools. The stages of the installation process are shown in Figure 4.

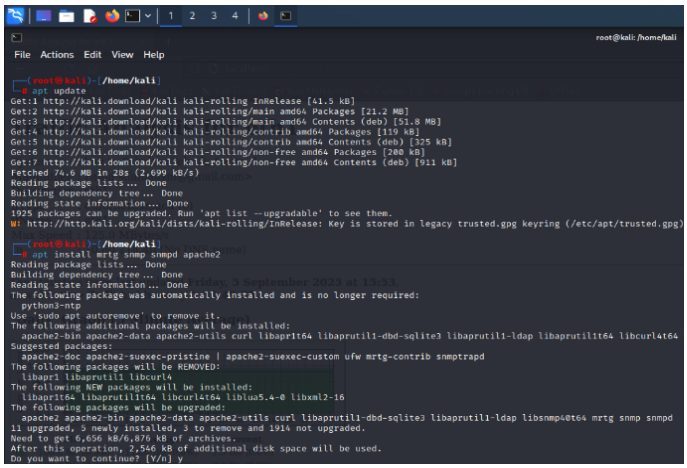

Figure 4. System Installation Overview

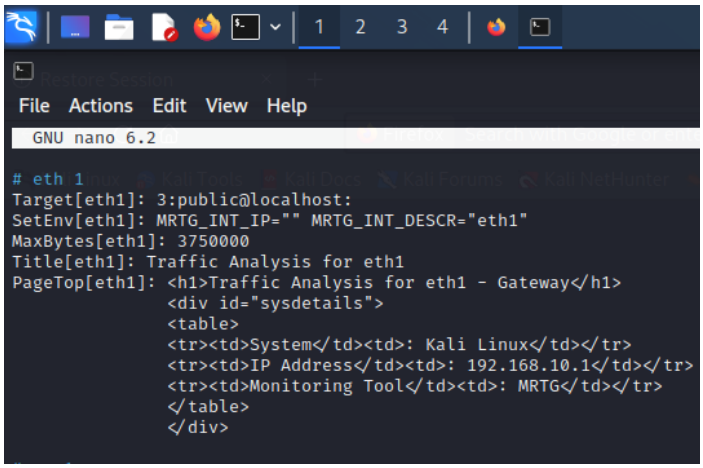

Figure 5. MRTG Configuration Parameters

In Figure 5, displayed the configuration applied with the purpose of retrieving the data. The configuration includes parameters set on the network interface that functions as

a gateway. The configured parameters include the data collection on target, the maximum network traffic limit (MaxBytes), the graph title (Title), and settings for displaying information on the web page (PageTop). These parameter settings enable MRTG to read incoming and outgoing traffic via the SNMP protocol and display them in the form of structured graphs.

The next configuration step is to enable the SNMP service via SNMPD on UDP port 161. In this setting the public community string is used to protect by only enabling the read-only access, meaning that MRTG can only read data from the device and cannot modify system settings. This configuration allows MRTG to safely poll data from the monitored device, as SNMPD only provides access to basic system information in accordance with security standards. This configuration is shown in Figure 6.

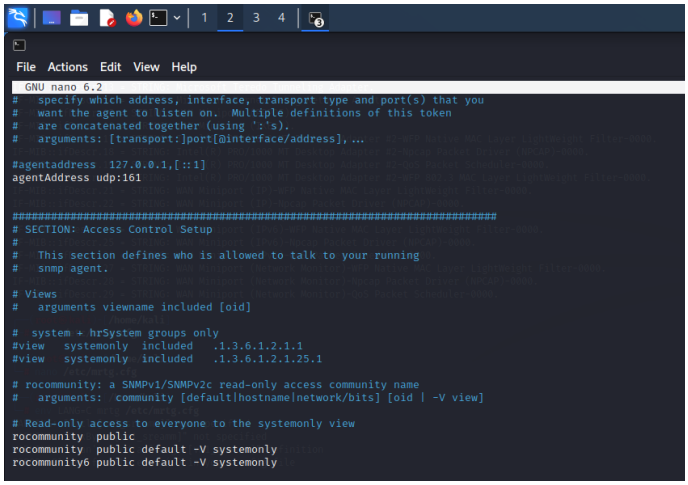

Figure 6. SNMP Configuration on the Network Gateway

The next step, the polling interval configured via crontab to automatically force MRTG to periodically run which in this case we set to five minutes. This configuration ensures that SNMP data retrieval, log file updates, and graph regeneration are performed consistently and continuously without requiring manual execution.

