PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 20, No. 2 September 2024 | DOI: 10.33480/pilar.v20i2.5535

INTEGRATION OF TELEGRAM BOT AND UPTIME KUMA FOR WI-FI NETWORK MONITORING USING MIKROTIK

Siti Nurjanah[1*]; Falentino Sembiring[2]; Rieska Rahayu Ayuningsih[3]

Information Systems[1, 2, 3]
Nusa Putra University, Sukabumi, Indonesia[1. 2. 3]
https://nusaputra.ac.id[1, 2, 3]
siti.nurjanah_si20@nusaputra.ac.id[1*], falentino.sembiring@nusaputra.ac.id[2], rieska.rahayu@nusaputra.ac.id[3]
(*) Corresponding Author

Abstract— *Wi-Fi network monitoring is a crucial aspect in ensuring the availability and security of widely used internet services. This research confirms the use of Telegram bots for notification integration with the Uptime-Kuma monitoring program and proxy devices for Wi-Fi network monitoring. The main router and network controller in this study were Mikrotik devices, while Uptime Kuma was used as a monitoring tool to track the performance and availability of the Wi-Fi network. When important events are discovered on the network, network administrators can receive quick notifications through integration with Telegram bots. In the context of Wi-Fi networks, the Security Policy Development Life Cycle (SPDLC) method is used to design relevant and effective security policies. It includes the stages of planning, implementation, monitoring, evaluation and regular updating of security policies to maintain optimal levels of security. The results show that the integration of Telegram bots with the Kuma Uptime monitoring tool can improve network availability. This allows quick reaction to Uptime and Downtime reports in network conditions, which record the percentage of time network services are available. Thus, administrators do not need to wait for complaints from users if the connection is suddenly lost, because changes in connection status will automatically send a notification to Telegram.*

Keywords: *mikrotik, security policy development life cycle, telegram bot, uptime kuma*

Abstract— *Monitoring jaringan Wi-Fi merupakan aspek krusial dalam memastikan ketersediaan dan keamanan layanan internet yang digunakan secara luas. Penelitian ini memastikan penggunaan bot Telegram untuk integrasi notifikasi dengan program pemantauan Uptime Kuma dan perangkat MikroTik untuk pemantauan jaringan Wi-Fi. Router dan pengontrol jaringan utama dalam penelitian ini adalah perangkat MIkrotik, sedangkan Uptime Kuma digunakan sebagai alat pemantauan untuk melacak kinerja dan ketersediaan jaringan Wi-Fi. Ketika ada peristiwa penting ditemukan di jaringan, administrator jaringan dapat menerima pemberitahuan cepat melalui integrasi dengan bot Telegram. Dalam konteks jaringan Wi-Fi, metode Security Policy Development Life Cycle (SPDLC) digunakan untuk merancang kebijakan keamanan yang relevan dan optimal. Ini mencakup tahap perencanaan, implementasi, pemantauan, evaluasi, dan pembaruan kebijakan keamanan secara teratur untuk menjaga tingkat keamanan yang optimal. Hasilnya menunjukkan bahwa integrasi bot Telegram dengan alat pemantauan Uptime Kuma dapat meningkatkan ketersediaan jaringan. Ini memungkinkan reaksi cepat terhadap laporan Uptime dan Downtime dalam kondisi jaringan, yang mencatat persentase waktu ketersediaan layanan jaringan. Dengan demikian, administrator tidak perlu menunggu adanya keluhan dari pengguna jika koneksi tiba-tiba terputus, karena perubahan status koneksi secara otomatis akan mengirimkan notifikasi ke Telegram.*

Kata Kunci: *mikrotik, security policy development life cycle, bot telegram, uptime kuma*

INTRODUCTION

The use of digital information technology in Indonesia continues to grow rapidly, reaching every corner of the country. This initiative is encouraged by the government to utilize digital information technology in various aspects, including increasing productivity and adding value to Micro, Small and Medium Enterprises (MSMEs) (Al Farisi, 2024). Currently, the internet has become a very important need because it has an impact on various aspects of daily life, from education to social interaction. To provide stable and quality internet connectivity,

competent internet services are needed (Utami, 2024).

Meanwhile, the use of Mikrotik devices as a network solution has become popular among MSMEs because of their reliability and affordable prices. However, managing Wi-Fi network security with Mikrotik devices often requires high levels of security monitoring (Safitri, A, & Prihantoro, 2024). Technological advances allow network devices to be accessed remotely. Usually, an administrator will log into the router to carry out network repairs and monitoring to detect attacks that enter the router (Kurnia & Juliandri, 2024). Mikrotik is a router operating system that has various features for network management. One of them is a router and firewall, as well as providing a hotspot service that allows the use of Wi-Fi technology in a WLAN wireless local network with a router that can connect to an internet service provider (ISP) (Kurniawan, 2024).

