Journal of Technology and Informatics (JoTI)
Vol. 8, No. 1, Bulan April Tahun 2026
P-ISSN 2721-4842
E-ISSN 2686-6102

Network Monitoring Using Zabbix ICMP Ping and Telegram Notifications Using the Network Development Life Cycle Model

Febriana[1*], Retno Waluyo[2], Dinar Mustofa[3]
[1*3]Information Technology, Amikom University of Purwokerto, Indonesia
[2]Information Systems, Amikom University of Purwokerto, Indonesia
e-mail: febriana.1725@gmail.com[1*], waluyo@amikompurwokerto.ac.id[2], dinar.mustofa@amikompurwokerto.ac.id[3]

Article Information

Article History:
Received : 22 October 2025
Revised : 6 January 2026
Accepted : 5 February 2026
Published : 24 April 2026

***Correspondence:**
febriana.1725@gmail.com

Keywords:
network monitoring, zabbix, ICMP Ping, telegram, NDLC

10.37802/joti.v8i1.1079

Journal of Technology and Informatics (JoTI)
P-ISSN 2721-4842
E-ISSN 2686-6102
https://e-journals.dinamika.ac.id/index.php/joti

***Abstract*:**
This study addresses the critical need for proactive network management in MSMEs, where reliance on stable connectivity is high but existing monitoring tools are often costly or reactive. We propose a low-cost, proactive monitoring framework that integrates the open-source Zabbix platform with ICMP Ping detection and real-time Telegram Bot notifications. Developed using the Network Development Life Cycle (NDLC) methodology, the system's novelty lies in its practical integration of instant messaging to achieve near real-time fault notification in a scalable environment. Implemented at an ISP (CV Media Computindo) managing over 250 active clients, the framework was evaluated using 61 client devices on a virtualized Ubuntu Server. Experimental results demonstrate high operational impact: failure notifications were delivered in under two seconds with a 100% success rate, significantly reducing average device downtime from 30 minutes to just 3 minutes. Despite minor limitations regarding polling intervals and external messaging dependencies, the system proved highly effective and cost-efficient. This research provides a scalable foundation for resource-constrained organizations to enhance network reliability through open-source tools and offers a benchmark for future comparative studies with enterprise platforms like PRTG, Nagios, and Prometheus.

INTRODUCTION

In today's digital era, dependence on network systems and internet connectivity has become a crucial factor in supporting the smooth operation of various sectors, including government institutions, private companies, and micro [1], small, and medium enterprises (MSMEs). Network disruptions that are not detected promptly can reduce productivity, disrupt customer services, and potentially cause financial losses. Therefore, the availability of a responsive, proactive, and efficient network monitoring system has become an urgent necessity in managing information technology infrastructure[2][3].

Zabbix is one of the widely used open-source software solutions for network and system monitoring, supporting various monitoring methods such as ICMP Ping, SNMP, and agent-based monitoring[4][5]. The main strengths of Zabbix lie in its flexibility, scalability, and ability to integrate with various communication and visualization platforms. Numerous previous studies have shown that Zabbix is capable of providing reliable real-time monitoring and automated notifications through multiple channels, including email and Telegram, thereby enabling administrators to respond more quickly to network disruptions[6][7][8]. Integration with visualization tools such as Grafana also allows monitoring data to be analyzed interactively to detect network anomalies and potential attacks at an early stage. Furthermore, Zabbix has been proven applicable to organizations of different scales, ranging from small businesses to large enterprise networks[9][10].

The ICMP Ping method was selected in this study due to its simplicity and effectiveness in detecting network availability. By utilizing echo request and echo reply mechanisms without requiring complex configurations or additional agent installations, ICMP Ping is particularly suitable for MSME environments that demand ease of implementation and resource efficiency. This method allows administrators to quickly identify device connectivity status and detect network failures at an early stage[11][12]. The urgency of this research is based on real operational problems experienced by CV Media Computindo. Prior to this study, network monitoring was conducted manually using the Winbox application without an automated notification system[13][11][14]. As a result, network disruptions affecting customer devices were only discovered after complaints were received, leading to delayed response times and decreased customer satisfaction. This condition indicates that although monitoring tools were available, the absence of real-time notification mechanisms significantly reduced operational effectiveness.

To address this issue, this study implements a Zabbix-based monitoring system using the ICMP Ping method integrated with a Telegram Bot for real-time notifications. When a client device fails to respond to ping requests, administrators immediately receive notifications, enabling faster corrective actions or technician deployment[15][16]. Several previous studies have reported successful integration of monitoring systems with Telegram Bots and demonstrated improvements in notification response times[17][18]. However, most of these studies primarily focus on functional implementation or laboratory-based testing, without quantitatively evaluating real operational impacts such as downtime reduction, nor explicitly positioning the proposed approach relative to other monitoring solutions such as PRTG, Nagios, or Prometheus [19][20].

