BIS INFORMATION TECHNOLOGY AND COMPUTER SCIENCE

Volume 2 2025 | DOI: 10.31603/bistycs.184
6th Borobudur International Symposium on Science and Technology (BIS-STE) 2024

UNIMMA PRESS
Universitas Muhammadiyah Magelang

Mini OLT power supply alarm bot for internet disruption prevention

Syahidan Cahya Rohmana[1], Uky Yudatama[1], Setiya Nugroho[1*], Nuryanto[1], Emilya Ully Artha[1]

[1] Informatics Engineering, Universitas Muhammadiyah Magelang, Magelang 56172, Indonesia
[*]Corresponding author email: setiya@unimma.ac.id

Abstract

PT Telkom Witel Magelang needs to maintain the quality of service for the increasing number of Internet users in Indonesia. The problem is the existence of Mini Optical Line Terminal (Mini OLT) devices, which frequently experience interference due to power loss. This problem is caused by the lack of an early warning system when the power supply is cut off, so the device shuts down before preventive measures are taken. Based on this background, this research aims to develop a Telegram bot as an early warning notification tool to prevent mass disruption of Telkom Internet services. This research uses the waterfall model system development method, which includes the stages of needs analysis, system design, implementation and testing. The built system uses the electrical voltage sensor on the Mini OLT to detect the ACVolDown condition, which indicates the disconnection of the power supply. The results show that the Telegram bot is able to provide accurate and timely notifications, with the fastest response time being 6 seconds and the longest being 33 seconds. Blackbox testing proves that all bot commands work properly on various Telegram platforms.

Keywords

Mini OLT, ACVolDown, Power loss prevention

Introduction

Published:
April 28, 2025

Selection and Peer-review under the responsibility of the 6th BIS-STE 2024 Committee

Internet service providers (ISPs) face numerous challenges that can cause connection interruptions. These include regulatory and competitive pressures, especially for small rural ISPs [1], and difficulties in maintaining service quality, as evidenced by frequent user complaints [2]. ISPs must also contend with traffic load variations and potential calamities, necessitating effective load distribution strategies [3]. Unreliable power supply is a significant cause of Internet connection outages in the telecommunications industry. Power outages affecting 10% or more customers in U.S. counties occur about 50 times daily, typically impacting 3,000 customers for nearly two hours [4]. In Nigeria, erratic power supply severely hampers the telecom sector's productivity [5]. Power interruptions disrupt production, damage equipment, and cause financial losses for

manufacturing companies [6]. The economic cost of unreliable grid power in Nigeria is substantial, forcing industries to rely on expensive self-generation [7]. University e-libraries in Nigeria face significant challenges due to power outages, with many Internet-connected computers remaining inactive [8].

Research on overcoming internet connection loss due to power outages has explored various approaches. Studies have assessed the impact of outages on end-host responsiveness, revealing weak correlations between power outage impacts and service restoration periods [9]. Proposed solutions include local backup servers for parallel tasks during outages [10], Wi-Fi routers with power backups and range extenders [11], and intelligent monitoring of IP address availability to detect outages [12]. Other innovations involve automatic modem reset systems [13], solar-powered resilient communication systems [14], and augmenting cloud connectivity with opportunistic networks for rural patient monitoring [15]. In emergencies, deploying fuel generators and batteries has been crucial for maintaining communication services [16]. These diverse approaches aim to enhance internet connectivity resilience during power outages. Utilizing machine learning algorithms and Monte Carlo simulations, researchers have developed predictive models for power outages [17]. Implementing IoT and blockchain technologies facilitates peer-to-peer energy sharing within microgrids, enabling communities to manage power resources effectively during outages [18]. Microgrids can operate in islanded mode during blackouts, utilizing user flexibility and energy storage to maintain power balance [19]. Researchers have proposed models for network reconfiguration that enhance resilience by maximizing the demand satisfaction rate during outages, ensuring minimal disruption to connectivity [20]. However, there are still things that researchers have not done to overcome internet connection loss due to power outages. One of them is by providing a notification to the ISP service officer when a power outage occurs.

This research will notify us when there is a power outage on the mini OLT device. The mini OLT functions to transmit light signals as a data transmission medium. This mini OLT will strengthen the signal for customers far from the ISP office. The mini OLT has a backup power system with a battery that automatically turns on when the power supply is cut off. This battery will last about 2 to 6 hours. This research aims to prevent internet connection loss by building a notification system during a power outage on the mini OLT device. The maintenance team can make early preparations to prevent the Mini OLT from going down, with information about the power supply being cut off on the Mini OLT. This can avoid disruption to the customer's internet connection. The application that will be created is a bot that will automatically send messages via the telegram short message application.