In this era, the need to identify and monitor networks is becoming increasingly important (Choudhari, Kurle, Nimbalkar, & Talekar, 2024). SINA.Net MSMEs often face various challenges in managing their networks, including limited human resources and lack of technical understanding. In addition, manually monitoring the network can cause delays in responsiveness in dealing with changes that occur in the network server environment in real-time. As a result, there are often deficiencies in network monitoring, proactive problem handling, and implementation of optimal security policies.

The open source Telegram bot provides a solution to this problem (Hafiz, Briliyant, Priambodo, Hasbi, & Siswanti, 2024)Telegram also considers itself to be the safest and fastest mass messaging application (Normadhoni, Dewanti, Namaskara, Akhadi, & Fauzi, 2021).The Telegram application also has advanced features, namely the Bot feature, meaning that Telegram bots can facilitate monitoring and provide automatic notifications of real-time network activity. Using Telegram Bot to improve the quality of customer complaint services can increase effectiveness in resolving problems and increase customer satisfaction(Arifin, 2024). While Uptime-Kuma provides the ability to continuously monitor network availability and performance. Functions to monitor the availability (uptime) of websites and online services (Lee, 2024).

In this research, the author combines the SPDLC concept with modern technology such as Telegram bots and Uptime Kuma to build an optimal Wi-Fi network monitoring system. Through case studies on the SINA.Net Wi-Fi network, we will provide a concrete picture of how this application can improve network security and optimize operational management.

Two related studies on network monitoring are included in the previous studies referenced in this section. First, research who designed a monitoring system to collect Mikrotik router monitoring data from The Dude using Telegram Chat_Bot. The researcher produced a fast solution to get real-time information about the condition of existing Mikrotik routers (Hakim & Nugroho, 2024). Second, research that discusses network security issues and the emergence of various threats that target network systems and communications. To overcome this, the Multivariate Statistical Network Monitoring (MSNM) monitoring method is used, a promising approach in detecting anomalies. The result is that a type of Denial of Service (DoS) attack that relies on authentication and its variations can be detected by the MSNM-Sensor (Soufiane, Magán-Carrión, Medina-Bulo, & Bouden, 2024).

From this research, there are similarities in providing notifications automatically, namely by using the Telegram Bot feature but not using the Kuma Uptime tool and using the same approach method and retrieving the objects under study. Meanwhile, the difference comes from case studies conducted in different locations. These findings show that Telegram bots and this method can be optimally applied in monitoring network server performance and security (Kurnia & Juliandri, 2024).

The innovation of this research lies in an approach that combines network monitoring technology such as Kuma Uptime with the use of Telegram bots to improve network security and availability in SINA.net MSMEs.

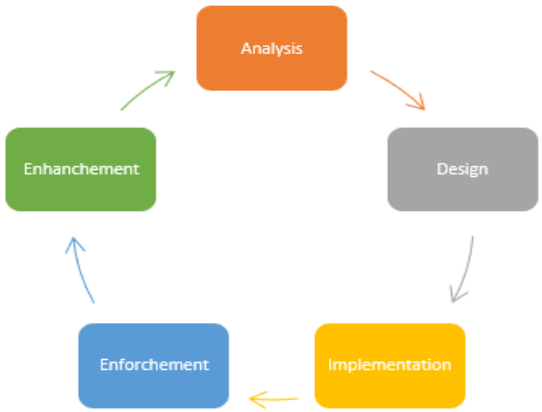
MATERIALS AND METHODS

The SPDLC method is an approach designed to plan updates in a network. This approach involves a series of phases or steps in the network system development cycle shown in Figure 1. Several steps involved in this research include Analysis, Design, Implementation, Enforcement, and Enhancement (Yuliandari, Walim, Raja, Ningsih, & Wahidin, 2024).

Analysis

The problem analysis stage begins with identifying and collecting related information, as well as determining the needs of all system components needed to handle the existing problem. This problem identification aims to find security obstacles currently being faced by the network and evaluate system performance in an organizational entity or company (Mukmin, Purnawansyah, & Hasnawi, 2024).

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 20, No. 2 September 2024 | DOI: 10.33480/pilar.v20i2.5535



Source: (Yuliandari et al., 2024)
Figure 1. SPDLC Method

Design

The system planning process carried out before it is built, which includes creating a flowchart of the system to be developed, including awork flow diagram and the necessary stages. Flowchart graphically, that is, displaying the steps. Today, flowcharts are recognized as an invaluable tool in aiding reasoning and presenting information clearly, which can help in the visualization of complex procedures. Apart from that, flowcharts are also used to define processes or projects that need to be carried out (Allawi, 2020). This step is intended to logically plan the server network structure so that you can visualize the system to be built (Yuliandari et al., 2024).