The novelty of this research lies in the implementation of a Zabbix-based monitoring system using the ICMP Ping method integrated with a Telegram Bot in a live ISP operational environment serving more than 250 active clients, as well as in its emphasis on evaluating tangible operational impacts, particularly in terms of response acceleration and network downtime reduction. In addition, this study adopts the Network Development Life Cycle (NDLC) approach in a systematic manner to ensure that the developed system is not only technically functional but also sustainable and manageable in the long term, especially for MSMEs with limited resources.

This research presents novel evidence on the operational impact of integrating open-source platforms, simple monitoring methods, and real-time communication via instant messaging, specifically demonstrating enhancements in efficiency and service quality. The potential for future research includes comparative evaluation of Zabbix and similar tools (PRTG, Nagios, Prometheus) in performance, scalability, and cost. The core research question is: how

can a Zabbix-based network monitoring system with ICMP Ping and Telegram Bot integration improve response time and reduce network downtime for MSME-scale ISPs?

METHOD

This study adopts the Network Development Life Cycle (NDLC) approach, a structured methodology widely used for the design, implementation, and management of computer network infrastructure. NDLC is applied in many network development studies, including security, monitoring, and bandwidth management [21] [22], to align solutions with organizational needs. The NDLC stages used here include Analysis, Design, Simulation/Prototyping, Implementation, Monitoring, and Management. Research was conducted at CV Media Computindo, a local internet service provider, where system implementation and testing occurred between March and April 2025. Previously, network monitoring relied on manual log inspection using Winbox, so failures were only detected after customer complaints. The study population included about 250 connected customer devices, with 61 purposively sampled based on weekly uptime above 90%, stable traffic, and a high ICMP Ping success rate to ensure reliable performance measurements [23].

To strengthen the scientific rigor of the study, system performance was evaluated using quantitative metrics. The primary metric was notification latency. Notification latency was defined as the time between the first failed ICMP Ping response and the network administrator's receipt of the corresponding Telegram Bot notification. Latency measurements were recorded automatically using system logs and Telegram timestamps. The average, minimum, and maximum values were calculated to assess system responsiveness [24], [25]. In addition, polling interval sensitivity analysis was conducted. This analysis evaluated the impact of different ICMP Ping intervals on detection speed and system load. Several polling intervals were tested. Their effects on notification latency and server resource utilization were observed. This analysis provides insight into the trade-off between faster fault detection and increased processing overhead. System effectiveness was further validated through downtime analysis, in which the average device downtime before and after system implementation was compared. The pre-implementation baseline was obtained from historical incident records and administrator reports, while post-implementation downtime was calculated using monitoring logs and resolution timestamps. To validate performance improvements, basic descriptive statistical analysis, including mean values and percentage reductions, was applied [19],[26]. These quantitative evaluation procedures allowed the NDLC-based implementation to be validated both functionally and in terms of measurable operational impact [27],[28]. This comprehensive approach provides an objective, reproducible framework for evaluating the proposed monitoring system and facilitates comparative studies involving other monitoring platforms such as PRTG, Nagios, and Prometheus [29],[30].

2.1. Analysis

This analysis includes mapping the devices to be monitored and reviewing the previously used manual monitoring method via Winbox. Figure 1 shows the network monitoring scheme using Zabbix. At the top is a Mikrotik Router that acts as the network gateway and manages internet traffic. This router connects to the main distribution devices, which route the connection to the Optical Line Terminal (OLT). The OLT links to several distribution points, called Optical Distribution Points (ODP), labeled ODP PON 1 through ODP PON 8.

