DESIGN OF A TELEGRAM-INTEGRATED GRAFANA NETWORK MONITORING SYSTEM FOR ENHANCED FAULT DETECTION AND REAL-TIME NOTIFICATION

[1*]Nurul Fahmi Arief Hakim, [2]Siscka Elvyanti, [3]Yogi Ardiansyah
[1,2,3]Fakultas Pendidikan Teknik dan Industri, Universitas Pendidikan Indonesia
[1,2,3] Jl. Setiabudhi No 229, Bandung, Jawa barat
[1]nurulfahmi@upi.edu, [2]sisckael@upi.edu, [3]yogiardiansyah@upi.edu

Abstrak

Monitoring perangkat jaringan memiliki permasalahan seperti terputusnya konektivitas antar router. Teknisi jaringan diharuskan untuk memonitoring seluruh perangkat jaringan setiap saat. Artikel ini bertujuan untuk membahas hasil sistem monitoring perangkat jaringan di Gedung A FPTK UPI menggunakan Grafana yang terintegrasi Telegram sebagai upaya pemantauan dan perbaikan pada perangkat jaringan yang bermasalah. Metode yang digunakan yaitu simulasi menggunakan perangkat lunak jaringan yang disesuaikan dengan kondisi sebenarnya. Grafana dan Prometheus digunakan dalam pembuatan sistem monitoring perangkat. Prometheus bekerja untuk mengambil data dari SNMP (Simple Network Management Protocol) dan mengolah data tersebut menggunakan exporter. Grafana dapat membuat visualisasi pada sistem monitoring perangkat jaringan dari data yang telah diproses. Penelitian ini menggunakan metode simulasi pada software PNETLab dan VMware. Berdasarkan hasil yang diperoleh, tampilan dashboard Grafana dapat menampilkan traffic interface pada router. Dashboard yang ditampilkan yaitu ketika ether 2 yang terhubung dengan router lantai 2 utara mengalami gangguan yang menyebabkan router lantai 2 utara tidak mendapatkan akses jaringan internet sehingga muncul peringatan berupa notifikasi pesan R_LT2_UTARA | Down dari DSTIbot melalui Telegram. Upaya perbaikan dari permasalahan tersebut dilakukan dengan cara ether 3 dikoneksikan dari router lantai 1 tengah ke router lantai 2 utara agar router lantai 2 utara tetap mendapatkan akses jaringan internet. Perbaikan tersebut menampilkan notifikasi pesan R_LT2_UTARA | Up dari DSTIbot melalui Telegram.

***Kata kunci**: Grafana, monitoring jaringan, Prometheus, SNMP Exporter*

Abstract

Network device monitoring has problems such as connectivity loss between routers. Network technicians are required to monitor all network devices at all times. This article aims to discuss the results of the network device monitoring system in Building A FPTK UPI using Grafana integrated with Telegram as an effort to monitor and repair problematic network devices. The method used is simulation using network software that is adjusted to actual conditions. Grafana and Prometheus are used in creating a device monitoring system. Prometheus works to retrieve data from the SNMP (Simple Network Management Protocol) and process the data using an exporter. Grafana can create visualizations on the network device monitoring system from the data that has been processed. This study uses a simulation method on PNETLab and VMware software. Based on the results obtained, the Grafana dashboard display can display the traffic interface on the router. The dashboard displayed is when ether 2 connected to the north 2nd floor router experiences interference which causes the north 2nd floor router to not get internet network access so that a warning appears in the form of a notification message R_LT2_UTARA | Down from DSTIbot via Telegram. The repair effort for the problem was carried out by connecting ether 3 from the middle 1st floor router to the north 2nd floor router so that the north 2nd floor router still gets internet network access. The repair displays the message notification R_LT2_UTARA | Up from DSTIbot via Telegram.

***Keywords**: Grafana, network monitoring, Prometheus, SNMP Exporter.*

INTRODUCTION

The rapid advancement of network technology, especially in telecommunications like internet access and local area networks (LANs), has created an essential foundation for information and communication across multiple sectors, including academia, government, industry, and households [1]. The stability, security, and efficacy of network infrastructure are increasingly intricate and vital for daily operations, posing considerable hurdles [2]. Network disruptions, caused by hardware malfunctions, physical damages like broken LAN cables or fiber optics, or cyber threats such as hacking and denial-of-service (DoS) attacks, can lead to considerable declines in operational efficiency and productivity [3]. Moreover, the expanding network scale in enterprises and colleges makes manual network monitoring unfeasible, requiring substantial human resources and prolonged troubleshooting durations to effectively identify and rectify errors [4], [5].