Implementation

Implement detailed computer network topology design that covers all system requirements in a real environment (Mukmin et al., 2024). The implementation stage involves creating a Telegram Bot configuration and its integration with Uptime Kuma to generate timely notifications.

Enforcement

At this stage, penetration testing is carried out on systems that have been developed previously (Yuliandari et al., 2024). The trial was carried out by running the Telegram bot program and the Uptime Kuma that had been created. The results of this trial will determine the success of the system that has been built as a solution to existing problems.

Enhancement

This final step involves evaluating the results of penetration tests that have been carried out to review the effectiveness of the system that has been built (Yuliandari et al., 2024). In addition, optimization was carried out on every design element, including hardware, software, and other requirements such as network monitoring and adding necessary components.

RESULTS AND DISCUSSION

Analysis

In situations where an administrator must continuously monitor the status of a network server to ensure smooth operations, the network server plays a central role as the core of the infrastructure that provides internet services to users. If there is an interruption or failure on the network server, internet availability for users may be hampered or even not available at all. Therefore, the smooth running of daily activities, information security, and customer satisfaction depend greatly on the accuracy and readiness of server administrators in monitoring the network.

When a network disruption occurs, administrators only get information from users via WhatsApp messages, which often results in delays in detecting the problem. Sometimes, users don't report problems immediately or don't even realize that the problem they are experiencing is network related. The manual process of monitoring a network through user complaints consumes time and resources, as administrators must manually check each complaint and perform analysis to identify the cause of the problem.

Data communication media, or messages conveyed as a result of responses to network conditions, are the main focus in analyzing network monitoring problems. The network monitoring system uses a Mikrotik router and Uptime Kuma. If a problem occurs on the network, a notification will be immediately sent via the Telegram bot to the network administrator. This Telegram bot is connected to Uptime Kuma, and notifications will be managed by Alertmanager or the Uptime Kuma notification feature. This way, network administrators will be immediately notified of problems that occur, without even having to actively monitor Uptime Kuma.

Required Specifications:

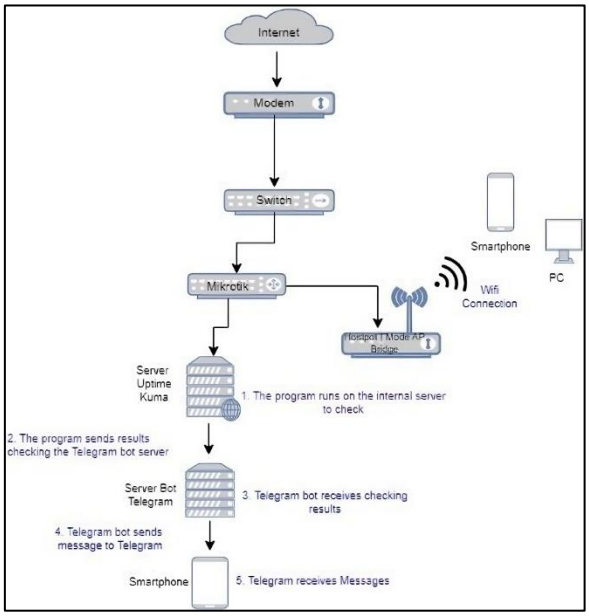
1. VM Virtual Box application
2. Debian 12.05 Iso Files
3. RAM 4GB
4. Processor 2
5. Memory 30 GB

Design

System configuration ensures performance as expected. Planning provides details about the network topology and system infrastructure that will be built (Prasetyo & Soetanto, 2024). This research will be carried out by the author to understand the requirements needed for implementation including users of the Telegram Bot

API, which is available via request for the Telegram application on smartphones managed by network administrator. The Telegram bot is used as a communication and information tool, while the monitoring system is configured using Mikrotik and Uptime Kuma.