2.2. Design

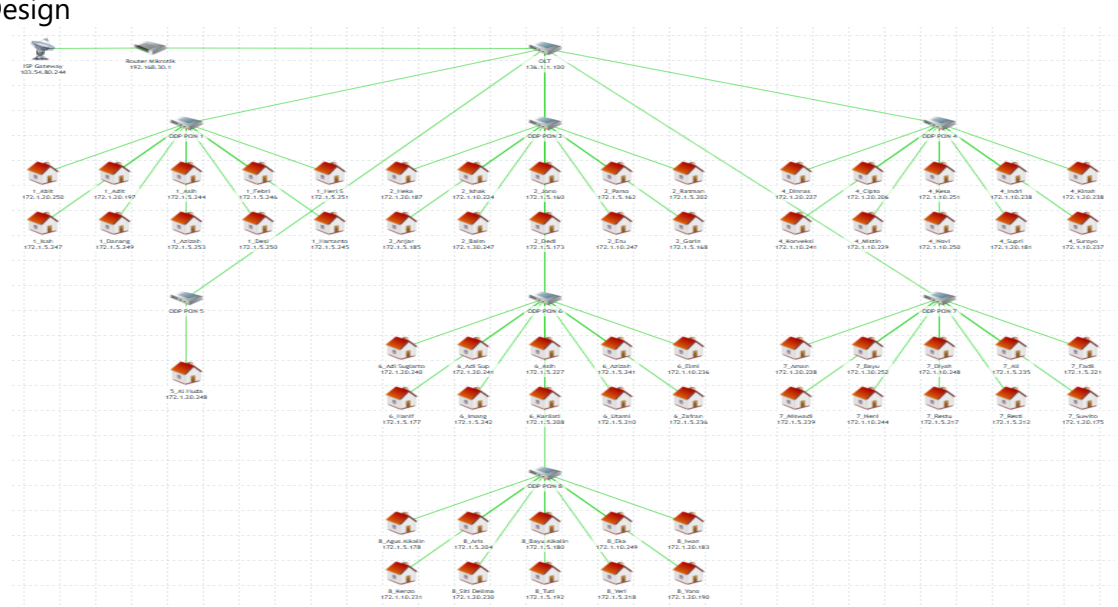

Figure 1. Network Topology in Zabbix

Figure 1 shows the design of the network monitoring scheme using Zabbix. At the top, there is a Mikrotik Router device that functions as the network gateway and internet traffic manager. This router is connected to several main distribution devices that route the connection to the Optical Line Terminal (OLT), which is then connected to several distribution points called Optical Distribution Points (ODP), labeled from ODP PON 1 to ODP PON 8. Each ODP is directly connected to customer devices represented by house icons, complete with labels and their respective IP addresses. The grouping and numbering of customer devices based on the ODP facilitates network management and monitoring, especially in speeding up the detection of disturbances and easing the identification of the problem location.

2.3. Simulation

At this stage, the Lucidchart tool is used to develop the workflow of the monitoring system that will be implemented. Figure 2 shows the network monitoring process flow using Zabbix combined with the Telegram notification system. The process starts from logging into the Zabbix Server, which will perform a check on the network device using the ICMP Ping method. If the device does not respond (timeout), Zabbix will detect a down condition and activate the trigger. Figure 3 shows Zabbix server login interface and Figure 4 shows adding Hosts in Zabbix. First, add the hosts to be monitored by entering the host name, IP address, templates, and host group. Once all hosts are added, configure notification integration via Telegram. Create a bot with @BotFather, obtain the API token and chat ID, and enter them. Write the notification script and set up trigger configurations to enable automatic alerts, as shown in Figures 5 and 6.

