

---

## **Development Of Netwatch Host Using Telegram As A Strengthening Model Of Institutional Performance Quality Governance**

**Alek Wijaya<sup>1)\*</sup>, Ade Kemala Jaya<sup>2)</sup>, Dinda Ayu Ningsih<sup>3)</sup>, Doli Lyanda<sup>4)</sup>**

<sup>1)4)</sup>Informatic Engineering, Computer Science, Universitas Bina Darma, Indonesia

<sup>2)3)</sup>Management, Economy, Universitas Bina Darma, Indonesia

<sup>1)</sup>[alex\\_wj@binadarma.ac.id](mailto:alex_wj@binadarma.ac.id), <sup>2)</sup>[adekemalajaya@binadarma.ac.id](mailto:adekemalajaya@binadarma.ac.id), <sup>3)</sup>[dindaayuningsih97gmail.com](mailto:dindaayuningsih97gmail.com),

<sup>4)</sup>[dolil.yanda2000mail@gmail.com](mailto:dolil.yanda2000mail@gmail.com),

---

### **ABSTRACT**

Improving the quality of an institution's performance is very dependent on the facilities implemented in carrying out its work process. Currently, the facility being developed at the institution is by implementing IoT technology that utilizes various types of IoT devices. However, most institutions have not been able to monitor every IoT device used so that it also affects the quality of performance of the institution. Therefore, in the study, the Network Development Life Cycle (NDLC) method is used., researchers made efforts to strengthen the institutional performance quality governance model. The researchers developed Netwatch Host technology using Telegram, which is intended to monitor the condition of each IoT device in the institution and then send details of the condition via the Telegram Application. This is intended so that the IoT devices used by employees can be maintained so that they can respond quickly when there is an IoT device that is down or has a problem.

**Keywords:** Netwatch; Telegram; NDLC Method; IoT; Strengthening Model;

---

### **1. INTRODUCTION**

In this Multidisciplinary Research, researchers collaborated between the Research Road Map from the Informatics Engineering Study Program and the Research Road Map from the Accounting Study Program. Therefore, the theme of this research is Technology Development to Strengthen Governance Models in Improving the Quality of Institutional Performance. In the process of improving performance quality, of course, currently most institutions have implemented the use of IoT devices to support their work processes. However, these institutions have not yet implemented a system that can monitor the condition of the IoT devices they use. Therefore, researchers want to optimize the existing system by first analyzing the network,

In this study, the researchers used the Network Development Life Cycle (NDLC) approach., which designed and implemented the method. After the researcher gets an overview of the method used with the observations made at the institution, the researcher will implement the idea or design that will be carried out. The data collection method is by making observations, namely taking data directly from institutions, especially IoT device data contained in institutions. By using the netwatch host, researchers can monitor the condition of the IoT device connection without having to always look at the Monitoring System. After that, researchers can use mobile-based notifications, namely utilizing the Telegram application as a security system in institutional performance governance.

It should be noted that hosts include computers and electronic devices that are connected to networks, both computers and other electronic devices, hosts that are found in institutions in general, namely access points, computers, laptops, and smartphones. After the researcher knows the connected host, the researcher will focus on the host which is the main requirement which can support the institution's work processes. Hosts are the main requirement to help improve institutional performance, which requires flexible connections, namely access points.

IoT device connections should be monitored to help employees work across organizations and improve performance on the maintenance side, so employees don't need to remotely connect to IoT devices for continuity monitor the server's permissions. Monitoring using notifications really helps employees know the status of servers on the network. Notifications for network monitoring have various alternatives like email, SMS and social media. Considering how email works are less flexible for tracking and SMS is rarely used, the author uses social media notifications that are commonly used as messages, namely telegrams.

\* Corresponding author



Netwatch host is a system for monitoring hosts using the NetWatch tool (Fathur, Setiadie Wiriaatmadja, & Ratama, 2022; Fauzi, 2019; Rahman, Khudori, Nurdin, & Qomaruddin, 2022). This Netwatch host can monitor IoT devices connected to the local network by entering the IP address of a host (Sulistyo & Sutanto, 2018). Telegram is a popular messaging service based on open source platform introduced in 2013 by Russian Pavel Durov (Fahana, Umar, & Ridho, 2017). Telegram is an application that allows users or users to send messages quickly and safely (Nalakhudin, Imron, & Wiedanto Prasetyo, 2021; Ratnasari, Ciptadi, & Hardyanto, 2021). Telegram can also be said to be an application that provides a cloud-based multi-platform instant messaging service that is non-profit and free (Irsyam, 2019; Panjaitan & Syafari, 2019). The governance model is a model which is a collection of rules and ways to implement procedures and operational standards in achieving strategic goals (Fahana et al., 2017).