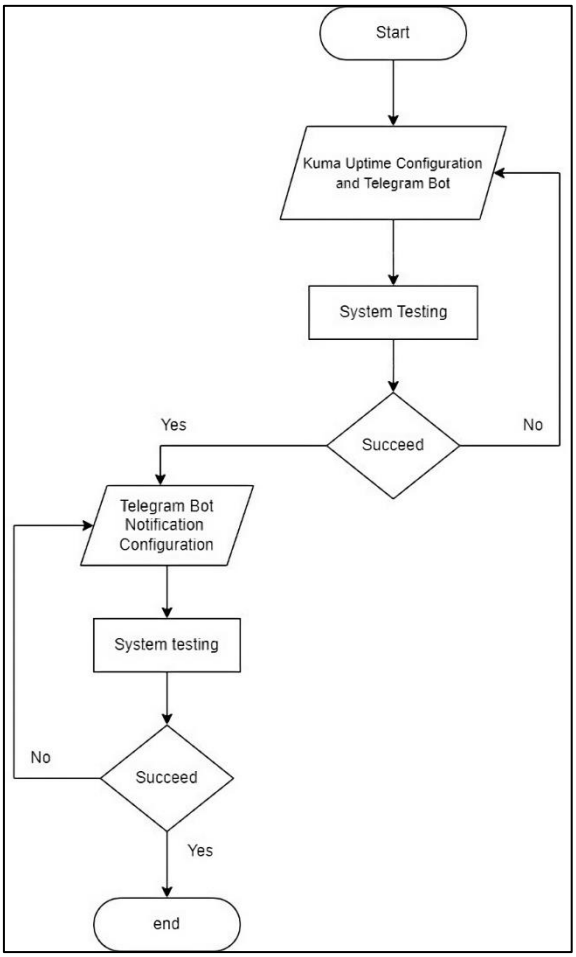
The process from the internet to Telegram and then back to the smartphone to receive notifications from Uptime Kuma is explained in Figure 2. Which explains the network monitoring flow. The program runs on an internal server to check the network, then the program sends the results of the check to the Telegram bot server. The telegram bot receives the checking results after that the telegram bot sends a message to telegram, and telegram receives a notification.



Source: (Research Results, 2024)

Figure 2. Network Topology

Flowchart which describes the sequence of implementation procedures in this research can be seen in Figure 3 below. Uptima Kuma installation and configuration will undergo testing in the first phase. The next step will be carried out if the configuration testing process is completed successfully or without problems. Like the previous stage, the next implementation involves configuring the Telegram bot. Once this is done, testing will be performed on the resulting configuration. If there are problems with the steps you take, immediately start over again. Monitoring steps are then carried out in accordance with the SPDLC stages if each process has been successfully completed.

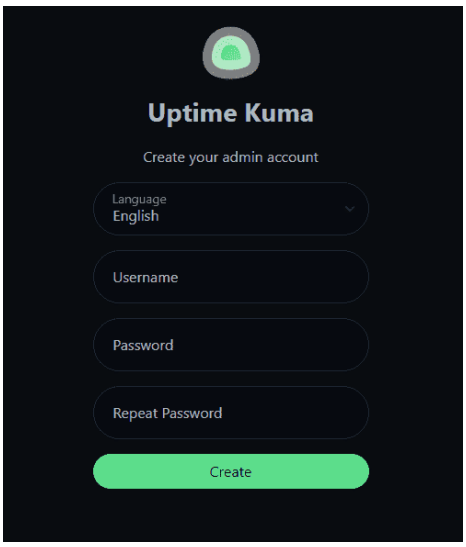


Source: (Research Results, 2024)

Figure 3. Flowchart

Implementation

At this stage, we will apply the network topology design and flowchart has been designed from the start (Yunanri. & Fitriana, 2024).



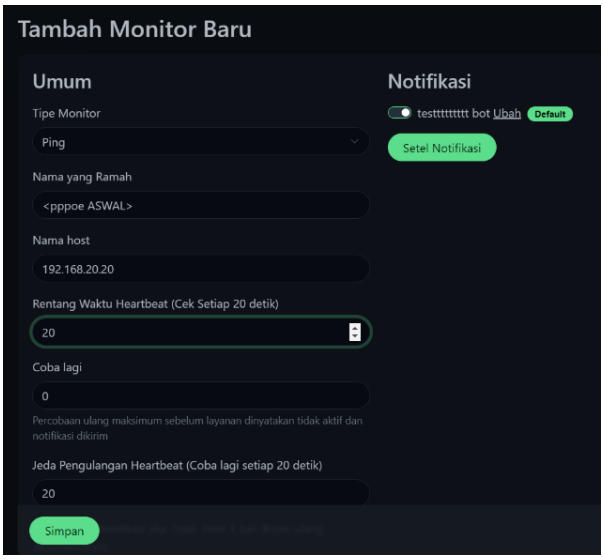
Source: (Research Results, 2024)

Figure 4. Login Display

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 20, No. 2 September 2024 | DOI: 10.33480/pilar.v20i2.5535

Next, configure and install Uptime Kuma on VM Virtual Box with Iso Debian 12.05. After completing the next install try accessing Uptime Kuma in the browser. Here the author selects chrome and a login screen will appear like Figure 4.

