JOURNAL INNOVATIONS COMPUTER SCIENCE
E-ISSN: 2961-970X, P-ISSN: 2961-9718
Volume 4 Number 2, November 2025, pp 335-344.
DOI: https://doi.org/10.56347/jics.v4i2.346

Analysis of Enterprise Network Performance Using the SNMP (Simple Network Management Protocol) Method

Hilmi Alwanto [a*], Mesra Betty Yel [b]
[a*,b] Informatics Engineering, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

ABSTRACT
This study examines the implementation of the Simple Network Management Protocol (SNMP) integrated with the Cacti monitoring platform to evaluate enterprise network performance within a simulated environment using PNETLab. A quantitative approach was applied through continuous data collection and measurement of key performance indicators such as throughput, packet loss, delay, and availability. The experiment utilized virtual Mikrotik routers connected to an Ubuntu-based Cacti server configured for SNMP polling and RRDTool data storage. Real-time visualization enabled efficient tracking of network behavior and early detection of anomalies. The results showed that under normal conditions, the network achieved stable performance with throughput between 70–90% of link capacity, zero packet loss, latency below 150 milliseconds, and availability above 99%, meeting ITU-T/TIPHON Quality of Service (QoS) standards. When faults were simulated, the system accurately detected and displayed traffic interruptions, allowing rapid identification and resolution of network issues. Compared with other monitoring tools such as Zabbix and Nagios, the SNMP–Cacti integration proved simpler to configure while maintaining analytical precision and reliability. These findings confirm that Cacti, supported by SNMP, provides an efficient, scalable, and low-overhead solution for enterprise network monitoring. Future development may incorporate SNMPv3 for enhanced security and automated alert systems or predictive analytics to improve responsiveness and proactive maintenance in larger infrastructures.

ARTICLE HISTORY
Received 4 August 2025
Accepted 13 October 2025
Published 30 November 2025

KEYWORDS
SNMP; Cacti; Network Monitoring; Quality of Service; Enterprise Network.

1. Introduction

The rapid advancement of information technology has positioned computer networks as the backbone of modern organizational infrastructure, supporting data communication, application services, and operational productivity. Within enterprise environments, maintaining reliable, stable, and secure network performance is essential to ensure consistent Quality of Service (QoS) standards (ETSI, 2000). However, persistent issues such as packet loss, suboptimal bandwidth utilization, latency, and device downtime continue to pose challenges that may degrade service quality and hinder business operations (Prasetyo & Nugroho, 2021). A major obstacle for network administrators lies in the difficulty of monitoring performance in real time. In many cases, devices must be examined individually, which prolongs fault

CONTACT Hilmi Alwanto hilmi.mqj@gmail.com Informatics Engineering, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

identification and delays corrective action. The absence of an integrated monitoring system often allows network disturbances to propagate before they are detected (Purnomo *et al*., 2022). To address this, automated monitoring systems capable of collecting and analyzing performance data efficiently have become increasingly vital (Khan & Khan, 2018). The Simple Network Management Protocol (SNMP) remains one of the most widely adopted standards for network management and performance monitoring (Cisco Systems, 2022; Stallings, 2013). SNMP enables data collection from network devices such as routers and switches, offering metrics including bandwidth usage, packet transmission rates, and uptime statistics. Nonetheless, SNMP functions primarily as a data-gathering mechanism and requires an external visualization platform to transform raw data into interpretable information. One widely recognized solution is Cacti, a web-based monitoring application that leverages SNMP for data polling, utilizes RRDTool for time-series data storage, and provides graphical representations for analysis (Cacti Group, 2023; Oetiker, 2015; Sari & Putra, 2020).

Several studies have highlighted the practical benefits of integrating SNMP with visualization tools such as Cacti and Zabbix in enterprise monitoring. Pradana, Widiasari, and Efendi (2022) demonstrated that SNMP-based monitoring significantly improves network transparency, while Rahma, Indriyani, and Sandi (2023) confirmed its scalability in server infrastructure management. Similarly, Husna and Rosyani (2021) as well as Ishaq and Firmansyah (2023) emphasized the role of multi-platform integrations (e.g., Grafana and Telegram) in enhancing real-time notification and response efficiency. Comparative evaluations by Lebiednik, Nowak, and Wróbel (2019) also found Cacti to be an effective and lightweight alternative to more complex monitoring tools such as Zabbix (Zabbix LLC, 2022) and Nagios (Nagios Enterprises, 2022). This study employs PNETLab as a controlled simulation environment to integrate virtual network devices with a Cacti-based monitoring server. The platform provides a safe and reproducible environment to evaluate performance before real-world deployment. By applying a quantitative approach, this research aims to assess the effectiveness of SNMP-based monitoring through Cacti in identifying and analyzing enterprise network performance. The expected outcome is a technically grounded evaluation of how such integration supports reliable, efficient, and scalable network monitoring solutions for enterprise environments.