As for conducting this research, it certainly requires several case examples that have been generated from several previous studies, Research that has been carried out by Tommi Alfian Armawan Sandi, Sujiliani Heristian and Ilham Nur Leksono resulted in a Netwatch development to optimize failover on proxy (Sandi, Heristian, & Leksono, 2021). The research results obtained by Agung Sulistyo and Felix Andreas Sutanto are the Utilization of Telegram Bot at BMKG in developing a warning system for connectivity disruptions (Sulistyo & Sutanto, 2018). Research conducted by Ridha Fachsal Noor, who integrated netwatch with telegram in implementing network device monitoring at the Karimun Regency DPRD (Havest, 2020).

This research has several objectives that can be described (Sujadi & Mutaqin, 2017), namely as follows, First knowing the types of IoT devices as facilities that affect the quality of institutional performance (Sanjaya & Setiyadi, 2019), Second knowing how netwatch host technology works with telegram in monitoring the condition of IoT devices in institutions (Yudi & Budi Prakoso, 2020). Third Understand the effect of controlled IoT device conditions in strengthening the governance model to improve institutional performance (Prayitno & Lubis, 2020).

From the objectives that have been described, it is hoped that this research can provide the following benefits, First Get to know IoT devices that affect the quality of institutional performance, Second Can understand how netwatch hosts work using telegrams as notifications for monitoring the condition of IoT devices. Third Being able to understand the condition of work facilities in the form of IoT devices has an effect on improving the quality of institutional performance (Eko Nugroho & Daniarti, 2021).

## 2. LITERATURE REVIEW

There are several studies into previous research in this study. For the first research is research conducted by Tommi Alfian, Armawan Sandi, Sujiliani Heristian and Ilham Nur Leksono, where in this research the researchers conducted research related to a Netwatch development which aims to optimize Failover on Proxy can also be said in designing this network testing system implement failover optimization using netwacth on proxy. In the first test in this study, the researcher tested disable and enable interfaces that could be used to change the traffic flow if one of the ISPs was disconnected for a long time until it was active again, which made it difficult to predict when the ISP was down, but by using failover in this study, the researchers succeeded in using netwatch between the main and backup ISPs to anticipate ISP failures, as evidenced by the absence of a decrease in traffic (Sandi et al., 2021).

The next research is research conducted by Agung Sulistyo and Felix Andreas Sutanto where researchers used Telegram bots at BMKG which aims to develop a warning system for connectivity disturbances. Where the purpose of this research is to make it easy for technicians or network admins to get information faster when a disturbance occurs so that efficiency and effectiveness in handling network disturbances can be increased by monitoring equipment such as routers, the system will also test connections every interval on a network which is in the Netwatch system which integrates the Telegram API for notifications such as changes in traffic status on a network to technicians or admins. This study aims to make it easier for technicians or network admins to get information more quickly if a disturbance occurs, thereby increasing efficiency and effectiveness in handling network disturbances. By monitoring equipment such as routers, the system will test connections every certain interval on the network connections that exist in the Netwatch system. The system integrates the Telegram API as a notification medium when there is a change in status and notifies network traffic information to technicians or admins (Sulistyo & Sutanto, 2018).

The last research is research conducted by Ridha Fachsal Noor who integrates netwatch with telegram monitoring of network devices in the Karimun Regency DPRD. It is clear that in this study the researchers carried out monitoring of network devices using Netwatch which was integrated with an application in the form of Telegram by making the Karimun Regency DPRD office the object of research. The purpose of this research itself is to minimize the duration of troubleshooting at access points on a network with stages starting from the research preparation stage,

\* Corresponding author

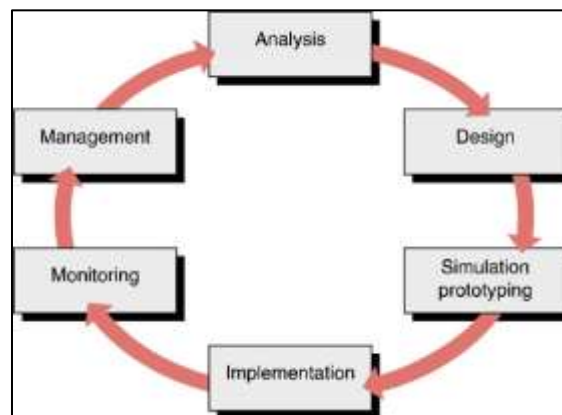


the data collection stage and the research implementation stage. The result of this research itself is in the form of a system that can help a technician or in carrying out monitoring tasks in real time without having to be on a server monitor for 24 hours (Havest, 2020).

