Jurnal Ilmiah Setrum

Volume 14, No.1, Juni 2025 **p-ISSN : 2301-4652 / e-ISSN : 2503-068X**

Data Communication Between PLC Using Internet-Based Modbus Protocol

Hudzaifi Fuad Ibrahim[1*], Asep Andang[1], Firmansyah MSN[1]

[1]Electrical Engineering, Faculty of Engineering, Siliwangi University, Tasikmalaya, Jawa Barat.

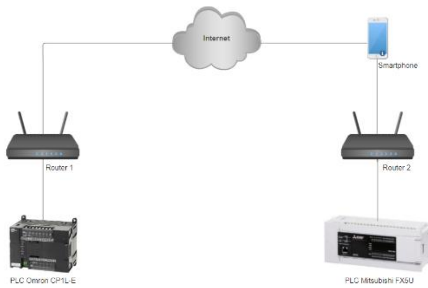
Informasi Artikel

Naskah Diterima : 16 Oktober 2024
Direvisi : 25 November 2024
Disetujui : 28 Mei 2025

doi: 10.62870/setrum.v14i1.29172

***Korespodensi Penulis :** hudzaifi21@gmail.com

Graphical abstract



Abstract

This study aims to analyze the performance of communication between Programmable Logic Controller (PLC) using Modbus TCP protocol over the internet. Mitsubishi FX5U PLC as Modbus client and Omron CP1L-E PLC as Modbus server. Tests were carried out by measuring quality of service (QoS) parameters such as delay, jitter, throughput, and packet loss according to TIPHON standards, with variations in the delay time of each request, namely 10 ms, 25 ms, 50 ms, 70 ms, 75 ms, 80 ms, and 100 ms. The test results show that the delay is between 36 ms to 61 ms with an average of 45 ms, which gives a TIPHON index value of 4. Jitter varies between 10 ms to 86 ms with an average of 56 ms, giving a TIPHON index value of 3. Packet loss is mostly 0%, except at delay of 10 ms and 25 ms with a result of 0.1%, giving a TIPHON index value of 4. Thus, the delay time of 75 ms is the most optimal choice with a delay value of 40 ms, jitter 68 ms, and packet loss 0%. This inter-PLC communication system is proven to be optimal and can be implemented in an industrial environment with good performance.

Keywords: PLC, Modbus TCP, delay, jitter, throughput, packet loss, industrial Communication

1. INTRODUCTION

Industrial automation has advanced significantly, with Programmable Logic Controller (PLC) becoming crucial for managing production processes[1]. The diversity of PLC from various manufacturers presents integration challenges due to differing technical specifications and communication protocols. Modbus, a commonly used protocol, facilitates data transmission but complicates interoperability between diverse PLC[2].

The internet has revolutionized industrial operations, enabling PLC to communicate using Modbus TCP/IP protocol over the internet for remote monitoring and control[3]. However, this integration may result in reduced communication quality and increased security risks, affecting system reliability.

Furthermore, This research is intended to investigates on how PLC specification differences and network constraints influence communication performance in industrial environments, while seeking optimal solutions for automation integration.

2. LITERATURE REVIEW AND METHODOLOGY

2.1 Literature Review

A. PLC

Programmable Logic Controller (PLC) is an industrial digital computer used for automation process[4]. The equipment components or parts of a PLC can be seen in the folowwing Figure 1.

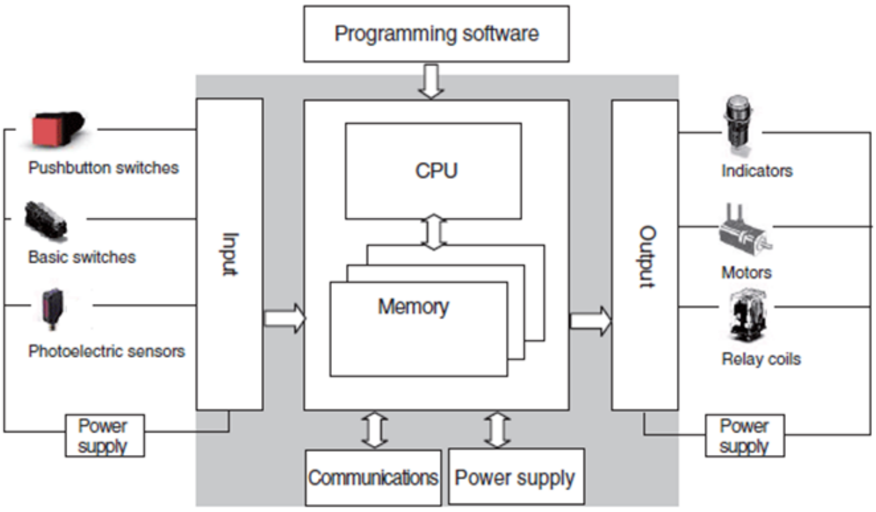


Figure 1. PLC Diagram

The CPU executes programs stored in the memory, while I/O modules handle data exchange between the memory and external devices like sensors and actuators. In this research, the PLCs used are the Mitsubishi FX5U and the Omron CP1L-E.