2. Methodology

This study applies a quantitative research approach based on direct observation and measurement of enterprise network performance using the Simple Network Management Protocol (SNMP) as the core data collection method. The experimental environment was designed within the PNETLab virtualization platform, enabling controlled simulation of network devices and scenarios before real-world implementation. The simulated topology included several Mikrotik routers configured with SNMP to enable automated and periodic data retrieval. The parameters monitored comprised key performance indicators such as bandwidth utilization, packet loss rate, device uptime, and interface error counts. Data polling was performed continuously at five-minute intervals and stored in a time-series log format for subsequent quantitative analysis. For network visualization and monitoring, the Cacti application was deployed on an Ubuntu server and fully integrated with SNMP. This configuration allowed real-time graphical representation of performance metrics through RRDTool's time-series database (Oetiker, 2015; Cacti Group, 2023). Cacti's web-based interface enabled

efficient interpretation of traffic patterns and early detection of performance anomalies, aligning with the findings of Sari and Putra (2020) on its reliability in enterprise environments. In parallel, the experiment simulated network faults by adjusting traffic loads and deliberately disconnecting selected interfaces to evaluate how effectively the system detected and represented anomalies. The method ensured reproducibility and control in identifying the correlation between traffic behavior and system responsiveness, as also suggested by Lebiednik, Nowak, and Wróbel (2019), who emphasized the importance of benchmarking multiple monitoring tools for enterprise networks.

To strengthen data interpretation, additional analytical processing was carried out using clustering-based machine learning techniques, categorizing network conditions into normal, overload, device malfunction, and link error states. This analytical layer reflects the recommendations by Sari, Safrianti, and Jalil (2023), who advocate integrating intelligent analytics into network monitoring for improved responsiveness under varying traffic loads. The methodological framework aligns with studies by Khan and Khan (2018) and Rahma, Indriyani, and Sandi (2023), which emphasize the significance of automated, scalable, and data-driven monitoring systems for complex infrastructures. The experiment also considered implementation insights from Husna and Rosyani (2021), Ishaq and Firmansyah (2023), and Pradana, Widiasari, and Efendi (2022), who highlight the operational advantages of combining SNMP-based data collection with visual and notification-based systems such as Zabbix, Grafana, and Telegram. These comparative perspectives guided the validation process to ensure the SNMP–Cacti integration achieved both technical efficiency and practical reliability. Overall, this methodological design adheres to established SNMP configuration principles (Cisco Systems, 2022; Stallings, 2013) and QoS standards defined by ETSI (2000), ensuring that performance evaluations remain accurate, consistent, and applicable to enterprise-scale network environments.

3. Results

The experimental implementation of the enterprise network monitoring system was carried out using both hardware and software components as summarized in Table 1. The simulation environment was established in PNETLab, integrating multiple virtual routers, a monitoring server, and client devices to emulate real enterprise network conditions.

Table 1. Research Equipment Specifications

No	Device / Software Type	Specification / Version
1	Laptop	Intel Core i11, RAM 8 GB
2	VMware Player	Version 17 Pro
3	Virtual Environment	PNET_4.2.10
4	Operating System	Ubuntu 22.04 LTS
5	MikroTik Router	Version 6.49.19 (Stable)

The implemented system architecture consisted of three Mikrotik routers (R-1, R-2, R-3), multiple PC clients, and a central Ubuntu server hosting the Cacti monitoring application. The server acted as the main monitoring hub, conducting SNMP polling across all network devices, storing data via RRDTool, and presenting real-time performance metrics through graphical visualization. This configuration ensured continuous monitoring of throughput, packet loss, delay, and availability parameters within the simulated enterprise network.