2.4 Simulation

Simulation was performed as a last step, after all components had been installed and configured. The main consideration at this stage was to assess network connectivity and to ensure proper data flow within the system. As shown in Figure 7, NAT rules were correctly applied, which means that data packets can be forwarded between interfaces depending on the configuration. The routing function has been enabled to allow sharing of Internet connections, and the IP forwarding function has been verified and set to 1 to ensure that the system can forward packets as a router. iptables have been implemented in the firewall configuration to enable NAT and allow data traffic between interfaces.

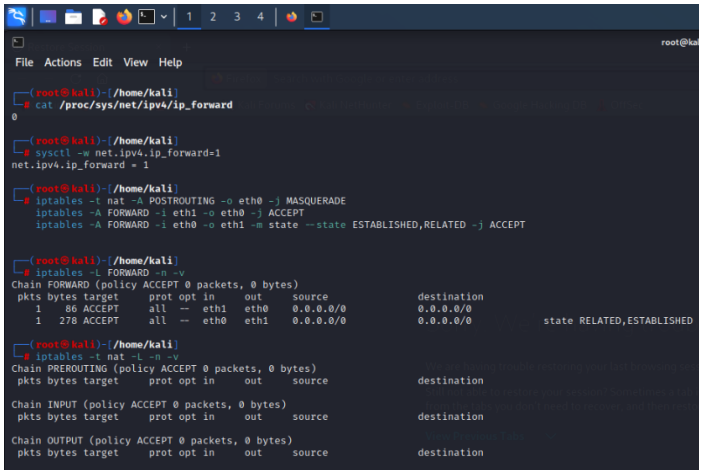

Figure 7. NAT Rules Configuration Using Iptables

In the process of data collection, the simulation perform by generating a massive network activities such as downloading and video streaming. The aim is to generate values of incoming and outgoing traffic which are observable on MRTG charts. During the simulation, the graphs are updated in accordance with the MRTG polling interval to simulate the conditions of real data flows, which allows the system to process and record traffic in a consistent manner.

3. Results and Discussions

Test results can be viewed through the MRTG page via a web browser. The index page loads properly, the eth1 interface graph is displayed accurately, and statistical values such as Current, Average, and Max appear according to the configuration, as shown in Figure 8 and Figure 9.