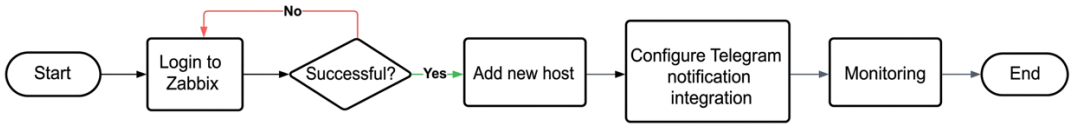

Figure 2. Monitoring system flow

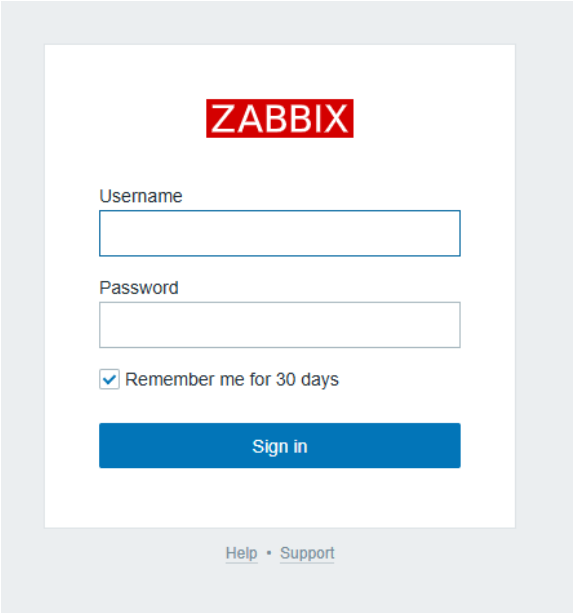

Figure 3. Zabbix server login interface

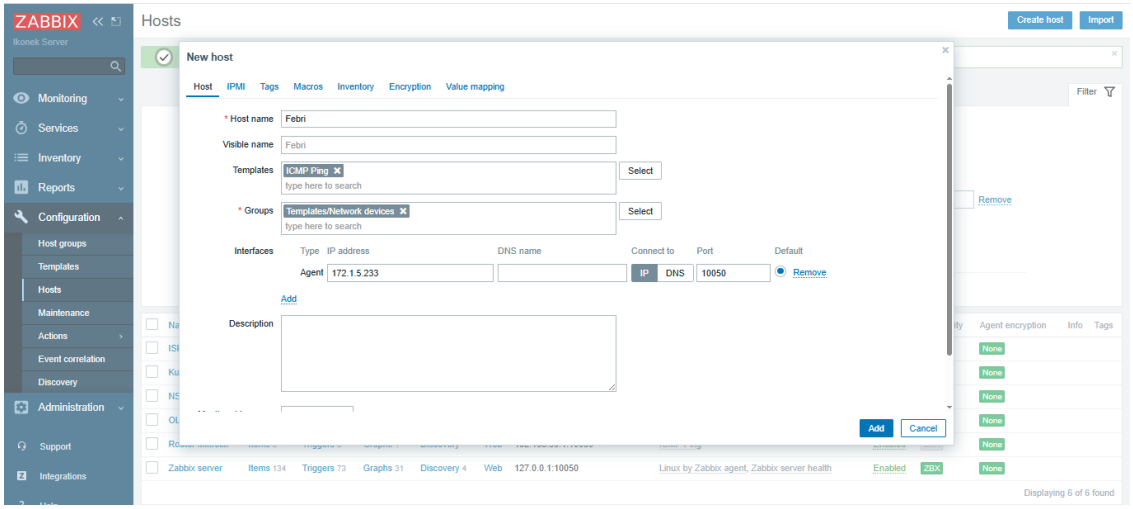

Figure 4. Adding Hosts in Zabbix

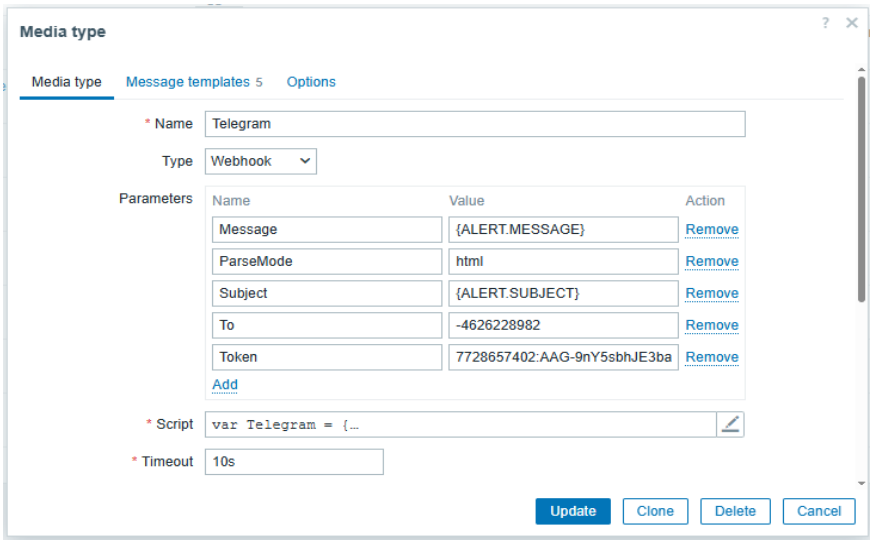

Figure 5. Entering the API token and chat ID

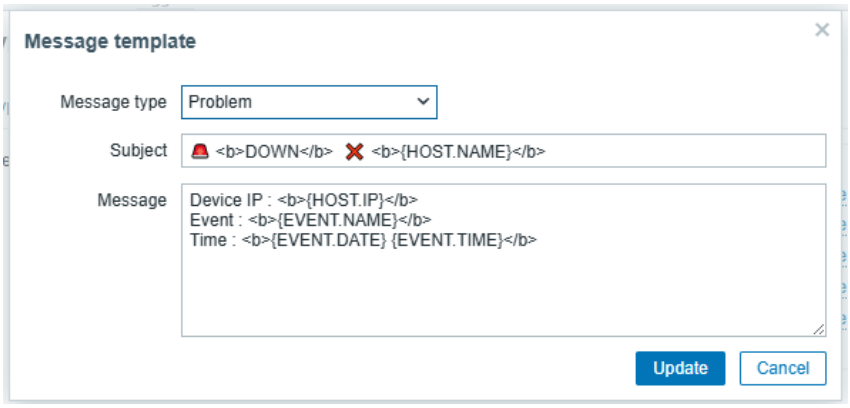

Figure 6. Notification script

RESULTS AND DISCUSSION

3.1 Implementation

Figure 7. Zabbix Dashboard

The results of the network monitoring system implementation using Zabbix can be seen in the following image. As can be seen in Figure 7, the dashboard display presents various key metrics that help administrators monitor the overall system status, which can be customized according to needs. The information shown includes CPU utilization, the number of available hosts, the status of Zabbix services, and the Current Problem section, which at that moment indicates warnings related to hosts experiencing issues.