It is from the three previous studies that underlies the researchers to conduct research in order to develop Netwatch hosts using telegrams as a model for strengthening performance quality governance in an institution where the South Sumatra University campus is the object of this study. The method used in this research is the Network Development Life Cycle (NDLC) method. The result is a monitoring system that speeds up the Network Administrator in identifying errors that occur at the University of South Sumatra, helping to find fault points and fixing them. And through this system, information is sent via telegram or telegram notification as long as it is connected to the internet at a time that depends on several factors, one of which is internet connection.

### 3. METHOD

In this multidisciplinary study a Network Development Life Cycle (NDLC) approach is used with an emphasis on action research to be implemented in the network. Network Development Life Cycle (NDLC) is one of the methods used in network deployment and development (Mulyanto & Prakoso Budi, 2020). The Network Development Life Cycle (NDLC) has six stages as follows:



**Figure 1.** NDLC Method Cycle

- 1) Analysis, is the first stage carried out by researchers including problem analysis and data collection related to IoT devices in institutions. In addition, researchers also studied several previous studies as the basis for conducting this research.
- 2) Design, is the second stage that the researcher is doing, where in this design stage a description of the architecture, the IoT device scheme and the design of the netwatch host technology will be made using the proposed telegram.
- 3) *Simulation Prototyping*, is the third stage that researchers do, which is on This simulation stage will build a prototype system from netwatch host with telegram to be tested.
- 4) Implementation, is the fourth stage yang researchers do, which at this stage design specifications will be carried out at the institution that will be carried out includes the installation of the netwatch host configuration, telegram and the installation of the IoT device configuration.
- 5) *Monitoring*, is the fifth stage that researchers carry out, in which at this monitoring stage tests are carried out on IoT device infrastructure and netwatch hosts that have been implemented or implemented in institutions whether they are running or not.
- 6) Governance is the sixth step that scholars take, in which, at this stage of management, political issues are adjusted so that the established system can be properly maintained.

\* Corresponding author



#### 4. RESULT & DISCUSSION

##### 3.1. Monitoring

After carrying out the next implementation stage, the monitoring phase will be carried out. In this chapter, the researcher will take action by testing the telegram monitoring system on physical devices and testing telegram-based SMS notifications built at the University of South Sumatra (USS).

##### 3.2 Monitoring Results and Response Time of Telegram Notifications

At this point, the author shows the results of the design of a telegram-based surveillance system that will generate a message.

##### 3.3 Monitoring Results

At this point, the author shows the results of designing a telegram-based surveillance system that will generate a message. The next step will display the current notification screen. the proof is that the APP telegram monitoring system screen shows the device status when the network fails and performs maintenance quickly so as not to waste much time.

##### 3.4 Test Scenario

There are several stages of the test scenario that will be carried out in the notification test, including the following

1. The first stage is to ensure that the device is on
2. The second stage is to ensure that the state of the network connection is normal
3. The third stage is to test the failure device
4. The fourth stage is testing by deciding to disconnect the host device link
5. The fifth stage is getting a down notification
6. The sixth stage turns on the link
7. The next step is getting a notification of an up
8. The last stage is if all the above scenarios have been implemented, the test is declared successful.

##### 3.5 Test Result Status

This test is done to check if the built system conforms to the previously given definition. The tests can be seen in the following table.

Tabel 1  
Test Result Status

No	Testing	Information	Results	Status
1	Down	The status of the device is up and the ping results are more than 3000 ms	The system sends a down message via the Telegram application to the user	Valid
2	Up	The device status is down and the ping result is less than 3000 ms	The system sends up messages via the Telegram application to users	Valid

Based on Table 1, there are 2 tests, namely the Down test and the Up test. Where in the Down test the device status is up and pinged for more than 3000 ms with the results of the system testing sending Down messages via Telegram to the user but the status is still valid. Whereas for the Up test the device status is down and the ping results are less than 3000 ms. With the results of the system sending an Up message on Telegram to the user, but similar to the previous test, the status in this test is still valid.