After entering the login page, enter the username you want to create and add a password, then click create. If you have successfully logged in and opened the Uptime Kuma console, the next step is to click the "Add New Monitor" option located in the top left corner of the screen.

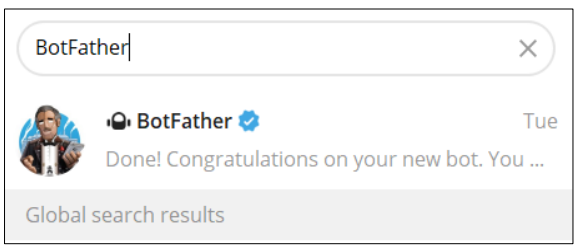


Source: (Research Results, 2024)

Figure 5. Add New Monitor Display

Figure 5 will bring up the "Add New Monitor" dialog. In it we can adjust the parameters needed for the new monitor. Here the author selects the monitor type "ping" because the author will monitor the network, then for a friendly name we can enter a user name, namely "<pppoe ASWAL>". Next Host Name enter the user's IP Address. Authors can also set options such as retries and other metrics related to notifications. For the Heartbeat Time Range and Heartbeat Repetition Pause, the author uses 20 seconds so as not to wait too long. After that click save.

Figure 6 creating a Telegram bot aims to obtain tokens from the bot, which can then be used to access the Telegram API.



Source: (Research Results, 2024)

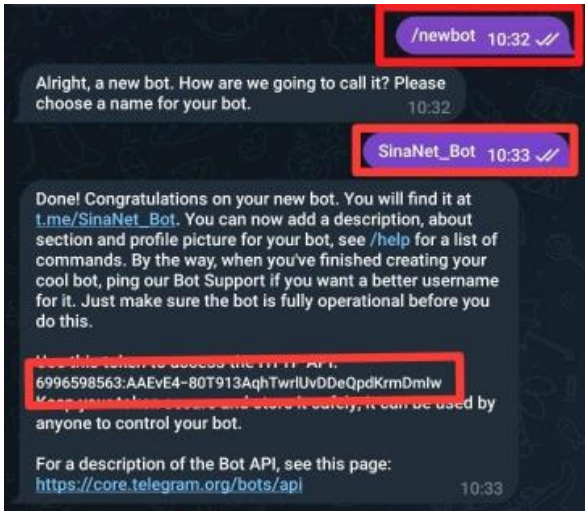
Figure 6. BotFather Search

Figure 7 shows to start a new conversation with a bot, authors need to type "/start" in Botfather.

Source: (Research Results, 2024)

Figure 7. Starting a New Conversation

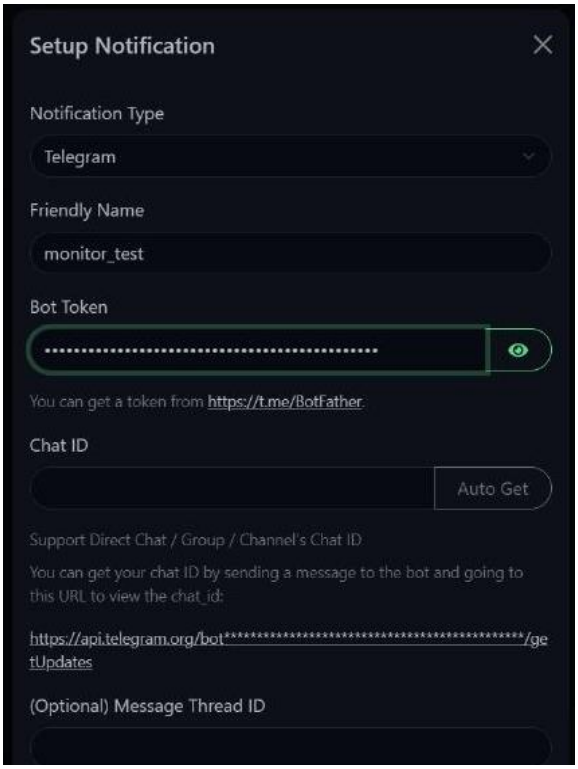
After that BotFather will provide information about the steps for creating abot. Next, send the command "/newbot'. This will start the process of creating a new bot. In this example, the author uses the username "SinaNet_Bot" where the username must end with _bot. In this step, BotFather will provide an API token. This token will be used to authenticate the bot when it wants to communicate with the Telegram API, which will be shown in Figure 8 below.