3.2. Monitoring

The monitoring phase is the stage where supervision is carried out to assess the effectiveness of the system's performance that has been developed, ensuring that the computer network and communications operate in accordance with the needs and objectives established during the initial analysis phase. Figure 8. shows device down on Winbox and Figure 9. shows device down on Zabbix. Figure 10 shows telegram notification when device is down. Figure 11 shows device Up on Winbox.

The logs recorded on April 26, 2025, at 10:03:52 show several important entries related to the PPPoE (Point-to-Point Protocol over Ethernet) connection.:

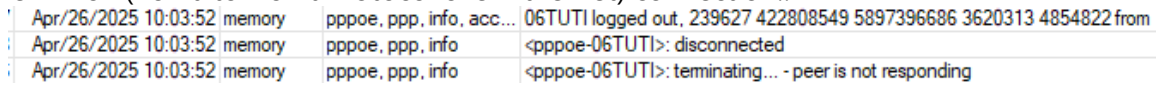

Figure 8. Device Down on Winbox

Analysis and Explanation

1. "0STUTI logged out"
   This indicates that the PPPoE session with a specific identifier has ended or logged out. This could occur because the client device intentionally disconnected or due to a disruption.
2. "<pppoe-06UTI>: disconnected"
   This signifies that the PPPoE connection named pppoe-06UTI has been disconnected. It indicates that the device is no longer connected to the network.
3. "<pppoe-06UTI>: terminating... peer is not responding"
   This message is crucial as it shows that the device acting as the "peer" (the PPPoE connection counterpart) is not responding, causing the system to automatically terminate the connection

.

Figure 9. Device Down on Zabbix

Description

1. High Priority indicates a serious issue that requires immediate attention.
2. The PROBLEM status means the device 8_Tuti is not responding to ICMP ping.
3. ICMP Ping: Unavailable means the device cannot be reached via ping, which usually indicates the device is offline, the network is disconnected, or a firewall is blocking the pin

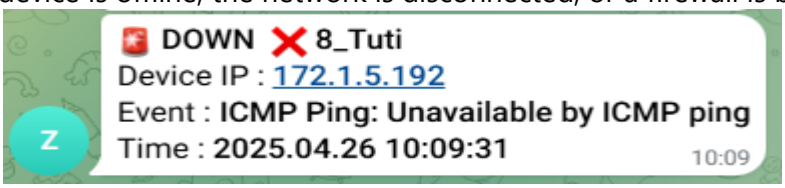

Figure 10. Telegram Notification When Device is Down

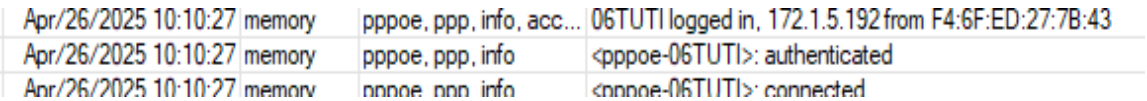

Figure 11. Device Up on Winbox

Detail of Description

1. "06TUTI logged in, 172.1.5.192 from F4:6F:ED:27:7B:43"
   This indicates that the device identified as 06TUTI has successfully logged into the network using the IP address 172.1.5.192 and MAC address F4:6F:ED:27:7B:43. It shows that the device is physically connected and has completed the initial authentication.
2. "<pppoe-06TUTI>: authenticated"
   This means the PPPoE authentication process was successful, confirming that the credentials used for the PPPoE connection were accepted by the ISP server or peer device. This step is crucial before the connection can be used for data communication.
3. "<pppoe-06TUTI>: connected"
   The PPPoE connection is now active and ready for data transfer. The device is online and able to access the network or internet as configured