To address these challenges, network device monitoring systems have been developed to record, analyze, and visualize network performance data in real time [6]. These technologies enable the proactive detection of network anomalies and malfunctions, thereby diminishing the probability of downtime and improving the overall resilience of the network. Nonetheless, conventional monitoring techniques often rely on human or semi-automated processes, which can prove inefficient for managing large network infrastructures [7]. The reliance on traditional notification methods, such email alerts, presents disadvantages, including the risk of spam filtering, delayed messages, and the loss of previous warning data due to automated deletion rules.

The Directorate of Information Systems and Technology (DSTI) at the Universitas Pendidikan Indonesia (UPI) currently manages network monitoring via a centralized system that heavily depends on email notifications. This approach has several notable disadvantages, including potential delays in responses due to the lack of immediate email alert reviews, frequent misclassification of emails as spam due to notification redundancy, and limited retention of historical alerts caused by automated deletion policies. Given these limits, there is an urgent need for a more efficient, real-time, cloud-integrated monitoring system that boosts network managers' ability to respond immediately to crucial events.

Multiple studies have examined automated network monitoring techniques that leverage alarm systems and visualization [8], [9]. The condition of network devices has been extensively monitored through the implementation of network device monitoring systems. Irawansyah, et al. create a system that can monitor the network with short message service (SMS) notifications using The Dude. The network monitoring system with SMS Notifications aims to enable network admins

to know the network conditions wherever they are. In monitoring the network, The Dude will display an indicator in the form of a color. The Dude can monitor the network on a computer network in the form of a notification of the device being on or off. The results of the research conducted still use SMS, where mobile phones require a fee to send messages. [10]. The web-based SNMP method is employed by Taftazanie, et al. to monitor network devices. The monitoring server accumulates device data, which is then presented in a web-based application. Crontab is employed to monitor each minute in the application. This web-based application has the capability to send the administrator warnings in the form of SMS and email when the server device encounters an error [11].

This investigation employs Grafana software as a network monitoring system by conducting a comparative analysis of prior studies. The system integrates Grafana with various data sources, including Prometheus for matrix support and SNMP Exporter for network device information. The warning system utilizes the Telegram application, leveraging the Bot API and Telegram API for notifications. The monitoring system was developed for network devices at the Faculty of Vocational Technology Education (FPTK) UPI, with alerts sent via Telegram. Grafana is open-source software used for visualizing and analyzing data from network devices such as switches, routers, firewalls, and servers [12], [13]. It features a dashboard that supports multiple data sources, including Prometheus, InfluxDB, Graphite, Azure Monitor, and Google Cloud Monitoring. Additionally, Grafana offers various plugins and extensions for integration with systems like Zabbix, Percona, AWS IoT TwinMaker, and Bosun. Finally, Telegram is used for smart phone notification. Telegram offers several distinct advantages over others, particularly for professional and technical applications such as network monitoring and automated notifications. Telegram is open and well-documented Bot API, which allows seamless integration with external systems like Grafana for real-time alerts and automated interactions. Telegram also excels in cloud storage, enabling users to access messages and files from multiple devices simultaneously without relying on local storage or continuous phone connectivity. This multi-platform support is crucial for IT teams who need constant access to notifications across desktops, tablets, and mobile devices. Telegram allows sending files up to 2 GB and supports various file types, which is particularly useful for sharing logs, reports, or system backups. Additionally, Telegram provides advanced privacy controls and highly customizable notification settings, giving users more control over how and when they receive alerts. These features make Telegram a more efficient, scalable, and reliable choice for real-time network monitoring notifications and collaborative problem-solving in professional environments [14], [15].