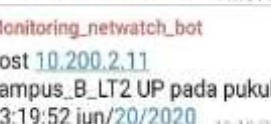
\* Corresponding author



**3.6 Response Time**

Based on the monitoring results, an analysis of the monitoring results will be carried out. Where this Response Time consists of Message Down Enter and Message Up Enter by taking into account the time difference. For this monitoring, it was carried out in the yards of campus A.1 to campus A.6 and in the yards of campus B LT.1 to LT.5 at the University of South Sumatra. For details, it can be seen in Table 2 below with the average time difference 5-7 seconds.






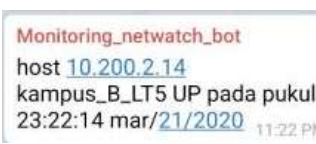
Table 2  
Response Time

No	Message Down Enter	Message Up Enter	Time Difference
1			7 sec
2			6 sec
3			7 sec
4			5 sec
5			6 sec
6			6 sec
7			5 sec
8			7 sec

\* Corresponding author





9			6 sec
10			7 sec
11			5 sec

### 3.7 Realtime Monitoring

On each device that is connected or disconnected, a notification will be given to the admin. Notifications will continue to run reporting conditions about the device. Realtime Monitoring itself consists of several Hostnames including Perangan\_campus\_A\_1, Yard\_campus\_A\_2, Background\_room\_campus\_A\_3 to Background\_room\_campus\_A\_6, campus\_B\_LT\_1 to campus\_B\_LT\_5 the results of realtime monitoring produced "YES" results. For details, see Table 3 below;

Table 3  
Realtime Monitoring

No	Host Name	Real time display		Realtime
		Connect	Disconnect	
1	Perangan_campus_A_1	✓	✓	Yes
2	Yard_campus_A_2	✓	✓	Yes
3	Background_room_campus_A_3	✓	✓	Yes
4	Background_room_campus_A_4	✓	✓	Yes
5	Background_room_campus_A_4	✓	✓	Yes
6	Background_room_campus_A_5	✓	✓	Yes
7	Background_room_campus_A_6	✓	✓	Yes

\* Corresponding author



8	Campus_B_LT_1	✓	✓	Yes
9	Campus_B_LT_2	✓	✓	Yes
10	Campus_B_LT_3	✓	✓	Yes
11	Kampus_B_LT_4	✓	✓	Yes
12	Kampus_B_LT_5	✓	✓	Yes

### 3.8 Device Control Testing

Each connected device has a feature to restart the device or block the device. Device Control Testing consists of several Hostnames namely Ward\_campus\_A\_1, Yard\_campus\_A\_2, Background\_room\_campus\_A\_3 to Background\_room\_campus\_A\_6, campus\_B\_LT\_1 to campus\_B\_LT\_5 the result of this Device Control Testing is "Success". The test results can be seen from the data below:

Table 4  
Device Control

No	Host Name	Control		Results
		Reboot	Block ip	
1	Perangan_campus_A_1	✓	✓	Success
2	Yard_campus_A_2	✓	✓	Success
3	Background_room_campus_A_3	✓	✓	Success
4	Background_room_campus_A_4	✓	✓	Success
5	Background_room_campus_A_4	✓	✓	Success
6	Background_room_campus_A_5	✓	✓	Success
7	Background_room_campus_A_6	✓	✓	Success
8	Campus_B_LT_1	✓	✓	Success

\* Corresponding author



9	Campus_B_LT_2	✓	✓	Success
10	Campus_B_LT_3	✓	✓	Success
11	Kampus_B_LT_4	✓	✓	Success
12	Kampus_B_LT_5	✓	✓	Success

### 3.9 Resource Usage

In using the router there are rules to control the network. The more rules, the more work the router will do, and if there are too many, the work of the router will be even harder. Because of that, detailed information on resource usage on the router is needed.