Method

The method utilized in this study, illustrated in Figure 1a, involves a system supported by a bot that continuously monitors the status of the Mini OLT database. Upon detecting a

power supply disruption to the Mini OLT, the bot promptly alerts the maintenance team. This enables them to prepare a generator before the Mini OLT's battery depletes and the system becomes inoperative. In the event of a Mini OLT shutdown, the Regional Operation Center coordinates with the designated officer to address the issue. If the shutdown occurs due to battery exhaustion, the maintenance team dispatches personnel to deliver and activate a generator to restore power to the Mini OLT. The workforce is strategically distributed, each overseen by a designated supervisor responsible for supporting field operations.

The Mini OLT operates at a standard voltage of 220 volts as defined by the State Electricity Company. Equipped with an advanced electric voltage sensor, the Mini OLT continuously monitors the incoming voltage from the alternating current power source. If a power supply disruption or a voltage drops below 180 volts, the voltage sensor triggers an alarm. This alarm updates the device's database with the status "Acvoldown" and automatically switches the power supply from the AC source to the backup battery. Figure 1b illustrates the operational workflow of the voltage sensor integrated into the Mini OLT. This mechanism ensures uninterrupted functionality and highlights the device's ability to adapt to fluctuating power conditions.

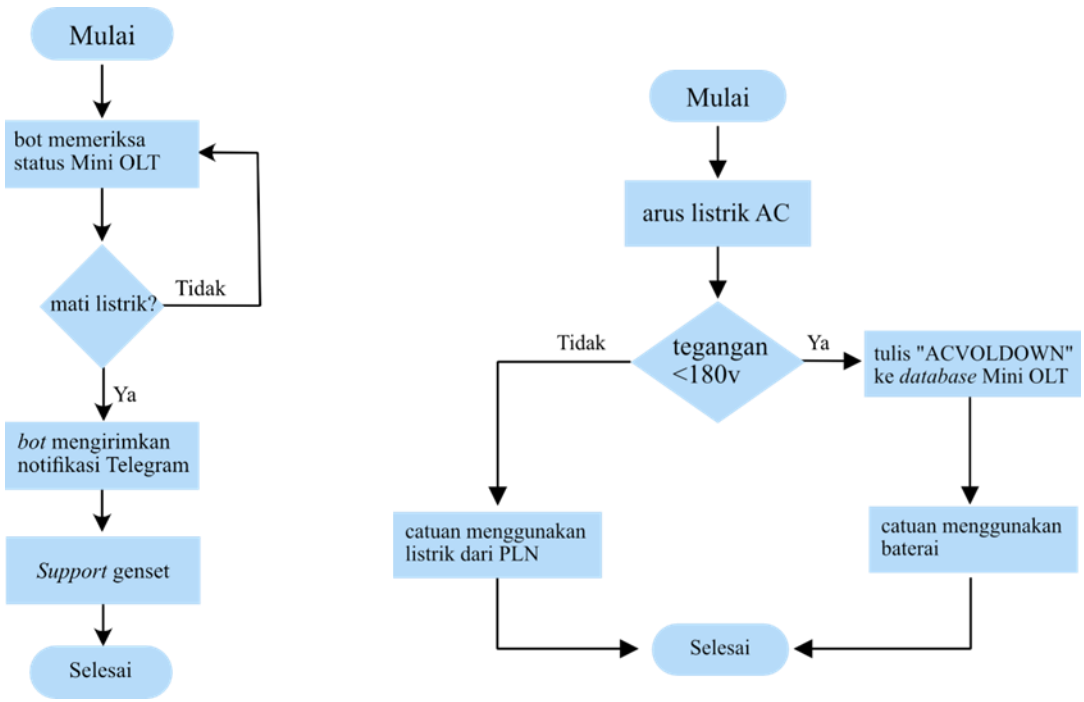


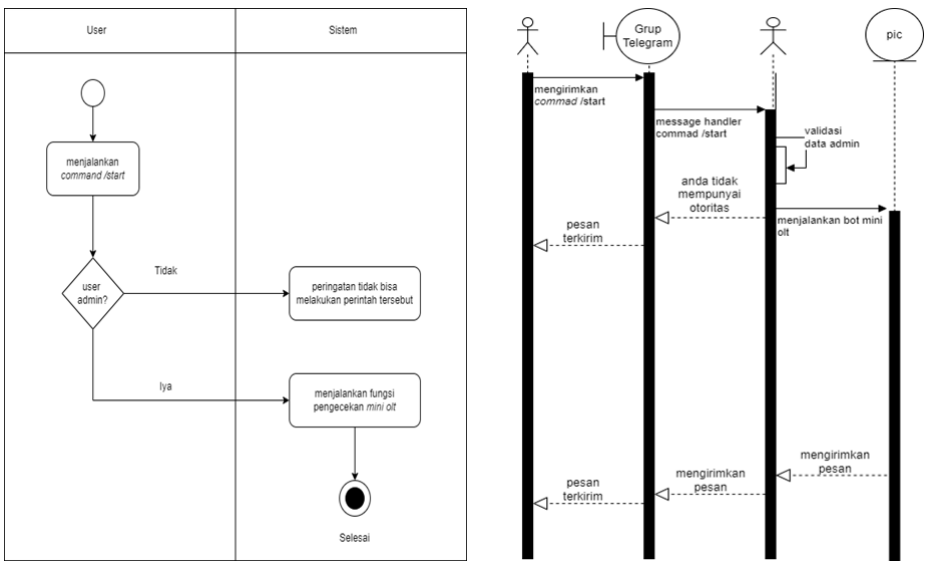
Figure 1. Flowchart of research method system (a. Notification delivery; b. Voltage current check)

The system comprises two main actors: the administrator and the user. The administrator holds comprehensive access rights, enabling them to execute a wide range of commands, including initiating the system (Start command), adding and deleting Optical Line Terminals (OLTs) and operators (nakers), editing OLT configurations, monitoring OLT status, viewing the list of OLTs, and utilizing the help feature. Conversely, the user has restricted access, limited to essential functionalities such as checking the status of OLTs, viewing the OLT list, and accessing the help feature.

This delineation of roles ensures an efficient division of responsibilities and enhances system security.

Figure 2a illustrates an activity diagram depicting the process of checking a mini OLT within the system design. The sequence begins when a user initiates the start command within the system. If the user's credentials verify them as an admin, they are promptly directed to execute the mini OLT checking function. Conversely, if the user is not registered as an admin, the system will generate a warning message, indicating that the start command cannot be performed or initiated under their access level.