METHOD

The research methodology is illustrated in Figure 1. The preliminary actions undertaken involve the installation and configuration of Prometheus, SNMP Exporter, Grafana, and Telegram. Prometheus is an open-source monitoring and alerting toolkit widely used for collecting metrics from network devices, servers, and services in real-time [16]. In this research, Prometheus plays a central role by continuously scraping and storing time-series data from the network devices at DSTI. Its core strength lies in its capability to query and retrieve metrics efficiently using its own query language, PromQL. This allows detailed tracking of various parameters such as network uptime, packet loss, CPU usage, and bandwidth. Prometheus also manages alerting rules, which define thresholds or conditions under which certain actions, such as notifications, should be triggered. Prometheus has been installed and setup on the DSTI server, and subsequently integrated with the SNMP Exporter, which has also been installed and configured on the DSTI server. Upon the execution of the SNMP Exporter job in Prometheus, the data collected by Prometheus will be viewed in Grafana and coupled with Telegram as a notification medium for the alert system. Visualizing data or information concerning Grafana network devices necessitates input from the Prometheus data source for integration with the data or information possessed by Prometheus. A dashboard is then established to facilitate the reading of all data or information. Upon the dashboard's presentation resulting from the monitoring system design, the subsequent step is to evaluate the issues within the network monitoring system of Building A, FPTK UPI, which aims to identify obstacles or problems promptly to assist the network administrator in addressing any encountered challenges. The test was conducted by severing the Ethernet connections of the two routers located on the first level, which are linked to the router on the second floor to the north. The problem scenario is replicated using PNETLab software, viewed through Grafana, and delivers notifications to Telegram via the administrator's smartphone.

Upon detecting an issue, such as the loss of connectivity to a network device, the SNMP Exporter will automatically transmit a metric to Prometheus, which Grafana can then view on the established dashboard. The issue details displayed on the Grafana dashboard will trigger a notice message to the designated Telegram account. The connectivity of the malfunctioning network equipment will instantly resume as ether 3 serves as a backup for the disconnected ether 2. Grafana will automatically visualize the network connectivity status between the router on the first floor and the router on the second floor north, subsequently sending a notification to Telegram to indicate that the router on the second floor north is operational again. The final stage is to evaluate the problem-testing

scenario and rectify the connectivity issue of the network device in Building A, FPTK UPI. Draw conclusions based on the outcomes of the conducted analysis.

The test scenario for the connectivity issue of network devices in Building A, FPTK UPI is depicted in the topology illustrated in Figure 2. The scenario involved disconnecting Ethernet cable 2, which linked the router on the first level to the router on the second floor, in order to evaluate the operation of Grafana as a monitoring and alerting system.