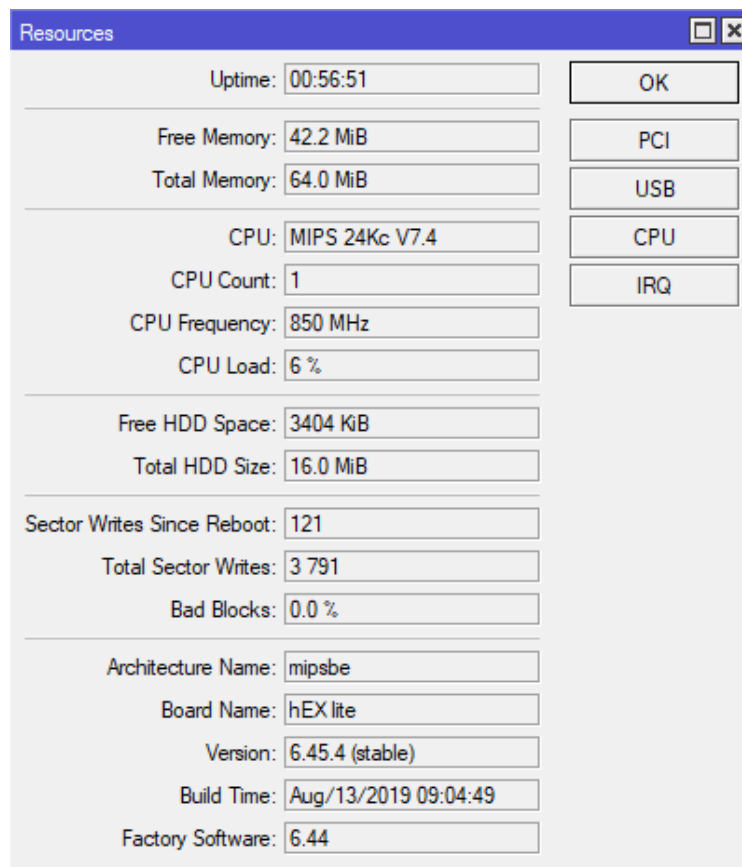


Figure 2 Resources

From the picture above, the use of memory resources is 43.3 mb of the 64.0 mb provided, then the CPU usage is 6%, thus the router's performance above is still quite good.

\* Corresponding author





**3.10 Recap of Access Point Monitoring Results**

To get the final results of the research conducted, a recap of the results of the 10-day monitoring data will be carried out on the date the monitoring system was implemented at the University of South Sumatra (USS), researchers will process the data into a single data unit. The data obtained for 10 days is shown in the following table.

Table 5  
 Recapitulates the results of monitoring access points for 10 days

Nama perangkat	Tanggal penelitian (2020)																			
	5 februari		6 februari		7 februari		8 februari		9 februari		10 februari		11 februari		12 februari		13 februari		14 februari	
	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN	DE	SN
Kampus_A_1	30	RTO	0	-	10	BF	0	-	0	-	0	-	0	-	0	-	0	-	0	-
Latar_K_A_2	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-
Latar_K_A_3	0	-	10	DU	0	-	0	-	0	-	0	-	40	DU	0	-	0	-	9	RTO
Latar_K_A_4	0	-	9	DU	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-
Kampus_B_1	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-
Kampus_B_2	0	-	0	-	0	-	0	-	0	-	0	-	0	-	10	RTO	0	-	0	-
Kampus_B_3	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-
Kampus_B_4	0	-	0	-	0	-	0	-	9	RTO	0	-	0	-	0	-	0	-	11	BF
Kampus_B_5	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	-	0	0

Information:

- DE* : Device error duration (minutes)
- SN* : Notification Status
- RTO* : Request timeout
- DU* : Destination unreasonable
- BF* : Boot failed

From the recap table of the University of South Sumatra (USS) monitoring access point data above, the researcher made a table comparing the breakdown time of each device, namely from 5 February 2020 to 14 February 2020 or within 10 days. The following is the result of a comparison of the number of times the device failed in the notification application research that the researcher did.

Table 6.  
 Duration of device error

Jenis gangguan	Kampus A_1	Latar K_A_2	Latar K_A_3	Latar K_A_4	Kampus B_1	Kampus B_2	Kampus B_3	Kampus B_4	Kampus B_5
Request Time gangguan	30 menit	-	9 menit	-	-	10 menit	-	9 menit	-
Destination unreachabled	-	-	50 menit	9 menit	-	-	-	-	-
Booting failure	10 menit	-	-	-	-	-	-	11 menit	-

\* Corresponding author



From the table above we can see the condition of the access point from day to day. The following is an explanation of the status of notifications that have been monitored using telegram notifications. From the data table above, we can see that for the condition of the access point network devices within 10 days of working hours they experience a few problems on their respective wireless devices, while the problems that are monitored in this study are Request time out (RTO) which in case of interference This is the condition that the access point device is experiencing interference, for example cables that are disconnected, disconnected, damaged connectors, switches and no internet connection on the device even though the device is running normally.