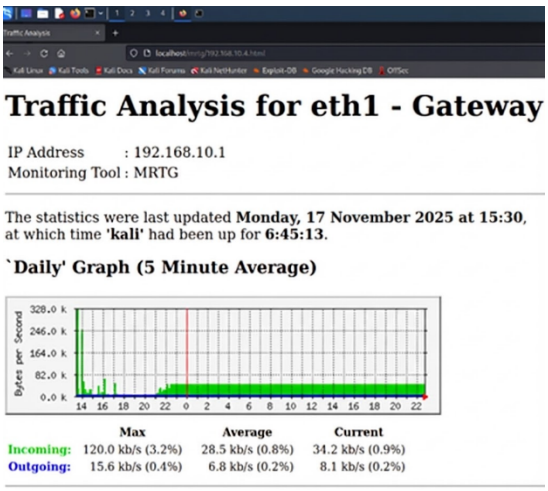

Figure 8. Network Traffic Graph Under Idle Conditions

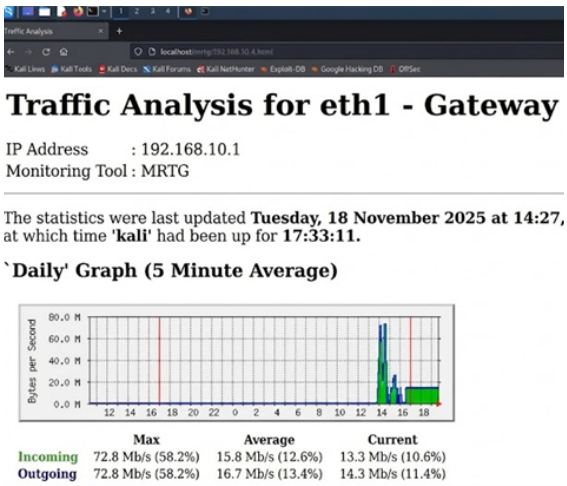

Figure 9. Network Traffic Graph During YouTube Streaming

As shown in Figure 8, the network traffic looks stable without a spike, which indicates minimal network usage. Summarized in Table 4.

Table 4. Network Traffic Under Idle Conditions

Traffic	Max	Average	Current
Incoming	120 Kb/s	28.5 Kb/s	34.2 Kb/s
Outgoing	15.6 Kb/s	6.8 Kb/s	8.1 Kb/s

Fron Figure 9, the graph shows the increased of network traffic due to massive video streaming conducted, which proven that MRTG have successfully recorded the traffic as summarized in Table 5.

Table 5. Network Traffic During YouTube Streaming

Traffic	Max	Average	Current
Incoming	72.8 Mb/s	15.8 Mb/s	13.3 Mb/s
Outgoing	72.8 Mb/s	16.7 Mb/s	14.3 Mb/s

The implementation of the network monitoring system using MRTG in the virtual network environment has been successfully completed as planned. The system able to periodically collect data on network traffic and displays them in the form of web-based charts. The graphs also updated every two or three sampling intervals to reflect the current network conditions in real time.

The test results show that the MRTG website is accessible, the traffic graphs are displayed correctly, and the network activity statistics are recorded. This suggests that MRTG may reflect variations in the traffic flows on the network according to the level of activity. Light activity produces stable graphs, while high activity results in an increase and a change in traffic, which indicates that the MRTG is responsive to the network conditions being recorded.

4. Conclusions

The results of this study show that MRTG can be implemented efficiently in a virtual network. The system provides reliable and continuous monitoring capabilities. MRTG not only allows the collection of traffic data on a regular basis but also displays information easily via graphs and statistics. A web interface enables administrators to monitor network conditions from any location, detect potential problems in advance, and assess the overall performance of the network which will help them for the network management decisions.

In addition, MRTG can be integrated with other scripts or SNMP configuration to extend the scope of MRTG monitoring, such as in specific protocols or bandwidth usage. This makes MRTG a practical and cost-effective solution for network monitoring without complex infrastructure investment. The implementation also proves that the use of open-source software can be applied effectively and customizable to be adapted to the needs of the organization.

5. References

Aritonang, M. A. S., & Simanullang, M. J. (2025). Penerapan Network Monitoring System Berbasis SNMP untuk Deteksi Dini Gangguan Jaringan. *Jurnal Pustaka AI (Pusat Akses Kajian Teknologi Artificial Intelligence)*, *5*(3), 735–742. https://doi.org/https://doi.org/10.55382/jurnalpustakaai.v5i3.1383

Defit, S. (2022). *Prediksi Tingkat Kebutuhan Bandwidth Jangka Panjang Menggunakan Metode Algortima Backpropagation*. *4*(1), 1–11. https://doi.org/10.47233/jteksis.v4i1.310

Husein, & Gunawan, D. (2023). PENERAPAN METODE SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) DALAM OPTIMALISASI KINERJA JARINGAN KOMPUTER STUDI KASUS PADA IDN BOARDING SCHOOL. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*. https://doi.org/10.35870/jimik.v4i3.410

Litha, A., Marampa, G. E., Duyo, R. A., Yuniarti, Y., & Sakir, R. K. A. (2023). Monitoring Kinerja Jaringan Kampus 2 Politeknik Negeri Ujung Pandang Menggunakan Aplikasi Solarwinds. *Jurnal Teknologi Elekterika*, *20*(2), 72–79. https://doi.org/https://doi.org/10.31963/elekterika.v20i2.4505