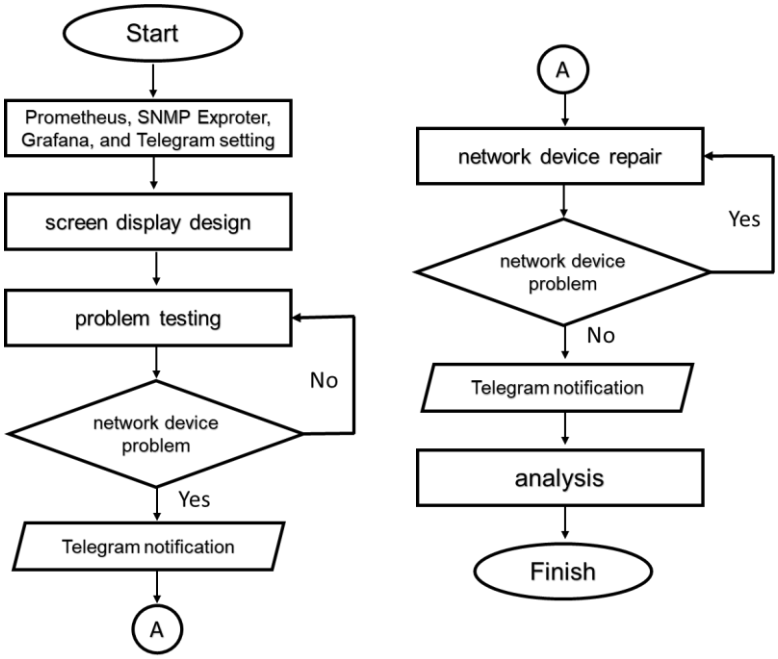

Figure 1. Research Methodology

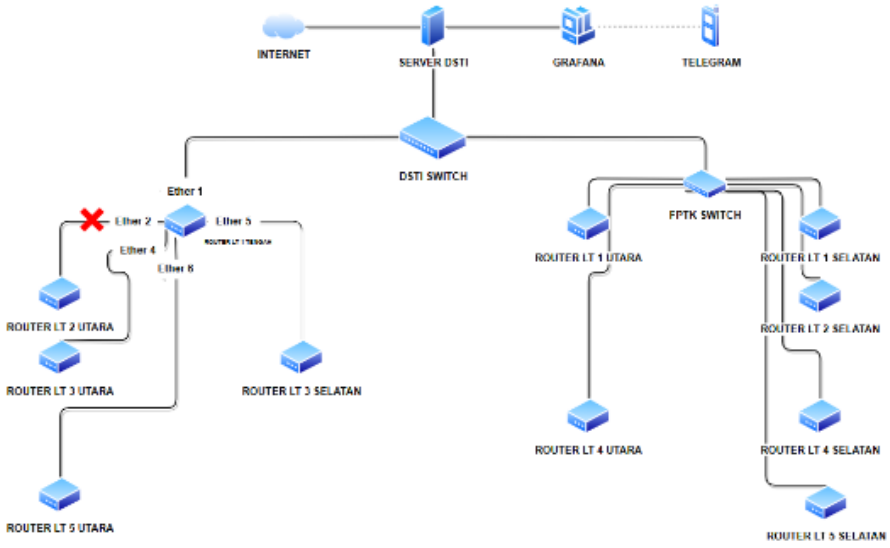

Figure 2. Network Topology for Device Connectivity Testing in Building A, FPTK UPI

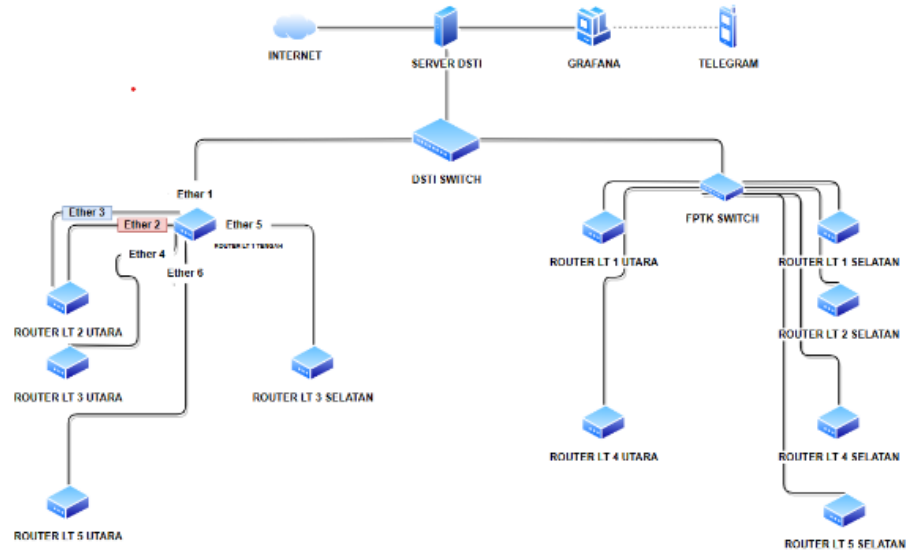

Figure 3. Testing Scenario Topology for Repairing Network Device Connectivity in Building A, FPTK UPI

The topology depicted in Figure 3 is the test scenario for restoring network connectivity in Building A, FPTK UPI. The repair scenario involves the addition of one connectivity, specifically ether 3, from the router on the first floor in the middle to the router on the second floor in the north. This serves as a fallback for the internet network, which is equipped with two connectivity points on the second floor in the north. When ether 2 is disconnected, ether 2 will automatically assume responsibility for establishing internet network connectivity from the router on the first floor in the midsection to the second floor in the north.

RESULT AND DISCUSSION

The results of the design of the network device monitoring system in Building A, FPTK UPI using Grafana are displayed in Figure 4. The display of the network device monitoring system is in the form of a dashboard because it was designed using Grafana. The information that is displayed on the Grafana dashboard comes from one of the routers that are situated in Building A FPTK UPI. More specifically, the router that is situated on the midst of the first floor. On the first level, in the middle, the Grafana dashboard includes data on the router, data on traffic interfaces, and data on the interfaces on the router. These are the parameters that are contained within the dashboard.