Figure 2b illustrates the sequence diagram for the Mini OLT Function. The process begins when the user initiates the command `/start` or `start` within the system. The system then validates the user's credentials. If the user is identified as an authorized administrator, the system responds with a confirmation message and activates the OLT Mini Bot. Conversely, if the user lacks administrative authorization, the system sends a notification indicating that the user does not have the requisite permissions to access or control the system. In the Mini OLT status check sequence diagram, the administrative user initiates the process by executing a command, such as `/check`, within the system. Upon receiving this input, the system processes the request and responds by delivering a message containing detailed status data. This data specifically highlights the condition and any issues identified in the Mini OLT, enabling efficient troubleshooting and system monitoring.



a. b.

Figure 2. Unified modeling language diagram-based design (a. Activity Diagram; b. Sequence Diagram)

The proposed system involves leveraging SSH protocol access to the Mini OLT database to identify instances where Mini OLT devices experience power supply interruptions. Specifically, the system is designed to monitor the alarm status list within the Mini OLT database, detecting any occurrences of the "Acvoldown" status indicating a power supply failure. Upon identifying such an alarm, the system will log the status into the Mini OLT bot database for record-keeping and send an automated notification to the

maintenance team via Telegram. This approach ensures timely intervention and enhances the reliability of network operations, making it a valuable contribution to telecommunications maintenance frameworks. The data delivery architecture image is shown in Figure 3. The system enables administrators to securely monitor and control the Mini OLT device via an internet-connected device. Administrator commands are processed by a bot, which translates them into a format compatible with the Mini OLT and communicates securely using the SSH protocol. The Mini OLT executes the commands, accesses its internal database if needed, and returns the results to the bot. The bot processes and stores the data, then forwards the final output to the administrator's device for display, ensuring efficient and reliable system management.