Mahrivi, I., & Nasution, M. I. P. (2024). Peranan Sistem Dan Teknologi Pada Proses Bisnis Organisasi. *Jurnal Ekonomi Bisnis Dan Manajemen*, *2*(1), 9–12. https://pdfs.semanticscholar.org/1c66/8f6bb31a6a4685ee53f36eebac8574a0b066.pdf

Manapa, E. S., Sampetoding, E. A. M., Sagala, T. W., & Taluay, H. R. (2020). Ulasan Penelitian Sistem Operasi Waktu Nyata di Indonesia: Review of Real-Time Operating System Research in Indonesia. *Journal Dynamic Saint*, *5*(2), 973–979. https://doi.org/10.47178/dynamicsaint.v5i2.1109

Najma, L., & Octaviana, M. E. A. (2024). Monitoring Jaringan Menggunakan PRTG (Studi Kasus: Fakultas Ekonomi Bisnis UPN "Veteran" Jatim). *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *6*(1), 44–53. https://doi.org/https://doi.org/10.33005/jifti.v6i1.149

Nendi, N., & Maulana, F. (2024). Monitoring Traffic Berbasis SNMP pada Jaringan Perumahan Permata Puri Harmoni 2. *Jurnal Sains Dan Teknologi*, *5*(3), 735–740. https://doi.org/https://doi.org/10.55338/saintek.v5i3.1346

Nurhidayat, A., & Sulistyo, W. (2023). Analisis Dan Implementasi Manajemen Bandwidth Untuk Optimalisasi Layanan Jaringan Internet BUMDes Di Jlumpang. *Progresif: Jurnal Ilmiah Komputer*, *19*(2), 647–658. https://doi.org/10.35889/progresif.v19i2.1271

Putra, J. S., Khairil, K., & Lianda, D. (2025). Implementasi Simple Network Management Protocol (SNMP) Untuk Melakukan Monitoring Dan Manajemen Jaringan Pada SMK N 5 Kota Bengkulu. *JURNAL MEDIA INFOTAMA*, *21*(1), 136–142. https://doi.org/https://doi.org/10.37676/jmi.v21i1.7539

Rizqi, R. M., Irawan, R., & Ardiansyah, A. (2025). *Kajian Sistematis : Ancaman dan Solusi Keamanan Jaringan pada Organisasi dan Individu*. *3*(4), 650–655. https://jurnalmahasiswa.com/index.php/teknobis/article/view/3361

Sembiring, F., & Pattihahuan, F. M. (2024). *PERAN BADAN SIBER DAN SANDI NEGARA DALAM KASUS SERANGAN SIBER YANG MENGAKIBATKAN KEBOCORAN DATA PRIBADI PUSAT DATA NASIONAL SEMENTARA 2 (PDNS2)*. *2*(February), 4–6. https://doi.org/10.25170/gloriajustitia.v5i1.6807

Siaulhak, S., & Muis, I. (2025). Implementasi Sistem Monitoring Jaringan Berbasis

Nagios di SMK Negeri 11 Luwu Menggunakan Notifikasi WhatsApp. *Jurnal Sintaks Logika*, *5*(2), 205–214. https://doi.org/https://doi.org/10.31850/jsilog.v5i2.4001

Sidqi, T. O., & Nathasia, N. D. (2021). Implementasi Manajemen Bandwith Menggunakan Metode Htb (Hierarchical Token Bucket) Pada Jaringan Mikrotik. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *6*(1), 132–138. https://doi.org/https://doi.org/10.29100/jipi.v6i1.1927

Utami, P. S., Kalsum, T. U., & Mardiana, Y. (2026). Designing A Computer Network At Sman 10 Kota Bengkulu With Bandwidth Management Web-Based Computer Network And Hybrid Topology. *Jurnal Media Computer Science*, *5*(1), 235–244. https://doi.org/https://doi.org/10.37676/jmcs.v5i1.9077