Source: (Research Results. 2024)

Figure 8. Creating a Telegram Bot

Next, in Figure 9 to connect Uptime Kuma with the Telegram Bot, go to the Uptime Kuma dashboard, select "Set Notifications". Here we can set the Notification type, username, and enter the bot token that we got earlier.



Source: (Research Results, 2024)

Figure 9. Uptime Kuma Notification Setup

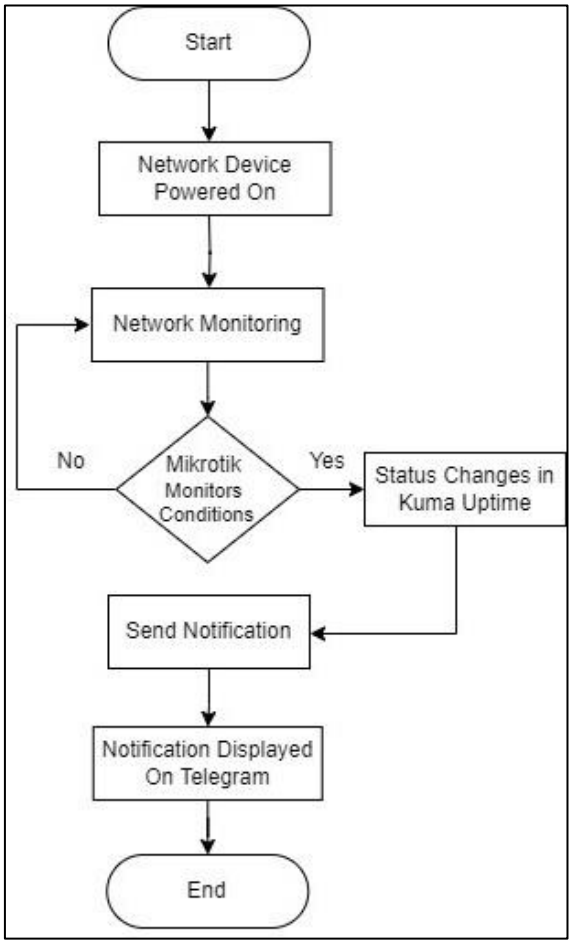
To get "Chat_ID" click the URL https://api.telegram.org/bot. If you have accessed the URL you will get the chat_id. If everything has been adjusted, then click test, if there is an incoming message notification to the Telegram application as in Figure 10, then creating a Telegram Bot notification with Uptime Kuma has been successful and don't forget to save.

Source: (Research Results, 2024)

Figure 10. Notification Test on Telegram

Enforchement

When the network device is turned on, the monitoring process starts automatically once the network device is functional. Administrators can check the network using Mikrotik capabilities. If there is a change in the network state, the Mikrotik device will notify Uptime Kuma regarding the change in status and send a Telegram bot notification. Notifications from Mikrotik will not be sent via Telegram if there is no change in network status.



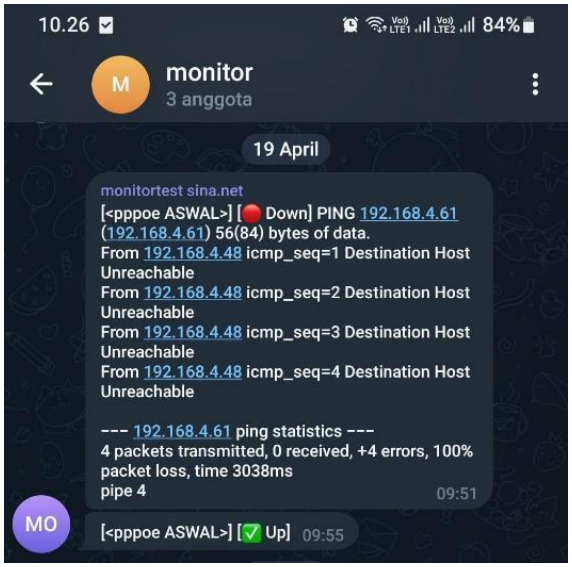
Source: (Research Results, 2024)

Figure 11. Testing Flowchart

Figure 11 explains the test flowchart, when the network device is turned on, the monitoring process starts automatically once the network device is functional. Administrators can check the network using Mikrotik capabilities. If there is a change in the network state, the Mikrotik device will notify Uptime Kuma regarding the change in status and send a Telegram bot notification. Notifications from Mikrotik will not be sent via Telegram if there is no change in network status.

In the Uptime Kuma testing stage in monitoring Wi-Fi networks, the author used Mikrotik with the help of Winbox software. To see changes in connection status on the Uptime Kuma dashboard, wait 20 seconds. The initial status before deactivation of the network looks 100%. If the number drops to 75% then the network will appear Down.