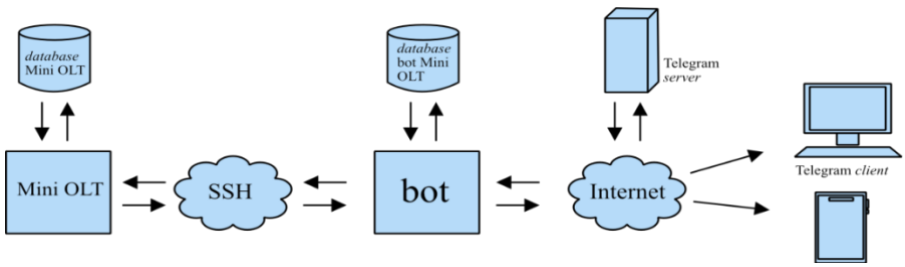


Figure 3. Data Delivery Architecture

Result and Discussion

Results

The developed system leverages the sensor integrated into the Mini OLT to detect alternating current voltages below 180 volts. When this condition occurs, the Mini OLT records the status as "Acvoldown" in the database. This status is subsequently accessed by a bot, which identifies the "Acvoldown" status in the Mini OLT database. Based on this detection, the bot automatically sends a notification message via Telegram to the maintenance team. This automated workflow ensures timely alerts and enables prompt maintenance responses. The following section details the results of the system's implementation and performance evaluation.

Figure 4 illustrates various methods employed to verify alarm status in OLTs. During a power outage, the alarm-checking process identifies the status "Acvoldown" on the Mini OLT alarm, applicable to OLT versions AN5516-04 and AN6000-2. The syntax displayed in the figure highlights the `show_alarm_current` function, which is specifically designed to retrieve real-time alarm data from OLT devices based on their version. For the AN5516-04 model, the function navigates through service, maintenance, and alarm directories before executing the `show alarm current` command. Subsequently, the alarm data is collected using the `recv()` method and decoded into JSON format for analysis. In contrast, for the AN6000-2 model, the function employs a more streamlined approach, issuing basic commands such as `config` and `show alarm current` without requiring directory navigation. Regardless of the model, the process includes time delays implemented via `time.sleep()` to allow the device adequate time

to process the commands. This structured methodology ensures accurate and reliable alarm status retrieval across different OLT versions.

```
def show_alarm_current(self, version):
    #command list untuk OLT versi AN5516-04
    if version == "AN5516-04":
        self.shell.send("cd service \n")
        self.shell.send("terminal length 0 \n")
        self.shell.send("cd . \n")
        self.shell.send("cd maintenance \n")
        self.shell.send("cd alarm \n")
        time.sleep(0.2)
        self.shell.send("show alarm current \n")
        time.sleep(4)
        self.alarm_current = self.shell.recv(65535)
        self.json_alarm_current = self.alarm_current.decode()

    #command list untuk OLT versi AN6000-2
    elif version == "AN6000-2":
        self.shell.send("config \n")
        time.sleep(1)
        self.shell.send("terminal length 0 \n")
        time.sleep(2)
        self.shell.send("show alarm current \n")
        time.sleep(4)
        self.alarm_current = self.shell.recv(65535)
        self.json_alarm_current = self.alarm_current.decode()
```

Figure 4. Source code section to check alarm status

```
Login:
[redacted]0305
Password: ************
                                                                Master

GPON00-D4-TEM-4FBA# config
GPON00-D4-TEM-4FBA(config)# terminal length 0
GPON00-D4-TEM-4FBA(config)# show alarm current
--------------------------------Current Alarm---------------------------------
Item Description                  Code vOLT     Object       Begintime           Endtime

1    CONFIG_HAVENOT_SAVED         761  0        3/0/0/0      2023-07-26 03:00:42

2    ACVOLDOWN                    810  0        801/0/0/0    2023-07-26 11:04:41

3    AC_FAIL                      773  0        801/0/0/0    2023-07-26 11:04:42

4    Battery_Discharging          1168 0        801/0/0/0    2023-07-26 11:04:42

5    ALL_ONU_DYING_GASP           1318 0        1/9/0/0      2023-07-26 11:04:36

6    ALL_ONU_DYING_GASP           1318 0        1/10/0/0     2023-07-26 11:04:42
```

Figure 5. Alarm check output result

Figure 5 illustrates the Mini OLT alarm status-checking process output for the device with the hostname GPON00-D4-TEM-4FBA. The figure depicts the output generated by executing the show alarm current command, which is a critical step in monitoring the

operational health of the device. The process begins by logging into the device using an account with appropriate configuration access privileges, followed by running a sequence of commands to retrieve and display active alarm data. The results section highlights a list of alarms currently active in the system, including the "ACVOLDOWN" alarm, which signals a disruption in the AC power supply. This alarm is accompanied by specific volt code details, information about the affected object, and the timestamps marking its occurrence (begin time) and resolution (end time). Other notable alarms identified include "AC_FAIL," "Battery_Discharging," and "ALL_ONU_DYING_GASP," which collectively indicate critical conditions affecting system stability. These alarm outputs are integral for real-time monitoring, enabling swift responses to system disruptions and ensuring the operational reliability of the device.