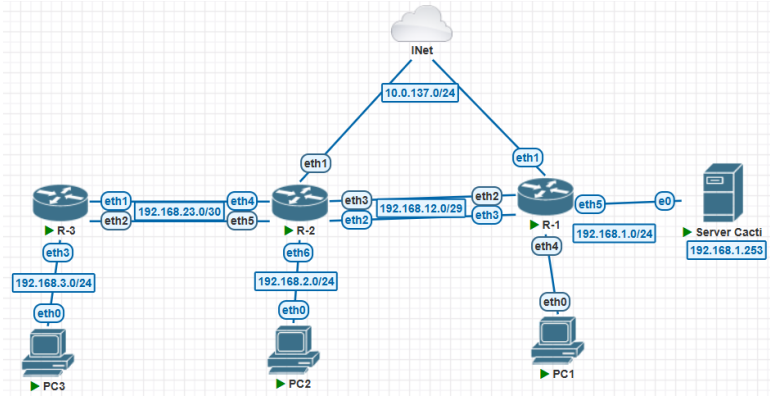

Figure 1. System Implementation Topology
(Description: Ubuntu server running Cacti connected to Mikrotik routers and PC clients within the PNETLab environment.)

The network topology illustrated in Figure 1 represents the overall structure of the simulation. The Cacti server, running on Ubuntu, was connected to Mikrotik routers and client devices within the virtualized PNETLab environment. The routers acted as inter-segment gateways, while clients generated traffic to simulate user activity. The Cacti server periodically polled SNMP-enabled routers to collect traffic data, ensuring centralized visibility across all interfaces. This configuration enabled administrators to observe real-time traffic changes, identify performance degradation, and track overall network health efficiently. Before data collection, verification was conducted to ensure the proper functioning of Cacti's supporting services—Apache2 as the web server and MariaDB as the database management system. Both services were confirmed to be active and stable on Ubuntu 22.04, as shown in Figures 2 and 3.

```
user@ubuntu22-server:~$ sudo systemctl status apache2
[sudo] password for user:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Mon 2025-08-11 08:05:50 WIB; 2h 14min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 606 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC>
   Main PID: 769 (apache2)
      Tasks: 11 (limit: 4558)
     Memory: 92.6M
        CPU: 47.814s
     CGroup: /system.slice/apache2.service
             ├─ 769 /usr/sbin/apache2 -k start
             ├─2451 /usr/sbin/apache2 -k start
             ├─3952 /usr/sbin/apache2 -k start
             ├─6774 /usr/sbin/apache2 -k start
             ├─7787 /usr/sbin/apache2 -k start
             ├─8178 /usr/sbin/apache2 -k start
             ├─8432 /usr/sbin/apache2 -k start
             ├─8704 /usr/sbin/apache2 -k start
             ├─8975 /usr/sbin/apache2 -k start
             ├─9220 /usr/sbin/apache2 -k start
             └─9604 /usr/sbin/apache2 -k start

Aug 11 08:05:48 ubuntu22-server systemd[1]: Starting The Apache HTTP Server...
lines 1-23...skipping...
```

Figure 2. Apache2 Service Status
(Excerpt from terminal output: systemctl status apache2)