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 20, No. 2 September 2024 | DOI: 10.33480/pilar.v20i2.5535



Source: (Research Results, 2024)
Figure 12. Notifications on Telegram

In Figure 12, you can see that the <pppoe ASWAL> network is experiencing "Down". The results obtained by the author are based on research that has been carried out, obtaining information from connection status change notifications as follows:

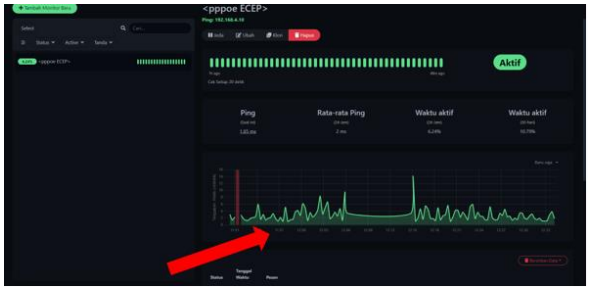
1. This message shows the results of an attempt to ping the IP address 192.168.4.61 from the source IP address 192.168.4.48 when the connection is "Down", which means it is not active.
2. PING 192.168.4.61 (192.168.4.61) 56(84) bytes of data.The ping command is carried out to the IP address 192.168.4.61 with a size of 56 bytes.
3. From 192.168.4.48 icmp_seq=1 Destination Host Unreachable.Indicates that there was an attempt to send a ping packet from IP address 192.168.4.48 to destination address 192.168.4.61, but the destination could not be reached. This can happen because the destination host is not connected or cannot be reached via the network used.
4. From 192.168.4.48 icmp_seq=2 Destination Host Unreachable. The message shows the same result as ICMP packet sequence number 2, namely that the destination host cannot be reached
5. From 192.168.4.48 icmp_seq=3 Destination Host Unreachable. The same thing happens with ICMP packet sequence number 3, where the destination host remains unreachable
6. From 192.168.4.48 icmp_seq=4 Destination Host Unreachable. This message also confirms the inability to reach the host destination, like the previous message.
7. --- 192.168.4.61 ping statistics ---provides ping statistics for the IP address 192.168.4.61
8. 4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3038ms. Explains that of the 4 packets sent, none were received, there were 4 errors, and 100% of packets were lost over a period of 3038 milliseconds.
9. Pipe 4Shows that 4 errors occurred.

Overall, the message indicates that there is a problem accessing the destination host 192.168.4.61 from the source IP address 192.168.4.48 when the connection is "Down", which indicates that the connection is inactive or disconnected. This problem requires further investigation to find the root cause.

Enhancement

Source: (Research Results, 2024)
Figure 13. Down Graph Display

Figure 13 shows a red graph which indicates the network is down or inactive.In the case of a network connection, a "down" status indicates that the connection cannot be established or is interrupted, causing the associated service to be unavailable or inaccessible.



Source: (Research Results, 2024)
Figure 14. Up Graphic Display

Figure 14 shows a green graph, which indicates that the network is in an active condition. This shows that everything is operating without any glitches or problems with the network connection at that time.

An evaluation of the overall monitoring time was carried out between the manual monitoring process and monitoring using Uptime Kuma and the

Telegram bot. Apart from comparing monitoring times, this stage also evaluates the flow in terms of speed. From the results of this evaluation, it can be concluded that Uptime Kuma with the Telegram Bot can detect the network when there are problems, such as active time and inactive time of the WiFi connection. Uptime Kuma can provide output in the form of network graphs.

CONCLUSION

By combining Telegram bot notifications with Uptime Kuma, administrator teams can respond to network availability more quickly, strengthening their ability to adapt to network conditions. Additionally the Mikrotik Device has proven to be a highly optimized solution for network infrastructure, featuring features that can be used to maintain and manage Wi-Fi networks. In the future, researchers can focus on developing increasingly complex Wi-Fi network monitoring models, and can incorporate newer tools, and can add variations in monitoring such as network security monitoring, so that network monitoring becomes more optimal.