Figure 6 is a message sent by a bot via the Telegram Messenger application. Section 6A shows the message sent containing information about the Mini OLT hostname, IP, short message, and username pic from the datel where the Mini OLT is located. Section 6B shows a message sent by the bot if the Mini OLT battery runs out after the power supply to the Mini OLT is cut off. Section 6C shows a message sent by the bot when the Mini OLT that previously experienced a power outage or had the status "ACVOLDOWN" has returned to normal or the Mini OLT power supply has been reconnected. Section 6D shows a message sent by the bot when the Mini OLT cannot be accessed but there was no previous power outage so it is assumed that there was LOS or Loss of Signal. Section 6E shows a message sent by the bot when the Mini OLT that previously had the status "DOWN" because it could not be accessed, has returned to normal and can be accessed.

Figure 6. Telegram bot alarm notification

Discussion

The algorithm described in Figure 7 illustrates the integration of a Telegram bot for automating device status monitoring and notification delivery, a critical capability for maintaining operational continuity in complex systems. This process begins with the initialization of key parameters, including the API token, chat ID, host, user credentials, and database connection details. The bot establishes a secure connection to the database, retrieving relevant data regarding the device's operational status. Subsequently, it initiates an SSH connection to the target device, launching a shell terminal to execute diagnostic commands, such as the `ping` command, to assess the device's connectivity. If the `ping` command succeeds, the variable `testPing` is set to `True`, confirming network connectivity.

Building upon this initial diagnostic, the bot attempts to access the device via Telnet to identify active alarms using the `show alarm current` command. The output of this command is meticulously analyzed to detect specific alarm conditions, including "Acvoldown" (indicative of an AC voltage drop), "LOS" (loss of signal), or "Battery Discharging" (battery depletion). Upon detecting any of these conditions, the bot triggers the immediate dispatch of a notification message to a predefined Telegram chat, detailing the device's status and the nature of the alarm. This ensures that operational teams receive real-time alerts for timely response.