The Apache2 service was reported active (running) since August 11, 2025, 08:05:50 WIB, confirming that the Cacti web interface was fully operational and ready to handle client requests. Additional diagnostic data included: Main PID: 769 Active processes: 11 Memory usage: 92.6 MB CPU time: 47.814 seconds.

```
user@ubuntu22-server:~$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.6.22 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-08-11 08:05:59 WIB; 2h 17min ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 619 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=
0/SUCCESS)
    Process: 669 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=
0/SUCCESS)
    Process: 687 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||
VAR=`/usr/bin/galera_recovery`; [ $? -eq 0 ]   && systemctl set-envir
    Process: 848 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=
0/SUCCESS)
    Process: 850 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 763 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 14 (limit: 30086)
     Memory: 204.3M
        CPU: 33.317s
     CGroup: /system.slice/mariadb.service
             └─763 /usr/sbin/mariadbd

Aug 11 08:05:58 ubuntu22-server mariadbd[763]: 2025-08-11  8:05:58 0 [Warning] 'innodb-file-format' was removed.
It does nothing now and exists only for comp
Aug 11 08:05:58 ubuntu22-server mariadbd[763]: 2025-08-11  8:05:58 0 [Warning] 'innodb-large-prefix' was removed.
It does nothing now and exists only for com
Aug 11 08:05:58 ubuntu22-server mariadbd[763]: 2025-08-11  8:05:58 0 [Warning] You need to use --log-bin to
make --expire-logs-days or --binlog-expire-logs-s
Aug 11 08:05:58 ubuntu22-server mariadbd[763]: 2025-08-11  8:05:58 0 [Note] Server socket created on IP:
'127.0.0.1'.
Aug 11 08:05:59 ubuntu22-server mariadbd[763]: 2025-08-11  8:05:59 0 [Note] /usr/sbin/mariadbd: ready for
connections.
Aug 11 08:05:59 ubuntu22-server mariadbd[763]: Version: '10.6.22-MariaDB-0ubuntu0.22.04.1'  socket:
'/run/mysqld/mysqld.sock'  port: 3306  Ubuntu 22.04
Aug 11 08:05:59 ubuntu22-server systemd[1]: Started MariaDB 10.6.22 database server.
Aug 11 08:05:59 ubuntu22-server /etc/mysql/debian-start[852]: Upgrading MySQL tables if necessary.
Aug 11 08:06:00 ubuntu22-server /etc/mysql/debian-start[867]: Checking for insecure root accounts.
Aug 11 08:06:00 ubuntu22-server /etc/mysql/debian-start[871]: Triggering myisam-recover for all MyISAM tables and
aria-recover for all Aria tables
lines 1-28/28 (END)
```

Figure 3. MariaDB Service Status
(Excerpt from terminal output: systemctl status mariadb)

MariaDB version 10.6.22 was also found to be active (running) since 08:05:59 WIB, serving as the data repository for Cacti's configurations, historical logs, and graphical records. Recorded metrics included: Main PID: 763 Active processes: 14 Memory usage: 204.3 MB CPU time: 33.305 seconds Active socket: /run/mysqld/mysqld.sock on port 3306. The successful operation of these two core services validated the readiness of the monitoring environment. Both Apache2 and MariaDB were critical for system functionality—Apache2 delivering the user interface, and MariaDB maintaining structured performance data. Ensuring both services were stable was essential for accurate visualization and uninterrupted data collection.

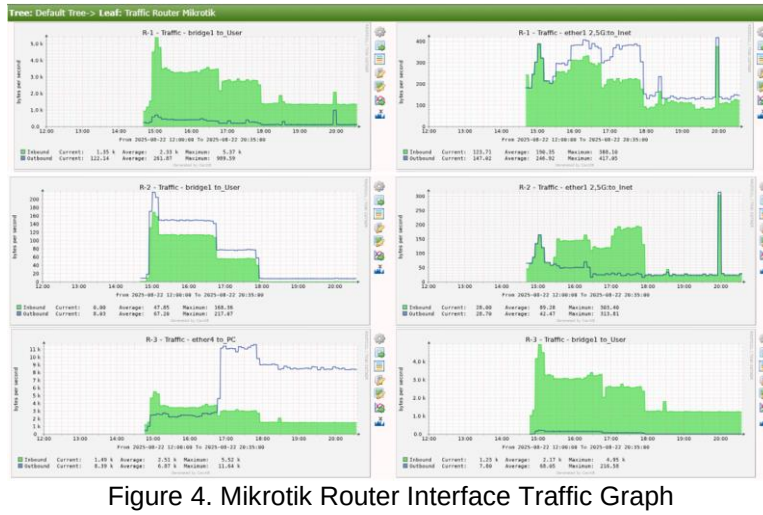

Figure 4. Mikrotik Router Interface Traffic Graph

Cacti's visualization interface generated continuous time-series graphs representing inbound and outbound traffic per router interface. Figure 4 shows a sample graph capturing the dynamic traffic behavior on one Mikrotik router. The graphical fluctuation pattern reflected the natural variation in network activity, verifying that SNMP polling effectively captured real-time changes. This visualization allowed network

administrators to quickly assess link utilization levels, detect early signs of congestion, and take preventive action before bottlenecks impacted service delivery.