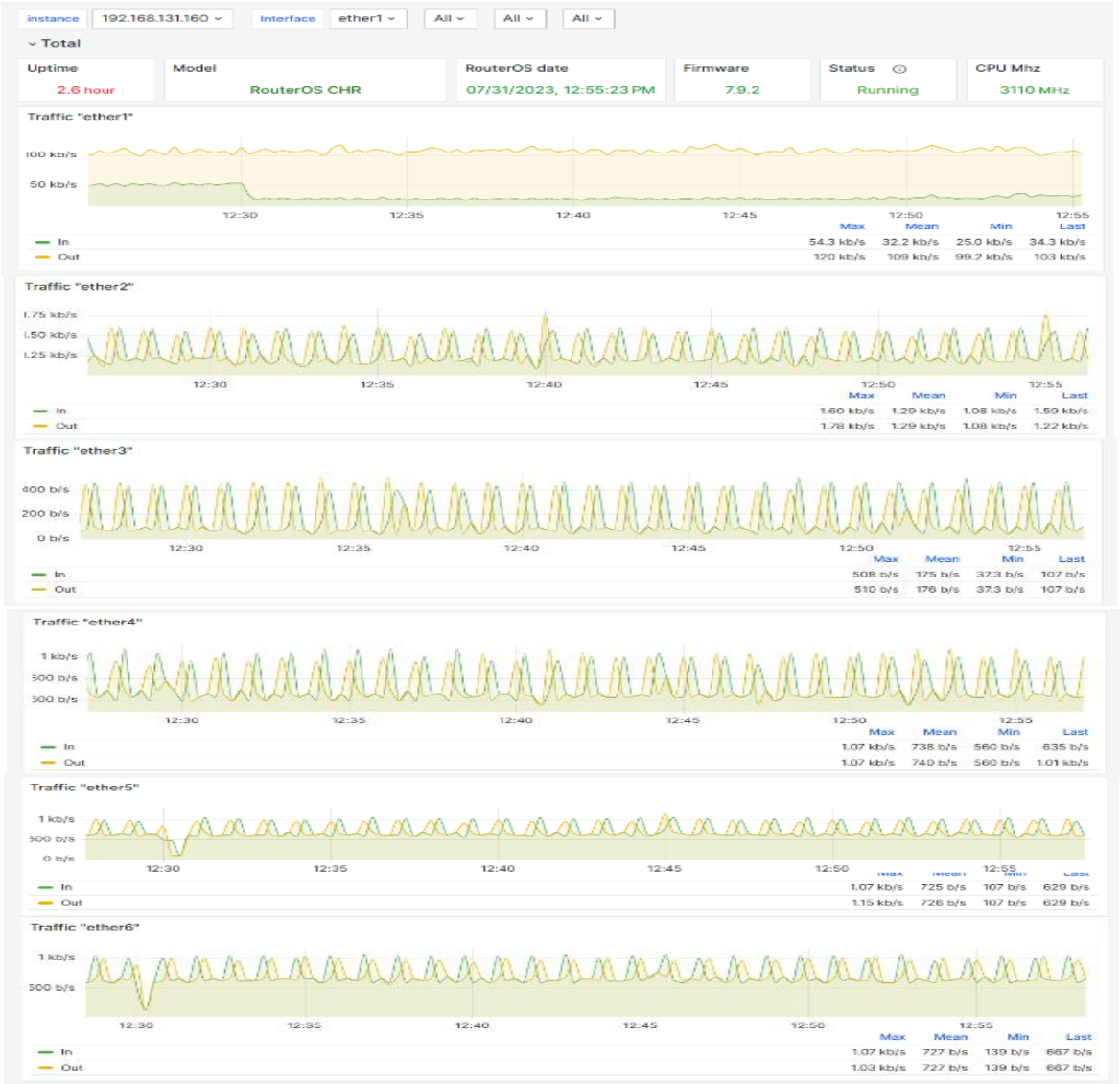

Figure 4. Network Monitoring System Results of Building A, FPTK UPI

Interfaces

Name	Status link/states	Link down count	MAC	Rate
ether1	UP	0	50:B6:38:00:11:00	1 Gb/s
ether2	UP	0	50:B6:38:00:11:01	1 Gb/s
ether3	UP	0	50:B6:38:00:11:02	1 Gb/s
ether4	UP	0	50:B6:38:00:11:03	1 Gb/s
ether5	UP	0	50:B6:38:00:11:04	1 Gb/s
ether6	UP	0	50:B6:38:00:11:05	1 Gb/s

Figure 5. Network Monitoring System Interface of Building A, FPTK UPI

Interface data is displayed in Figure 5. This data includes the name of the interface that is on the router, the link status and states that indicate whether or not an interface on the router is active, the link down count that indicates the number of interfaces that are disconnected, the media access control (MAC) that indicates the identity of the interface that is owned by the router, and the rate that indicates the speed of the interface that is owned by the router.