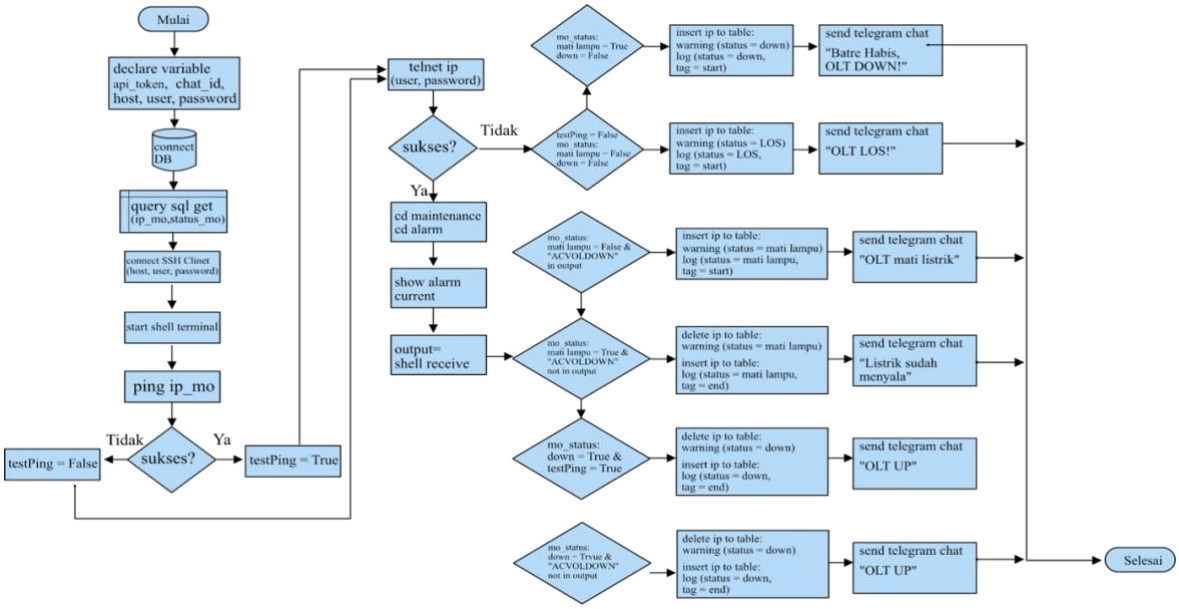


Figure 7. Telegram bot algorithm

In addition to notification delivery, the bot interacts with the database to log the alarm conditions, capturing the initiation or resolution of each alert. This logging provides a comprehensive record of device performance and operational anomalies, enabling historical analysis and continuous improvement in monitoring strategies. The seamless integration of database operations, SSH and Telnet protocols, and Telegram's notification capabilities ensures a robust and automated system for real-time device monitoring. This framework significantly enhances the efficiency of fault detection and response, aligning with best practices in operational technology and automation.

Testing is an essential phase in the development process to ensure that a Telegram bot operates as expected without errors. Black-box testing, as outlined in Table 1, was conducted once the development of the Telegram bot was completed. This testing approach employed the equivalence partitioning technique, which involves dividing the input domain of the Telegram bot into several equivalence classes or partitions. Each partition represents a set of inputs expected to yield similar results, allowing for the creation of targeted test cases. These test cases served as references for evaluating the bot's functionality under different scenarios.

The testing procedure encompassed three distinct platforms to assess the bot's performance comprehensively: Telegram Mobile, Telegram Desktop, and Telegram

Web. For Telegram Mobile, the testing was conducted using an Android device running version 11, paired with the Telegram application version 10.14.5. For Telegram Desktop, testing was performed on a device equipped with an Intel Core i7-4510U processor, running the Telegram Desktop application version x64.5.2.3. Meanwhile, Telegram Web testing was carried out on a compatible web browser.

Each platform underwent ten rounds of testing to ensure reliability and consistency in the results. Across all testing iterations, the Telegram bot exhibited optimal performance with no discrepancies or deviations between the observed and expected results defined in the test cases. This indicates the absence of bugs or defects in the bot's functionality. The results of this testing process affirm that the Telegram bot operates as intended, meeting the expected standards of usability and reliability on all tested platforms. The robust outcomes of these tests underscore the effectiveness of the development and testing methodologies employed, ensuring the bot's readiness for deployment and use in real-world scenarios.

Table 1. Example shows research data in table

No	Description	Results
1.	Running /start command on the telegram bot	Bot provides running the checking process
2.	Running /check command on the telegram bot	Bot provides information about the condition of the OLT
3.	Running /list_olt command on the telegram bot	Bot displays a list of mini OLTs in each region
4.	Running /add_olt command on the telegram bot	Can add new OLTs to the database
5.	Running /add_naker command on the telegram bot	Can add new images to the database
6.	Running /edit_olt command on the telegram bot	Can make changes to data
7.	Running the /delete_olt command on the telegram bot	Can delete OLT data from the database
8.	Running the /delete_naker command on the telegram bot	Can delete image data from the database
9.	Running the /help command on the telegram bot	Displays information on the list of mini OLT bot commands

Response time testing is conducted to evaluate the duration required for a bot to send notifications to a Telegram group when specific trigger events occur. In this context, the trigger events are the disconnection and reconnection of an electrical power supply, controlled via on and off switches. When the miniature circuit breaker (mcb) switch is turned off, the flow of electric current is interrupted, which prompts the bot to send a notification to the designated Telegram group, alerting members of the power disruption. Conversely, when the mcb switch is turned back on, restoring the electric current, the bot generates another notification to inform users that the power supply has been reinstated. The time elapsed between the pressing of the mcb switch (to either the off or on position) and the appearance of the corresponding notification in the Telegram group is meticulously recorded as the response time. This measurement

serves as a key performance indicator for the bot's responsiveness and reliability, providing critical insights into its effectiveness in real-time alert systems.