Table 2. Network Performance Monitoring Results (Normal Condition)

Parameter	Average Result	QoS Category (ITU-T/TIPHON)
Throughput	70–90% of link capacity	Good
Packet Loss	0%	Excellent
Delay	<150 ms	Good
Availability	>99%	Excellent

The data presented in Table 2 summarize the system's performance during normal operation. The observed throughput ranged from 70% to 90% of link capacity, indicating efficient bandwidth utilization without overloading. The packet loss remained at 0%, confirming stable transmission across all monitored routes. The average delay was recorded below 150 ms, which aligns with the ITU-T QoS standards for satisfactory data communication performance. Finally, the device availability exceeded 99%, signifying minimal downtime and consistent operational reliability. Collectively, these outcomes affirm that the system achieved optimal network performance under standard conditions.

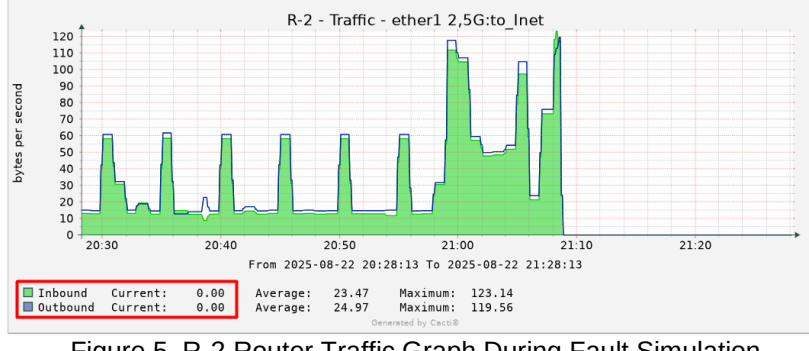

Figure 5. R-2 Router Traffic Graph During Fault Simulation

Figure 5 illustrates the traffic graph of router R-2 following a fault simulation, in which the interface ether1 was intentionally disconnected. The traffic pattern exhibited an immediate drop to zero, indicating a clear disruption along that link. Cacti's ability to visualize this event in real time allowed prompt identification of the fault's location and nature. This capability significantly reduces the time required for troubleshooting compared to manual inspection methods. The findings demonstrate that the SNMP–Cacti integration effectively detects both normal and abnormal network conditions, accurately distinguishing between stable and faulty states. By offering segmented visual data per interface, the system enables administrators to isolate issues rapidly and implement corrective measures. Compared with alternative monitoring platforms such as Zabbix or Nagios, the SNMP–Cacti configuration provided a more streamlined and quantifiable analysis of key parameters—throughput, delay, packet loss, and availability—making it not only a monitoring solution but also a reliable diagnostic and performance assessment tool. These results reinforce earlier findings by Lebiednik *et al*. (2019) and Sari & Putra (2020), underscoring Cacti's capability to deliver efficient, scalable, and analytically robust network monitoring.

4. Discussion

The integration of the Simple Network Management Protocol (SNMP) with the Cacti monitoring platform in an enterprise network simulation demonstrated a high degree of accuracy and reliability in tracking performance metrics. The system successfully visualized network behavior under both normal and faulty conditions, allowing administrators to identify and interpret network anomalies efficiently. This finding aligns with the observations of Purnomo *et al*. (2022), who emphasized that an effective network monitoring system must provide timely detection and visualization of faults to minimize downtime. The graphical and tabular outputs produced by Cacti simplified network diagnosis and supported rapid decision-making—an essential capability in enterprise environments where operational continuity is critical (Pradana *et al*., 2022). From an analytical perspective, the real-time visualization feature of Cacti proved advantageous in diagnosing performance degradation. Administrators could directly observe abnormal patterns without performing manual inspections on each device, thereby shortening response time and reducing the potential impact on Quality of Service (QoS).

These results are consistent with ETSI (2000) standards, which classify performance based on throughput, delay, packet loss, and availability. The findings also corroborate the conclusions of Prasetyo and Nugroho (2021), who reported that SNMP-based monitoring frameworks improve operational efficiency by automating the process of data collection and network analysis. Comparative studies underscore the unique strengths of the SNMP–Cacti integration when measured against other monitoring tools such as Zabbix and Nagios. While Zabbix offers advanced notification features, its configuration complexity can be challenging, particularly in large-scale networks (Husna & Rosyani, 2021; Ishaq & Firmansyah, 2023). In contrast, Cacti's reliance on SNMP and RRDTool provides a simpler yet equally effective monitoring process (Oetiker, 2015; Cacti Group, 2023; Sari & Putra, 2020). Rahma *et al*. (2023) demonstrated that Zabbix is well-suited for server monitoring, but Cacti's graphical interface and lightweight resource demands make it more suitable for continuous performance evaluation in enterprise environments. Similarly, Sari, Safrianti, and Jalil (2023) highlighted the importance of visualization in bandwidth monitoring systems, reinforcing the practicality of tools like Cacti for maintaining performance efficiency in digital industries. Lebiednik, Nowak, and Wróbel (2019) also found Cacti to outperform heavier solutions in terms of scalability and resource optimization, further validating its use in complex network infrastructures.