The results of the network device testing conducted on the Building A, FPTK UPI are illustrated in Figure 6. The issue is that ether 2, which is connected to the router on the second floor north, is rendered inoperable, preventing the internet network from passing through it. At 13:03:30 PM, the Grafana dashboard displays a graphic visualization of ether 2 traffic. The graph indicates that ether 2 encountered a decrease in traffic and did not receive any traffic after being disconnected. The interface information on the middle floor 1 router is depicted in Figure 7, following the disconnection of ether 2. In the Status link/states column, the disconnected ether is indicated in red. The warning result is a problem message that is transmitted by DSTIbot via Telegram, as illustrated in Figure 8. The message sent by DSTIbot contains the string "R_LT2_UTARA | Down," which indicates that the north 2nd floor router's connectivity has been disrupted.

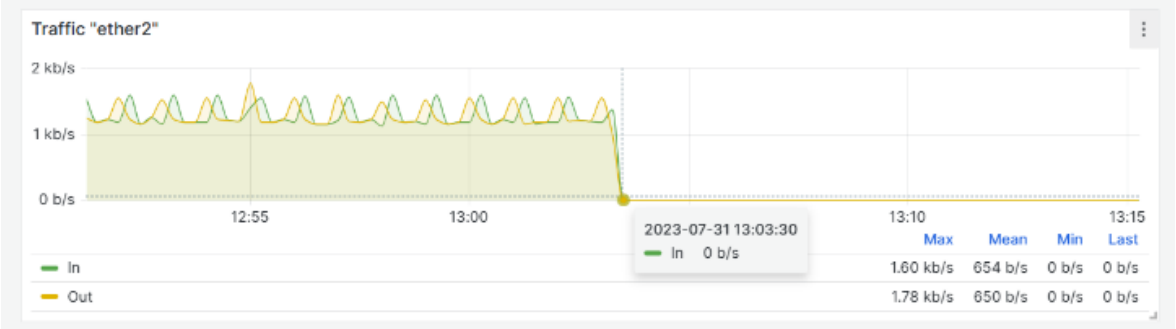

Figure 6. Testing Issues on Network Devices in Building A, FPTK UPI

Interfaces

Name	Status link/states	Link down count	MAC	Rate
ether1	UP	0	50:B6:38:00:11:00	1 Gb/s
ether2	DOWN	1	50:B6:38:00:11:01	0 b/s
ether3	UP	0	50:B6:38:00:11:02	1 Gb/s

Figure 7. Information on Interface Traffic Data for Network Device Problem Testing in Building A, FPTK UPI

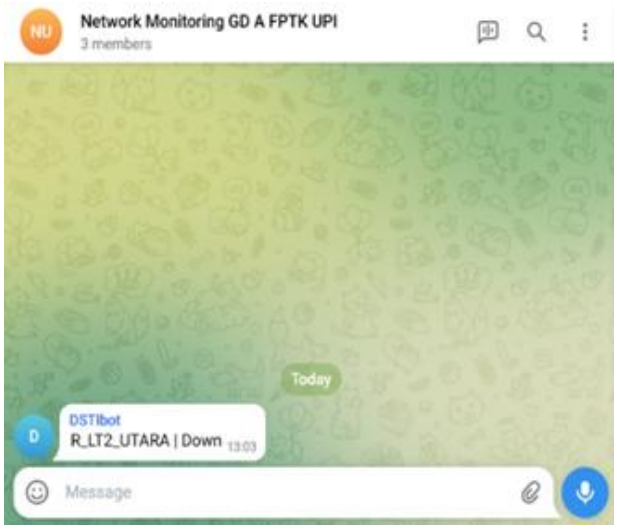

Figure 8. Telegram Notifications When Network Problems Occur

Figure 9. Interface of the Repaired Network Device of Building A, FPTK UPI

The results of the repair of the network device problem in Building A, FPTK UPI are illustrated in Figure 9. In this case, ether 3 has been connected to the router on the second floor north and is configured on the router on the first-floor center to function as a backup when ether 2 is disconnected. At 13:04:00 PM, the Grafana dashboard displays a graphic visualization of ether 3 traffic. The graph indicates that ether 3 encountered an increase in traffic and received traffic after ether 2 was disconnected. The router on the first-floor center's interface information is depicted in Figure 10, following the disconnection of ether 2. In the Status link/states column, the disconnected ether is indicated in red. Ether 3, which serves as a fallback and is also connected from router 1 on the first-floor center to the router on the second floor north, remains on the green side, indicating that the ether is operational.