REFERENCES

Al Farisi, M. M. (2024). Implementasi Kebijakan Desa Digital dalam Pengembangan UMKM di Desa Sidomulyo Kecamatan Silo Kabupaten Jember. *Jurnal Bisnis Dan Komunikasi Digital*, *1*(1), 7. https://doi.org/10.47134/jbkd.v1i1.1910

Allawi, N. (2020). What is the FlowChart. Retrieved from https://doi.org/10.13140/RG.2.2.25183.89767

Arifin, Z. (2024). Meningkatkan efektivitas penanganan gangguan jaringan internet menggunakan bot telegram dalam mendukung reliabilitas komunikasi data. *Jurnal Algoritma*, *20*(1), 148–155. https://doi.org/10.33364/algoritma/v.20-1.1276

Choudhari, Ms. A. B., Kurle, Ms. V. S., Nimbalkar, Ms. S. S., & Talekar, Mrs. S. S. (2024). Network identifier and monitoring. *International Journal of Advanced Research in Science, Communication and Technology*, *4*(4), 482–484. https://doi.org/10.48175/ijarsct-17482

Hafiz, N., Briliyant, O. C., Priambodo, D. F., Hasbi, M., & Siswanti, S. (2024). Remote penetration testing with telegram bot. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(3), 705–714. https://doi.org/10.29207/resti.v7i3.4870

Hakim, D. K., & Nugroho, S. A. (2024). Implementasi Telegram Bot untuk Monitoring Mikrotik Router. *Sainteks*, *16*(2). https://doi.org/10.30595/st.v16i2.7132

Kurnia, D., & Juliandri. (2024). Sistem Monitoring Login Failure dengan Via Telegram dari Serangan Brutus pada Router Mikrotik. *Majalah Ilmiah UPI YPTK*, *27*(2), 97–101. https://doi.org/10.35134/jmi.v27i2.55

Kurniawan, R. (2024). Analisis dan implementasi desain jaringan hotspot berbasis mikrotik menggunakan metode NDLC (network development life cycle) Pada BPU Bagas Raya Lubuk Linggau. *Jurnal Ilmiah Betrik*, *7*(01), 50–59. https://doi.org/10.36050/betrik.v7i01.12

Lee, B. (2024). Uptime Kuma: Open-source monitoring with Docker support. *4sysops*. Retrieved from https://4sysops.com/archives/uptime-kuma-open-source-monitoring-with-docker-support/

Mukmin, M., Purnawansyah, P., & Hasnawi, M. (2024). NOTIFIKASI BOT TELEGRAM UNTUK MONITORING JARINGAN PADA KEMENTRIAN KELAUTAN DAN PERIKANAN UNTIA. *Buletin Sistem Informasi Dan Teknologi Islam*, *3*(2), 127–133. https://doi.org/10.33096/busiti.v3i2.1162

Normadhoni, R., Dewanti, S. P., Namaskara, W. C., Akhadi, D. Y., & Fauzi, R. (2021). Penggunaan Bot Telegram sebagai Announcemnt System dalam Dunia Parenting. *Journal of Education and Technology*, *1*(1), 12–17. Retrieved from https://jurnalilmiah.org/journal/index.php/jet/article/view/34

Prasetyo, Y., & Soetanto, H. (2024). Implementasi Makopala network server Pada Router Mikrotik sebagai aplikasi usermanager untuk kampung wifi berbasis web. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *2*(2), 212–220. https://doi.org/10.36080/jk.v2i2.50

Safitri, V. E., A, I. K., & Prihantoro, C. (2024). Penerapan Network Monitoring Menggunakan The Dude Mikrotik dan Notifikasi Pesan dengan Aplikasi Telegram, WhatsApp, dan Email. *Decode: Jurnal Pendidikan Teknologi Informasi*, *4*(1), 94–106. https://doi.org/10.51454/decode.v4i1.200

Soufiane, S., Magán-Carrión, R., Medina-Bulo, I., & Bouden, H. (2024). Preserving authentication and availability security services through Multivariate Statistical Network Monitoring. *Journal of Information Security and Applications*, *58*, 102785. https://doi.org/10.1016/j.jisa.2021.102785

Utami, P. R. (2024). ANALISIS PERBANDINGAN QUALITY OF SERVICE JARINGAN INTERNET BERBASIS WIRELESS PADA LAYANAN INTERNET SERVICE PROVIDER (ISP) INDIHOME DAN FIRST MEDIA. *Jurnal Ilmiah Teknologi Dan Rekayasa*, *25*(2), 125–137. https://doi.org/10.35760/tr.2020.v25i2.2723

Yuliandari, D., Walim, W., Raja, B. K., Ningsih, R., & Wahidin, A. J. (2024). Simulasi Penerapan sistem monitoring jaringan snort NIDS pada web server Menggunakan metode SPDLC. *Jurnal Infortech*, *5*(2), 133–138. https://doi.org/10.31294/infortech.v5i2.17338

Yunanri., W., & Fitriana, Y. B. (2024). Analisis network security komputer tingkat desa menggunakan metode security policy development life cycle (SPDLC). *Jurnal Teknik Juara Aktif Global Optimis*, *1*(2), 11–21. https://doi.org/10.53620/jtg.v1i2.28