The system's performance results—throughput between 70–90% of link capacity, zero packet loss, latency below 150 ms, and availability exceeding 99%—confirm that SNMP-Cacti monitoring meets enterprise-level reliability requirements. These metrics correspond with the ITU-T and TIPHON QoS standards (ETSI, 2000) and demonstrate the system's capability to maintain stable service under varying network loads. Furthermore, the automated data collection through SNMP polling supports Khan and Khan's (2018) argument for real-time, self-reporting network systems that reduce administrative workload and enhance operational oversight. When a simulated fault was introduced by disabling interface *ether1* on router R-2, the system immediately detected and displayed a traffic drop to zero, allowing administrators to pinpoint the issue visually. This responsiveness aligns with the real-time anomaly detection principles outlined by Ishaq and Firmansyah (2023), who noted that integrating communication platforms such as Telegram could further enhance response times. Although the current study did not incorporate external notification systems, the graphical data generated by Cacti provided sufficient early warning to support proactive troubleshooting. Such responsiveness also mirrors the recommendations of Nagios Enterprises (2022) and Zabbix LLC (2022), which

emphasize the importance of continuous polling and alert-based reporting in enterprise-grade monitoring systems.

The controlled simulation environment using PNETLab provided a practical and secure platform for system evaluation, yet deploying the same configuration in live enterprise networks would present new challenges. As noted by Rahma *et al*. (2023), implementing monitoring systems in production environments requires more granular configurations to accommodate organizational variability. Similarly, scalability testing under higher traffic volumes—as recommended by Sari *et al*. (2023)—should be explored to verify system robustness under peak operational loads. Future research should therefore focus on extending the implementation to real-world infrastructures, integrating advanced SNMP versions such as SNMPv3 for enhanced security (Stallings, 2013), and coupling Cacti with automated notification or predictive analysis tools based on machine learning algorithms.Overall, the results validate that SNMP–Cacti integration provides a practical, low-overhead, and analytically sound monitoring solution for enterprise networks. It effectively bridges the gap between raw network statistics and actionable operational insights. By combining standardized protocols (Cisco Systems, 2022) with efficient data visualization and storage mechanisms, this monitoring framework supports both technical scalability and organizational decision-making. Such findings reinforce the position of SNMP-Cacti as a reliable foundation for adaptive network management in evolving enterprise systems.

5. Conclusion

The implementation and evaluation of enterprise network performance monitoring using the Simple Network Management Protocol (SNMP) integrated with the Cacti application demonstrated the system's reliability and efficiency in capturing real-time network behavior. The integration enabled administrators to obtain accurate and measurable information on key performance indicators such as throughput, packet loss, delay, and availability. The graphical visualization produced by Cacti facilitated quantitative analysis of these parameters under both normal and fault conditions, allowing for precise identification of performance fluctuations and operational bottlenecks. The experimental results confirmed that, under normal conditions, the network maintained stable performance characterized by throughput levels ranging from 70–90% of link capacity, zero packet loss, latency below 150 milliseconds, and availability exceeding 99%. These values correspond to the *Good* and *Excellent* categories defined by the ITU-T/TIPHON Quality of Service (QoS) standards, affirming that SNMP–Cacti–based monitoring effectively supports consistent service quality within enterprise environments.

Moreover, the simulated fault scenario demonstrated Cacti's capability to detect network disruptions almost instantaneously and represent them through interface-specific traffic graphs. This functionality significantly improved troubleshooting efficiency, enabling administrators to isolate and resolve issues without conducting manual, device-by-device inspections. The ability to visually correlate anomalies with specific interfaces provides a practical diagnostic advantage that enhances network maintainability and reduces downtime. Overall, the findings validate that SNMP-based monitoring through Cacti is an effective, efficient, and scalable solution for enterprise network management. Its simplicity of configuration, low computational overhead, and real-time visualization make it a suitable tool for maintaining operational continuity and optimizing network reliability. Future development may focus on integrating SNMPv3 for enhanced data security and incorporating automated alert mechanisms or machine-learning–driven anomaly detection to further improve response times and predictive maintenance capabilities within complex network infrastructures.