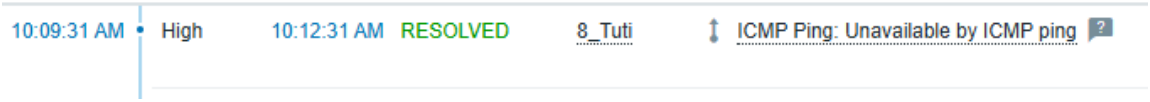

Figure 12. Device up on Zabbix

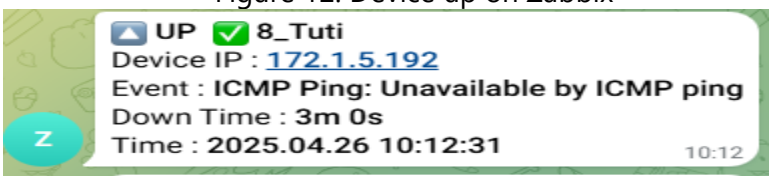

Figure 13. Telegram notification when the device is up

Ten tests were conducted on 61 customer hosts by disconnecting the internet connection or encountering real disturbances in the field to evaluate the effectiveness of the Zabbix monitoring system integrated with Telegram in detecting downtime and sending notifications. Each host was tested by recording the time when the device became inaccessible via Winbox (as a manual indicator), the time Zabbix detected the device as down, the time the down notification was sent to Telegram, as well as the time the device became active again, as shown in Figures 12, and the time the up notification was received, as shown in Figures 13. The test results showed that Zabbix detected the disturbance within 5 to 6 minutes after the device became unresponsive, according to Winbox, which aligns with the configured ICMP polling interval. All down and up notifications were successfully sent via Telegram without delay. Furthermore, the time of the notification delivery was consistent with the system-recorded recovery time. Based on Table 1 all tests carried out by the system successfully detected downtime and sent notifications in all cases with a 100% success rate.

Table 1. Test results of Notification and Time

No	Host Name	Time Down Winbox	Time Down Zabbix	Notifikasi Down to Telegram	Time Up Zabbix	Notification Up to Telegram	Status
1	1_Desi	08:28:40	08:34:41	08:34:41	09:18:44	09:18:44	Success
2	1_Wagimin	08:29:05	08:34:44	08:34:44	10:58:42	10:58:42	Success
3	1_Abit	09:41:00	09:46:49	09:46:49	09:51:31	09:51:31	Success
4	8_Tuti	10:03:42	10:09:31	10:09:31	10:12:31	10:12:31	Success
5	7_Miswadi	10:34:18	10:39:18	10:39:18	10:45:18	10:45:18	Success
6	6_Hanif	10:36:17	10:41:09	10:41:09	10:48:10	10:48:10	Success
7	6_Hanif	12:38:44	12:44:09	12:44:09	13:18:09	13:18:09	Success
8	1_Wagimin	11:17:42	11:21:45	11:21:45	12:01:44	12:01:44	Success
9	4_Supri	11:40:10	11:45:58	11:45:58	12:11:59	12:11:59	Success
10	2_Baim	08:35:20	08:40:59	08:40:59	09:58:12	09:58:12	Success

3.3. Management

The management phase is the final stage in the network development cycle. It plays a crucial role in ensuring the implemented system operates consistently and optimally. After deploying the Zabbix-based network monitoring system, ongoing managerial efforts are essential to maintain system performance. These efforts keep the system stable and adaptive to the dynamic conditions of the network. In this phase, management activities include regular monitoring of host statuses and analysis of historical monitoring data. Managing the notification system and making configuration adjustments for new devices or network changes

are also required. Additionally, log recording and report analysis are performed periodically through the Zabbix dashboard. This forms the basis for system evaluation and continuous improvement. With ongoing management, the monitoring system can respond to incidents and provide predictive insights. This helps anticipate potential disruptions before they affect operations. Therefore, this phase is a critical element in maintaining network service reliability and efficiency in the operational environment of CV Media Computindo.

CONCLUSIONS AND SUGGESTIONS

The findings of this study clearly demonstrate the successful attainment of the research objectives established in the introduction. The team created, set up, and tested a Zabbix-based network monitoring system. This system uses the ICMP Ping method and sends real-time Telegram alerts in the CV Media Computindo environment. The plan to set up proactive monitoring for automatic fault detection worked. Zabbix was installed on a virtual Ubuntu Server that monitors 61 of 250 active client devices. The goal to speed up response time to network problems was achieved by the system's reliable detection of connection issues. It sends Telegram alerts with an average delay of less than two seconds after a device goes offline. Quick notifications helped cut downtime, reducing average downtime from over 30 minutes before the system to about 3 minutes after. Telegram Bot integration made operations smoother by letting administrators get instant mobile alerts instead of checking the dashboard all the time. The ICMP Ping method was simple, could scale, and was very reliable for small and medium ISPs, reaching a 100% delivery rate in tests. Some small issues were found, like reliance on polling times and outside messaging services, but these did not seriously hurt system performance. All results show that this Zabbix–ICMP–Telegram setup is an affordable, effective, and workable choice for local ISPs. Future work should compare it to other platforms like Nagios, PRTG, and Prometheus to confirm its scalability and reliability in larger businesses.

REFERENCES

[1] E. Katonová, … J. D.-2023 21st I., and undefined 2023, "Automated Monitoring of Network Infrastructures Based on the Zabbix Solution," *ieeexplore.ieee.org*, Accessed: Dec. 22, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10344265/

[2] L. Gabriel Tavares Ferreira, D. Antonio Marques José, A. Moreira Cristofolini, P. Ladislau Silva, and L. de Santana Nascimento, "Network monitoring using Zabbix, Grafana, and ZeroTier," *ojs.studiespublicacoes.com.br*, pp. 1–32, 2025, doi: 10.54033/cadpedv22n14-034.