The next problem that arose during monitoring was boot failure, namely the condition of the access point, which experienced a hang/bootloop as was the case with the wireless device with the campus access point name\_A\_1 which had a similar problem, namely boot failure, which after being checked by the network administrator at the University of South Sumatra (USS), found that the wireless device from each access point that experienced this problem hangs/blanks. And the network administrator overcomes the problems experienced by the two devices by restarting the wireless device that had the previous problem, and waiting until the condition of the two access points is running normally again.

From this data table it can also be concluded that the device with the longest duration of problems is the device with the name Background\_K\_A\_3, which is having problems with the wireless device for 59 minutes within 10 days of research, and the device that has the least duration of device damage, namely the access point device with the name Kampus\_B\_4 with a duration of 20 minutes for device damage within 10 days of research. And for devices that during the research period did not experience any problems with access point devices, namely wireless devices with the names Background\_K\_A\_2, Kampus\_B\_1, Kampus\_B\_3, Kampus\_B\_5

Table 7  
RMA access point at the University of South Sumatra (USS)

NILAI	Kampus A_1	Latar K_A_2	Latar K_A_3	Latar K_A_4	Kampus _B_1	Kampus _B_2	Kampus _B_3	Kampus _B_4	Kampus _B_5
<b>REABILITY (MTTF)</b>	40 menit	0 MENIT	59 menit	9 MENIT	0 MENIT	10 menit	-	20 menit	-
<b>MAINTAINABILITY (MTTR)</b>	20 MENIT	0 MENIT	20 MENIT	9 menit	0 MENIT	5 MENIT	-	10 MENIT	-
<b>MEAN TIME BETWEEN FAILURE (MTBF)</b>	1180 MENIT	2400 MENIT	780 MENIT	2391 MENIT	2400 MENIT	1195 MENIT	2400 MENIT	1190 MENIT	2400 MENIT
<b>AVAILABILITY</b>	98,333%	100 %	97,50%	99,62%	100%	99,58%	100%	96,63%	100%

Information :

Reliability (mean time to failure / MTTF)

Maintainability (mean time to repair / MTTR)

Mean time between failure (total time the device was active)

10 research days = 2400 minutes

Availability =  $mtbf / (mtbf + mttr) * 100$

Access point with the name campus\_B\_4 l with a Reliability, Availability, and Maintainability (RMA) value of 96.63% are wireless devices that often experience problems or interruptions with their devices, with most of the problems occurring due to problems with cables and wireless devices that often cannot access the internet even though the status or condition of the device is alive and running normally. And conversely an access point with the name Background\_K\_A\_2, with a Reliability, Availability, and Maintainability (RMA) value of 100% is a very good device because in this 10-day study the condition of the access point always went well, did not experience any problems when monitoring the the device.

\* Corresponding author



## 5. CONCLUSION

Based on research that has been done by researchers, this telegram notification-based monitoring system for network devices can speed up the performance of the Network Administrator in identifying some of the errors that exist, for example errors that occur on the local network at the University of South Sumatra (USS), especially on the Host Access Point. Not only that, through monitoring network devices, Network Administrators can also find fault points and fix disturbances that occur on the local network. Even when each device is suddenly disconnected, the system will immediately send a telegram message notification to the Network Administrator, which can then assist them in maintaining network stability. In terms of this monitoring, researchers need an internet connection to be able to run the telegram application which is used in the process of sending notifications from monitoring results, this internet connection is also a factor that determines the time of sending notifications from the system to the telegram application which is handled by a Network Administrator.