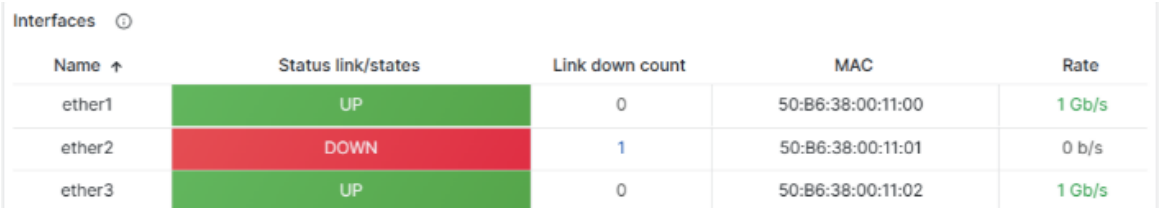

Figure 10. Display of Traffic Data Regarding the Repair of Network Devices in Building A, FPTK UPI

Table 1. Interface Traffic Data

Interface name	Max	Mean	Min	Last
Ether 3 (in)	1.63 kbps	682 bps	37.3 bps	1.22 kbps
Ether 3 (out)	1.59 kbps	683 bps	37.3 bps	1.22 kbps

Figure 11. Telegram Notification When the Network Has Been Repaired

Interface traffic data is displayed in Table 1 when ether 3 is connected to the north second floor router as a backup. The most recent traffic data recorded by Grafana indicates that ether 3 has the highest traffic (in) value (Max) of 1.63 kb/s, the highest traffic (out) value (Max) of 1.59 kb/s, the average traffic (in) value (Mean) of 682 b/s, and the average traffic (out) value (Mean) of 683 b/s. The lowest traffic (in & out) value (Min) is 37.3 b/s, and the most recent traffic (in & out) value (Last) is 1.22 kb/s.

An alert notification in the form of a maintenance message sent by DSTIbot via Telegram will be displayed to indicate that the issue has been resolved, as illustrated in Figure 11. The disruption in the connectivity of the north 2nd floor router has been resolved with the presence of ether 3 as a fallback, as the message sent by DSTIbot is R_LT2_UTARA | Up. This is due to the fact that the north 2nd floor router has received internet access from ether 3.

CONCLUSION

A dashboard for the middle 1st floor router is used to display the results of the network device monitoring system design for Building A, FPTK UPI using Grafana software. Router data, traffic interface data, and interface data comprise the Grafana dashboard's parameters. Uptime, Model, RouterOS date, Firmware, Status, and CPU MHz comprise router data. The data from the traffic interface is presented in the form of a graph that includes ether 1 traffic, ether 2 traffic, ether 3 traffic, ether 4 traffic, ether 5 traffic, and ether 6 traffic. The interface data on the router includes the name of the interface, status link/states, link down count, MAC address, and rate. The network device of Building A FPTK UPI, specifically ether 2, which is connected to the north 2nd floor router, is disabled during the testing process. This causes the internet network to be unable to travel through ether 2, resulting in the north 2nd floor router being unable to access the internet network. Consequently, the data on the ether 2 interface on the dashboard is reported as DOWN. Also, a message notification from DSTIbot via Telegram containing R_LT2_UTARA | Down is displayed as a warning of the issue. The issue with the network device of Building A, FPTK UPI, specifically ether 3, which is a fallback connected to the router on the second floor north, is being resolved. This led to an increase in traffic on ether 3, which continued to receive traffic after ether 2 was disconnected. Additionally, a warning is provided to address the issue of displaying a message notification from DSTIbot via Telegram that includes R_LT2_UTARA | Up.

Moreover, future research can explore the implementation of intelligent fault prediction models using machine learning algorithms based on the historical data collected through Grafana and Prometheus. By analyzing patterns such as traffic fluctuations, link down counts, and CPU load over time, predictive analytics could be developed to forecast potential failures before they occur, improving proactive maintenance strategies. Research can be conducted to enhance the responsiveness of the alerting system by integrating anomaly detection frameworks that can distinguish between normal and abnormal network behavior, minimizing false positives in Telegram notifications.

REFERENCES

[1] K. Thakur, A.-S. K. Pathan, and S. Ismat, “An overview of ICT technology advancement,” in *Emerging ICT Technologies and Cybersecurity*, Cham: Springer Nature Switzerland, 2023, pp. 1–43. doi: 10.1007/978-3-031-27765-8_1.