Table 2 presents the test results obtained from Mini Optical Line Terminal (OLT) devices branded Fiberhome, with two specific configurations: GPON01-D4-MGE-4FRAK operating on version AN6000-2 and GPON00-D4-MGE-4FRAK running version AN5516-04. The tests were conducted using a single Mini OLT device per test cycle. Each test cycle consisted of a series of five switch-off and five switch-on operations for each Mini OLT device. The performance evaluation revealed that for the GPON01-D4-MGE-4FRAK device with version AN6000-2, the response time ranged between a minimum of 8 seconds and a maximum of 33 seconds. In comparison, the GPON00-D4-MGE-4FRAK device operating on version AN5516-04 demonstrated a slightly better response range, with the fastest response recorded at 6 seconds and the longest at 29 seconds. These results provide insights into the responsiveness and stability of Fiberhome Mini OLT devices under repeated on-off cycles, highlighting differences in performance based on the device model and software version.

Table 2. Response Time Testing

Switch	Version	Response Time (seconds)				
		1	2	3	4	5
AN6000-2	Stove temperature (°C)	8	8	33	27	15
	Liquid temperature (°C)	21	33	15	17	31
AN5516-04	Stove temperature (°C)	29	21	6	13	9
	Liquid temperature (°C)	28	12	27	29	25

The historical landscape of addressing power outages in telecommunication systems has evolved significantly, with a focus on enhancing network resilience and minimizing service disruptions. Traditionally, manual monitoring and response mechanisms were employed, which often led to delayed interventions and prolonged service outages. Over the past decade, the integration of automated systems, such as smart sensors and IoT devices, has revolutionized the approach to managing power supply issues. These technologies have enabled real-time monitoring and quicker response times, thus reducing the impact of outages on end-users.

In this context, the current research builds on previous innovations by introducing an automated Telegram bot system that leverages advanced voltage sensors and secure communication protocols. Unlike earlier solutions that primarily relied on manual checks or localized backup systems, this study offers a more comprehensive and proactive approach. By utilizing a centralized notification system, the developed bot ensures that maintenance teams are immediately informed of power disruptions, allowing for swift remedial actions. This not only enhances the reliability of internet services but also reduces operational costs associated with prolonged outages and equipment damage.

Moreover, the use of the Telegram platform for notifications adds a layer of accessibility and convenience, given its widespread usage and robust messaging infrastructure. This strategic choice underscores the study's commitment to leveraging modern

communication tools to enhance operational efficiency. By situating this research within the broader historical narrative of technological advancements in power outage management, the originality and significance of the current findings are further emphasized. This approach not only addresses current challenges but also lays the groundwork for future innovations in maintaining resilient telecommunication networks.

Conclusion

This research successfully developed a Telegram bot system designed to provide real-time notifications regarding power supply disruptions in Mini Optical Line Terminal (OLT) devices. The bot's implementation demonstrated high reliability and efficiency in detecting AC voltage drops below 180 volts and subsequently notifying maintenance teams through automated Telegram messages. The system enables swift responses, preventing extended service outages and ensuring the stability of internet connectivity for end-users.

Testing results confirm the bot's effectiveness, with response times ranging from 6 to 33 seconds depending on the OLT device model and software version. Specifically, the Fiberhome Mini OLTs operating on AN5516-04 exhibited faster response times compared to those running on AN6000-2. Black-box testing across various Telegram platforms validated the system's robustness and compatibility, affirming its readiness for deployment in diverse operational environments.

The integration of voltage sensors, secure SSH-based database monitoring, and automated alert mechanisms significantly enhances the reliability of network operations. This innovative approach addresses a critical challenge faced by Internet Service Providers (ISPs), enabling proactive maintenance strategies and minimizing disruptions caused by power outages. Future work could explore expanding the system's capabilities, such as integrating predictive analytics for power supply issues and scaling its application to larger networks.

Acknowledgement

We would like to express our gratitude to PT. Telkom Indonesia Witel Magelang for providing various devices used in this study.

References

[1] M. B. McNally, D. Rathi, K. Joseph, J. Evaniew, and A. Adkisson, "Ongoing Policy, Regulatory, and Competitive Challenges Facing Canada's Small Internet Service Providers," *Journal of Information Policy*, vol. 8, pp. 167–198, Mar. 2018, doi: 10.5325/jinfopoli.8.2018.0167.

[2] P. Akbar, M. Agus Sunandar, and U. Muhammad Husni Tamyiz, "Analisis Quality Of Service Jaringan Wireless Pada Penyedia Jasa Layanan Internet Service Provider (Isp) Indihome & Iconnet," *JATI (Jurnal Mahasiswa Teknik Informatika)*, 2023.

[3] A. Al-Darrab, I. Al-Darrab, and A. M. A. Rushdi, "Software-Defined Networking load distribution technique for an internet service provider," *J. Netw. Comput. Appl.*, vol. 155, p. 102547, 2020.