## 6. REFERENCES

- Eko Nugroho, F., & Daniarti, Y. (2021). Rancang Bangun Qos (Quality Of Service) Jaringan Wireless Local Area Network Menggunakan Metode Ndlc (Network Development Life Cycle) Di Pt Trimitra Kolaborasi Mandiri (3kom). *Jika (Jurnal Informatika)*, 5(1), 79. <https://doi.org/10.31000/Jika.V5i1.3970>
- Fahana, J., Umar, R., & Ridho, F. (2017). Pemanfaatan Telegram Sebagai Notifikasi Serangan Untuk Keperluan Forensik Jaringan. *Jurnal Sistem Informasi*, (6), 2.
- Fathur, M., Setiadie Wiriaatmadja, J., & Ratama, N. (2022). Sistem Monitoring Jaringan Melalui Notifikasi Telegram Dengan Application Programming Interface (Api) Menggunakan Netwatch Mikrotik Pada Jaringan. *Oktal : Jurnal Ilmu Komputer Dan Sains*, 1(6), 771–781. Retrieved From <https://journal.mediapublikasi.id/index.php/Oktal>
- Fauzi, A. (2019). Analisis Kualitas Transmisi Data Pada E-Learning Streaming Multimedia Dengan Quality Of Service ( Qos ). *Seminar Nasional Inovasi Teknologi*, 93–106.
- Havest. (2020). Implementasi Monitoring Perangkat Jaringan Menggunakan Netwatch Terintegrasi Dengan Aplikasi Telegram Di Kantor Dewan Perwakilan Rakyat Daerah Kabupaten Karimun. *Jurnal Tikar No 2*, 1(2), 145–159.
- Irsyam, M. (2019). Sistem Otomasi Penyiraman Tanaman Berbasis Telegram. *Sigma Teknika*, 2(1), 81. <https://doi.org/10.33373/Sigma.V2i1.1834>
- Mulyanto, Y., & Prakoso Budi, S. (2020). Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawa Dengan Metode Network Development Life Cycle(Ndlc). *Jinteks (Jurnal Informatika Teknologi Dan Sains)*, 2(4), 223–233.
- Nalakhudin, K., Imron, M., & Wiedanto Prasetyo, M. A. (2021). Pemanfaatan Notifikasi Telegram Untuk Monitoring Perangkat Cctv Rumah Sakit Orthopaedi Purwokerto. *Technomedia Journal*, 6(1), 56–65. <https://doi.org/10.33050/Tmj.V6i1.1564>
- Panjaitan, F., & Syafari, R. (2019). Pemanfaatan Notifikasi Telegram Untuk Monitoring Jaringan. *Jurnal Simetris*, 10(2).
- Prayitno, M. H., & Lubis, H. (2020). Penerapan Logical Unit Number (Lun) Pada Drobo Virtual Storage Dengan Metode Network Development Life Cycle (Ndlc). *Explore: Jurnal Sistem Informasi Dan Telematika*, 11(1), 45. <https://doi.org/10.36448/Jsit.V11i1.1458>
- Rahman, T., Khudori, A., Nurdin, H., & Qomaruddin, M. (2022). Netwatch Mikrotik Pada Jaringan Pt Dinasti Kurnia Sejahtera. *Jusikom : Jurnal Sistem Komputer Musirawas*.
- Ratnasari, F., Ciptadi, P. W., & Hardyanto, R. H. (2021). Sistem Keamanan Rumah Berbasis Iot Menggunakan Mikrokontroler Dan Telegram Sebagai Notifikasi (Pp. 160–163).
- Sandi, T. A. A., Heristian, S., & Leksono, I. N. (2021). Optimalisasi Failover Dengan Netwatch Pada Mikrotik. *Conten : Computer And Network Technology*, 1(1), 23–30.
- Sanjaya, T., & Setiyadi, D. (2019). Network Development Life Cycle (Ndlc) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. *Mahasiswa Bina Insani*, 4(1), 1–10. Retrieved From <http://ejournal-binainsani.ac.id/>

\* Corresponding author



- 
- Sujadi, H., & Mutaqin, A. (2017). Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (Man) Dengan Menggunakan Metode Network Development Life Cycle (Ndlc) (Studi Kasus : Universitas Majalengka). *J-Ensitec*, 4(01). <https://doi.org/10.31949/J-Ensitec.V4i01.682>
- Sulistyo, A., & Sutanto, F. A. (2018). Warning System Gangguan Konektivitas Jaringan Pada Bmkg Semarang Dengan Telegram Bot. *Prosiding Sintak*, 126–133.
- Yudi, M., & Budi Prakoso, S. (2020). Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (Ndlc). *Jurnal Informatika Teknologi Dan Sains*, 2(4), 223–233.

\* Corresponding author



This is an Creative Commons License This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).