[2] M. Stephens, “Unmasking the subconscious fallacies within critical infrastructure protection,” *European Conference on Cyber Warfare and*

Security, vol. 23, no. 1, pp. 752–758, Jun. 2024, doi: 10.34190/eccws.23.1.2213.

[3] B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde, "Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges," *Cybersecurity*, vol. 7, no. 1, p. 10, May 2024, doi: 10.1186/s42400-023-00200-w.

[4] Y. Wan, C. Feng, K. Wu, and J. Wang, "Towards easy-to-monitor networks: network design and measurement path construction," *IEEE Trans Netw Sci Eng*, vol. 11, no. 5, pp. 4397–4412, Sep. 2024, doi: 10.1109/TNSE.2024.3418781.

[5] X. Li, K. Li, Y. Ding, D. Wei, and X. Ma, "Application of autonomous monitoring method based on distributed environment deployment in network fault," *J Phys Conf Ser*, vol. 1486, no. 2, p. 022048, Apr. 2020, doi: 10.1088/1742-6596/1486/2/022048.

[6] M. Asassfeh *et al.*, "An overview of tools and techniques in network forensics," in *2024 25th International Arab Conference on Information Technology (ACIT)*, IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/ACIT62805.2024.10876996.

[7] M. A. Musarat, A. M. Khan, W. S. Alaloul, N. Blas, and S. Ayub, "Automated monitoring innovations for efficient and safe construction practices," *Results in Engineering*, vol. 22, p. 102057, Jun. 2024, doi: 10.1016/j.rineng.2024.102057.

[8] V. R. Kebande, N. M. Karie, and R. A. Ikuesan, "Real-time monitoring as a supplementary security component of vigilantism in modern network environments," *International Journal of Information Technology*, vol. 13, no. 1, pp. 5–17, Feb. 2021, doi: 10.1007/s41870-020-00585-8.

[9] M. I. Zakaria, W. A. Jabbar, and N. Sulaiman, "Development of a smart sensing unit for LoRaWAN-based IoT flood monitoring and warning system in catchment areas," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 249–261, 2023, doi: 10.1016/j.iotcps.2023.04.005.

[10] R. Irawansyah, K. Khairil, and R. T. Alinse, "Designing a computer network monitoring system with SMS notifications using the dude," *Jurnal Komputer, Informasi dan Teknologi*, vol. 3, no. 2, Dec. 2023, doi: 10.53697/jkomitek.v3i2.1494.

[11] S. Taftazanie, A. B. Prasetijo, and E. D. Widianto, "Aplikasi pemantau perangkat jaringan berbasis web menggunakan protokol SNMP dan notifikasi SMS," *Jurnal Teknologi dan Sistem Komputer*, vol. 5, no. 2, p. 62, May 2017, doi: 10.14710/jtsiskom.5.2.2017.62-69.

[12] E. G. Rani and D. T. Chetana, "Using GitHub and Grafana Tools: Data Visualization (DATA VIZ) in Big Data," in Computer Vision and Robotics, P. K. Shukla et al., Eds. Singapore: Springer, 2023, ch. 38, pp. 477–491. doi: 10.1007/978-981-19-7892-0_38.

[13] M. Chakraborty and A. P. Kundan, "Grafana," in *Monitoring Cloud-Native Applications*, Berkeley, CA: Apress, 2021, pp. 187–240. doi: 10.1007/978-1-4842-6888-9_6.

[14] M. Á. Conde, F. J. Rodríguez-Sedano, F. J. Rodríguez Lera, A. Gutiérrez-Fernández, and Á. M. Guerrero-Higueras, "WhatsApp or telegram. which is the best instant messaging tool for the interaction in teamwork?," in *Proc. Int. Conf. Human-Computer Interaction*, vol. 12784, Springer, 2021, pp. 239–249. doi: 10.1007/978-3-030-77889-7_16.

[15] M. Barthelmäs, M. Killinger, and J. Keller, "Using a Telegram chatbot as cost-effective software infrastructure for ambulatory assessment studies with iOS and Android devices," *Behav Res Methods*, vol. 53, no. 3, pp. 1107–1114, Jun. 2021, doi: 10.3758/s13428-020-01475-4.

[16] M. Chakraborty and A. P. Kundan, "Architecture of a modern monitoring system," in *Monitoring Cloud-Native Applications*, Berkeley, CA: Apress, 2021, pp. 55–96. doi: 10.1007/978-1-4842-6888-9_3.