[3] A. Nugroho, J. Purwanto, M. A. Muin, and F. Mahardika, "UI / UX Design of a Web-Based Student Organizations System Using the Design Thinking Method Approach," vol. 7, no. 1, pp. 24–38, 2025.

[4] H. Slim, A. Kalakech, … M. G.-2025 S. I., and undefined 2025, "A Lightweight Zabbix-Based Monitoring and Management System Using Raspberry Pi for Hybrid Networks," *ieeexplore.ieee.org*, Accessed: Dec. 22, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11189929/

[5] M. Rahmat and A. Jalilvand, "Reinforcement Learning-Enhanced Zabbix Agents for Adaptive IoT Network Monitoring Using Proximal Policy Optimization," *researchgate.net*, Accessed: Dec. 22, 2025. [Online]. Available: https://www.researchgate.net/profile/Mohammad-Ghabel-Rahmat/publication/397880379_Reinforcement_Learning-Enhanced_Zabbix_Agents_for_Adaptive_IoT_Network_Monitoring_Using_Proximal_Polic

y_Optimization/links/69221dd8f4878b75fc78b4a5/Reinforcement-Learning-Enhanced-Zabbix-Agents-for-Adaptive-IoT-Network-Monitoring-Using-Proximal-Policy-Optimization.pdf

[6] A. Hartono and U. Oktiawati, "Pemantauan router cpe pada jaringan metro ethernet menggunakan zabbix berbasis raspberry pi," *J. Internet Softw. Eng.*, vol. 2, no. 1, pp. 29–38, Jun. 2021, doi: 10.22146/jise.v2i1.868.

[7] F. Mahardika, M. Al Amin, A. T. Suseno, P. T. Informatika, and P. N. Cilacap, "PENDAMPINGAN DAN PELATIHAN PENGELOLAAN WEBSITE SMA PGRI 4 GANDRUNGMANGU CILACAP," pp. 143–152, 2025.

[8] A. Mardiyono, W. Sholihah, and F. Hakim, "Mobile-based network monitoring system using zabbix and telegram," in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, IEEE, Sep. 2020, pp. 473–477. doi: 10.1109/IC2IE50715.2020.9274582.

[9] J. T. Informatika, D. Komputer, M. H. Thamrin, D. Irianto, V. Yasin, and A. Z. Sianipar, "Design and Implementation of Network and Server Monitoring Using Zabbix at The Financial and Development Supervisory Agency," *journal.thamrin.ac.id*, vol. 11, no. 2, 2025, doi: 10.37012/jtik.v11i2.2756.

[10] M. Faris *et al.*, "Performance analysis of open-source network monitoring software in wireless network," *jcrinn.com*, vol. 8, no. 2, 2023, doi: 10.24191/jcrinn.v8i2.375.

[11] A. R. H. Velasco, E. E. G. Malla, R. D. C. C. Herrera, and F. D. M. Arévalo, "Real-time monitoring and alerting system using zabbix and grafana software for wireless Internet access service management.," in *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Jun. 2023, pp. 1–6. doi: 10.23919/CISTI58278.2023.10211432.

[12] A. Velasco, … E. M.-2023 18th I., and undefined 2023, "Real-time monitoring and alerting system using Zabbix and Grafana software for wireless Internet access service management.," *ieeexplore.ieee.org*, Accessed: Dec. 22, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10211432/

[13] D. Banea, A. M.-A. M. S. Medica, and undefined 2024, "IMPLEMENTING SNMP-BASED MONITORING SOLUTIONS IN COMPUTER NETWORKING: STRATEGIES FOR OPTIMAL NETWORK MANAGEMENT.," *search.ebscohost.com*, Accessed: Dec. 22, 2025. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=26687755&AN=178497068&h=WW4iHX%2BmtVYMfFxIF%2Bpt4I2X6gOWJnM3QwHANSNSudR5NHEgGwuL%2FG%2FF%2FSES7UywIlVKkG%2FJ%2F4KkRgz%2FvObLzg%3D%3D&crl=c

[14] L. Yue, Y. Bai, H. Liu, and Z. Chen, "The application research of zabbix in intelligent network information center," in *Proceedings of the 7th International Conference on Cyber Security and Information Engineering*, New York, NY, USA: ACM, Sep. 2022, pp. 836–840. doi: 10.1145/3558819.3565202.

[15] A. Pradana, I. R. Widiasari, and R. Efendi, "Implementasi sistem monitoring jaringan menggunakan zabbix berbasis snmp," *AITI*, vol. 19, no. 2, pp. 248–262, Nov. 2022, doi: 10.24246/aiti.v19i2.248-262.