[4] S. Anderson, T. Bell, P. Egan, N. Weinshenker, and P. Barford, "Measuring the Impacts of Power Outages on Internet Hosts in the United States," in *IFIP Advances in Information and Communication Technology*, Springer Nature Switzerland, 2023, pp. 62–90. doi: 10.1007/978-3-031-49585-4_4.

[5] C. Agbeboaye, F. O. Akpojedje, and B. I. Ogbe, "Effects of Erratic and Epileptic Electric Power Supply in Nigerian Tel ecommunication Industry: Causes and Solutions," *J. Adv. Sci. Eng.*, vol. 2, no. 2, pp. 29–35, Dec. 2019, doi: 10.37121/jase.v2i2.61.

[6] M. C. Nyangwaria and M. P., "Relationship between Power Supply Interruptions and Financial Performa nce of Manufacturing Companies in Machakos County," 2019.

[7] S. Olowosejeje, P. Leahy, and A. Morrison, "The economic cost of unreliable grid power in Nigeria," *African Journal of Science, Technology, Innovation and Development*, vol. 11, no. 2, pp. 149–159, Jan. 2019, doi: 10.1080/20421338.2018.1550931.

[8] G. Efenedo and W. O. Edegbo, "Internet connectivity and power outages in university electronic libra ries in Nigeria," *JICTDAR*, vol. 5, no. 2, pp. 83–89, 2023, doi: 10.47524/jictdar.v5i2.84.

[9] A. Scott, B. Tucker, E. Patrick, W. Nathan, and B. Paul, "Measuring the Impacts of Power Outages on Internet Hosts in the United States," *Critical Infrastructure Protection*, 2023.

[10] A. A. A., S. T. Shimal, and A.-K. A., "TQAIOD: A Backup Technique to Surpassing the Internet Outage," *International Conference on Computer Science and Software Engineering*, 2020.

[11] D. Harshal, Y. M. Bharati, G. Aniket, and W. Anurag, "Wi-Fi Router With Power Backup and Range Extender," *2022 IEEE Delhi Section Conference (DELCON)*, 2022.

[12] N. Bayat, K. Mahajan, S. Denton, V. Misra, and D. Rubenstein, "Down for failure: Active power status monitoring," *Future Generation Computer Systems*, vol. 125, pp. 629–640, Dec. 2021.

[13] W. Joao, F. Joao, and C. Sandro, "IoT System for Internet Connection Monitoring with Automatic Modem Reset," *International Journal of Computer Applications*, 2019.

[14] A. M. B. Celdrick *et al.*, "Localized Solar-Powered Resilient Communication System Using Wi-Fi Routers and Access Points with Integrated Smartphone Application through Raspberry Pi Chat Server," *International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management*, 2019.

[15] M.-O. Esther *et al.*, "Augmenting Cloud Connectivity with Opportunistic Networks for Rural Remote Patient Monitoring," *International Conference on Computing, Networking and Communications*, 2019.

[16] A. I. Zabrodskyy, "Peculiarities of the Operation f Optical Communication in case of emergencies." State University of Information and Communication Technologies, 2024.

[17] Mahtab Murshed, Manohar Chamana, Konrad Schmitt, Suhas Pol, Olatunji Adeyanju, and Stephen Bayne, "Renewable Energy Integration for Power Outage Mitigation: A Data-Driven Approach in Advancing Grid Resilience Strategies," 2023, [Online]. Available: http://dx.doi.org/10.20944/preprints202308.2119.v1

[18] N. B. S. Shibu, Aryadevi Remanidevi Devidas, S. Balamurugan, Seshaiah Ponnekanti, and Maneesha Vinodini Ramesh, "Optimizing Microgrid Resilience: Integrating IoT, Blockchain, and Smart Contracts for Power Outage Management," *IEEE Access*, vol. 12, pp. 18782–18803.

[19] Philipp Danner, Anna V. Volkova, and Hermann de Meer, "Two-Step Blackout Mitigation by Flexibility-Enabled Microgrid Islanding," 2024, [Online]. Available: http://dx.doi.org/10.1145/3632775.3661986

[20] Ahmed Imteaj, Vahid Akbari, and M. Hadi Amini, "A Novel Scalable Reconfiguration Model for the Postdisaster Network Connectivity of Resilient Power Distribution Systems," *Sensors*, vol. 23, no. 3, pp. 1200–1200, 2023.