Acknowledgment

The author expresses sincere gratitude to Allah SWT for His blessings and guidance, which have enabled the successful completion of this research. Appreciation is extended to Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika (STIKOM CKI) Jakarta for providing academic support and facilities throughout the study. The author also wishes to thank family members and colleagues for their continuous prayers, encouragement, and support during the research process. Without the assistance and cooperation of these individuals and institutions, this study would not have been successfully completed.

References

Cacti Group. (2023). *Cacti: The complete RRDTool-based graphing solution.* Retrieved from https://www.cacti.net/

Cisco Systems. (2022). *Simple network management protocol configuration guide.* Cisco Documentation. Retrieved from https://www.cisco.com/

European Telecommunications Standards Institute (ETSI). (2000). *Telecommunications and internet protocol harmonization over networks (TIPHON): General aspects of quality of service (ETSI standard).*

Husna, M., & Rosyani, P. (2021). Implementasi sistem monitoring jaringan dan server menggunakan Zabbix yang terintegrasi dengan Grafana dan Telegram. *Jurikom (Jurnal Riset Komputer), 8*(6), 247–256. https://doi.org/10.30865/jurikom.v8i6.3631

Ishaq, M., & Firmansyah, F. (2023). Implementasi sistem monitoring menggunakan Zabbix dan notifikasi realtime Telegram. *Jurnal Insan: Journal of Information System Management Innovation, 3*(2), 72–77. https://doi.org/10.31294/jinsan.v3i2.2432

Khan, R., & Khan, S. (2018). Design and implementation of an automated network monitoring and reporting back system. *Journal of Industrial Information Integration, 9,* 24–34. https://doi.org/10.1016/j.jii.2017.11.001

Lebiednik, P., Nowak, R., & Wróbel, M. (2019). Performance evaluation of monitoring tools for enterprise networks. *International Journal of Computer Networks & Communications, 11*(4), 1–12. https://doi.org/10.5121/ijcnc.2019.11401

Nagios Enterprises. (2022). *Nagios core – Monitoring.* Retrieved from https://www.nagios.org/

Oetiker, T. (2015). *RRDtool: Round robin database tool.* Retrieved from https://oss.oetiker.ch/rrdtool/

Pradana, A., Widiasari, I., & Efendi, R. (2022). Implementasi sistem monitoring jaringan menggunakan Zabbix berbasis SNMP. *AITI: Jurnal Teknologi Informasi, 19*(2), 248–262. https://doi.org/10.24246/aiti.v19i2.248-262

Prasetyo, D., & Nugroho, Y. (2021). Analisis kinerja jaringan menggunakan SNMP dan Zabbix pada infrastruktur enterprise. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 8*(2), 215–223. https://doi.org/10.25126/jtiik.2021821523

Purnomo, P., Nugroho, M., Kabes, M., Putra, S., & Fathanah, J. (2022). Sistem pemantauan jaringan data di stasiun bumi LAPAN. *Format: Jurnal Ilmiah Teknik Informatika, 11*(1), 33–44. https://doi.org/10.22441/format.2022.v11.i1.004

Rahma, A., Indriyani, F., & Sandi, T. (2023). Perancangan dan implementasi monitoring perangkat server menggunakan Zabbix pada PT. Rizki Tujuh Belas Kelola. *Jurnal Insan: Journal of Information System Management Innovation, 3*(2), 85–95. https://doi.org/10.31294/jinsan.v3i2.3009

Sari, L., Safrianti, E., & Jalil, F. (2023). Rancang bangun sistem monitoring bandwidth server pada PT. Industri Kreatif Digital. *Malcom: Indonesian Journal of Machine Learning and Computer Science, 3*(2), 168–179. https://doi.org/10.57152/malcom.v3i2.914

Sari, M., & Putra, A. (2020). Implementasi network monitoring system menggunakan Cacti. *Jurnal Sistem Informasi dan Teknologi (JSIT), 9*(1), 45–54.

Stallings, W. (2013). *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2* (3rd ed.). Addison-Wesley.

Zabbix LLC. (2022). *Zabbix documentation 6.0 LTS.* Retrieved from https://www.zabbix.com/