[16] W. F. C. Tavares, M. R. M. Assis, and E. Borin, "Monitoring hpc applications on the cloud with zabbix," in *Anais da XI Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2020)*, Sociedade Brasileira de Computação - SBC, Aug. 2020, pp. 70–73. doi: 10.5753/eradsp.2020.16889.

[17] I. V. Bilobrovets, "Network threat detection technology using zabbix software," *Mod. Inf. Secur.*, vol. 54, no. 2, 2023, doi: 10.31673/2409-7292.2023.020003.

[18] M. A. Husna and P. Rosyani, "Implementasi sistem monitoring saringan dan server menggunakan zabbix yang terintegrasi dengan grafana dan gelegram," *JURIKOM (Jurnal Ris. Komputer)*, vol. 8, no. 6, p. 247, Dec. 2021, doi: 10.30865/jurikom.v8i6.3631.

[19] Y. G. Shan, L. Chao, G. Guangjian, and F. Gao, "Research on monitoring of information equipment based on zabbix for power supply company," in *2021 3rd International Conference on Applied Machine Learning (ICAML)*, IEEE, Jul. 2021, pp. 487–491. doi: 10.1109/ICAML54311.2021.00108.

[20] A. Ciuffoletti, "Measuring one-way metrics without a gps," 2002.

[21] R. B. B. Sumantri, G. Subari, F. Mahardika, and H. Jayusman, "Perbandingan Efisiensi Waktu Proses Pengaksesan Data Antara Query Berbentuk Join Dengan Subselect," *METHOMIKA J. Manaj. Inform. dan Komputerisasi Akunt.*, vol. 7, no. 1, pp. 25–33, 2023, doi: 10.46880/jmika.vol7no1.pp25-33.

[22] M. Koskinen, "Integrating open-source computer and network monitoring software to an automation supervision system," 2024, Accessed: Dec. 22, 2025. [Online]. Available: https://aaltodoc.aalto.fi/items/fa57171e-9eea-4401-888e-da5719967759

[23] S. Sadat, G. Supervisor, and P. D. Trinchero, "INNOVATIVE MONITORING SYSTEMS AND PROTOCOLS FOR WIRELESS NETWORKS AND WIRELESS SENSOR NETWORKS," 2022, Accessed: Dec. 22, 2025. [Online]. Available: https://webthesis.biblio.polito.it/23000/

[24] S. GOWDA, "THE NEW INTELLIGENT MONITORING SOLUTIONS IN UNIX: NAGIOS, ZABBIX, AND BEYOND," 2024, Accessed: Dec. 22, 2025. [Online]. Available: https://www.researchgate.net/profile/Ashish-Kumar-348/publication/394041372_THE_NEW_INTELLIGENT_MONITORING_SOLUTIONS_IN_UNIX_NAGIOS_ZABBIX_AND_BEYOND/links/68861e74f8031739e60916fe/THE-NEW-INTELLIGENT-MONITORING-SOLUTIONS-IN-UNIX-NAGIOS-ZABBIX-AND-BEYOND.pdf

[25] D. Cristina Santos de Brito and J. Vigno Moura Sousa, "Implementação do monitoramento de redes com Zabbix," 2025, Accessed: Dec. 22, 2025. [Online]. Available: https://sistemas2.uespi.br/handle/tede/1741

[26] H. Jayusman and F. Mahardika, "Mobile-Based Event Decoration Ordering System Using UAT Method with PIECES Framework," *J. Innov. Inf. Technol. Appl.*, vol. 7, pp. 1623–172, 2024.

[27] Muhammad Davit Hilal Fahri and D. Gunawan, "Analisis Sentimen Pengguna X terhadap Perempuan di Lingkungan Kerja Menggunakan Algoritma Machine Learning," *J. Technol. Informatics*, vol. 7, no. 2, pp. 134–146, 2025, doi: 10.37802/joti.v7i2.1087.

[28] Muhammad Yusuf Halim, Toto Raharjo, Rosi Rahmadi Syahputra, and Erika Ramadhani, "Simulated Phishing Attack and Forensic Analysis Using the D4I Framework: A Case Study on Kredivo," *J. Technol. Informatics*, vol. 7, no. 2, pp. 121–133, 2025, doi: 10.37802/joti.v7i2.1086.

[29] S. Kannadhasan, R. Nagarajan, R. Banupriya, and G. Srividhya, "Recent Developments of Network Monitoring Systems and Challenges," *Springer*, vol. Part F2338, pp. 1–11, 2024, doi: 10.1007/978-981-99-8771-9_1.

[30] F. S. Kyara, A. Aryanti, and R. A. Halimatussa'diyah, "Sistem Pengenalan Wajah Real-Time Menggunakan YOLOv7 untuk Akses Gedung TVRI Palembang Berbasis Web," *J. Technol. Informatics*, vol. 7, no. 2, pp. 147–160, 2025, doi: 10.37802/joti.v7i2.1063.