The Mitsubishi FX5U PLC, part of the MELSEC iQ-F series, is recognized for its high performance and integration capabilities. It is equipped with a robust Ethernet interface and supports advanced features such as PID control and motion control for up to four axes[5]. The FX5U offering scalability and enhanced data processing speeds. Specifications can be seen in table 1.

Table 1. Mitsubishi FX5U PLC specifications

No.	*Category*	*Description*
1.	Power Supply (V)	24V DC, 100-240V AC
2.	CPU Type	FX5U
3.	Program Memory Capacity	64K Steps
4.	Integrated Digital Inputs	32
5.	Integrated Digital Outputs	32
6.	Integrated Analog Inputs	2
7.	Instruction Processing Time (ns)	34
8.	Communication	Ethernet Port, RS-485
9.	Expansion Slot	8 Modules
10.	External Memory Port	SD Card Slot

The FX5U is programmed using GX Works 3, mitsubishi electric software for creating ladder diagrams (LD) and structured text (ST), which offers integrated debugging, simulation, and project management features[6].

Otherwise, the Omron CP1L-E PLC, known for its compact size and versatility, supports Ethernet communication and can be setup as a Modbus TCP/IP server or client, facilitating communication with other devices over a network[7]. Specifications can be seen in table 2.

doi : 10.62870/setrum.v14i1.29172

Table 2. Omron CP1L-E PLC specifications

No.	*Category*	*Description*
1.	Power Supply (V)	24V DC
2.	Data Memory	32 KB
3.	Program Memory	60 KB
4.	Integrated Digital Inputs	14
5.	Integrated Digital Outputs	10
6.	Integrated Analog Inputs	2
7.	Instruction Processing Time (ms)	≤ 1
8.	Communication	Ethernet Port, RS-485,RS-232
9.	Built-in Function	PID Control, Timer, Counter, and Logic Function
10.	External Memory Port	SD Card Slot

The CP1L-E is programmed using CX-Programmer, a software that supports multiple programming languages, including Ladder Diagram (LD), Function Block Diagram (FBD), and Structured Text (ST). This software provides functions for debugging, simulation, and real-time monitoring.

B. MODBUS TCP

Modbus TCP/IP is a widely implemented communication protocol used in industrial automation, designed to facilitate data exchange between devices over Ethernet networks[8]. Its architecture allows for seamless communication between various types of equipment, including Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), and other field devices, enabling the monitoring and control of industrial processes.

One of the key features of Modbus TCP/IP is its ability to operate over existing Ethernet networks, making it a cost-effective solution for both small and large-scale applications[9]. The protocol adheres to a client-server model where the client sends requests to the server to read or write data.

1. Message Format Stucture

The message format structure consists of two main components, the MBAP (Modbus Application Protocol) header and the PDU (Protocol Data Unit), as shown in the table below:

Table 3. Modbus TCP Message Format

Type	*Name*	*Description*
MBAP	Transaction ID	Unique identifier for the transaction.
	Protocol ID	Set to zero for Modbus
	Length	Total number of bytes in the message.
	Unit ID	Identifies the server device
PDU	Function Code	Indicates the action to be performed.
	Data	Contains addresses and values needed for the operation.

2. Function Codes

Function codes define specific operations within Modbus TCP/IP, as shown in the table below:

Table 4. Modbus TCP Function Codes

Code	Function	Description
01	Read Coils	Reads status of discrete outputs.
02	Read Discrete Inputs	Reads values from discrete inputs..
03	Read Holding Registers	Read a value from holding register.
04	Read Input Registers	Read a value from input register.
05	Write Single Coil	Writes a value to one coil.
06	Write Single Register	Writes a value to one holding register.
15	Write Multiple Coils	Writes a value to multiple coil.
16	Write Multiple Registers	Writes a value to multiple Register.
23	Read/Write Multiple Registers	Read and Writes a value to multiple Register.

3. Error Handling

Error handling is implemented through exception codes,as shown in the table below to communicate issues to the client.

Table 5. Modbus TCP Error Code

Code	Error	Description
01	Illegal Function	Unsupported function code
02	Illegal Data Address	Invalid requested address
03	Illegal Data Value	Unacceptable specified value
04	Server Device Failure	Unacceptable error on the server.

C. ROUTER

Router is a device that sends and receives data between networks by assigning local IP addresses to each device[10]. Its functions include connecting devices within the network, forwarding data packets, and ensuring that packets reach their intended destinations. The router used in this research is a D-Link router which can be seen in Figure 2.

Figure 2. D-link Router

Additionally, routers can serve as firewalls to protect the network from cyber attacks and help connect local networks to the internet [11]

D. WIRESHARK

Wireshark is an open-source software for network protocol analysis that allows users to capture and analyze network traffic in real-time[12]. Supporting various protocols such as TCP/IP, UDP, and Modbus TCP/IP, Wireshark aids in diagnosing network issues and identifying potential security threats. Its advanced features, such as display filters and filtering modes, enable specific analyses and investigations of data, including the decryption of encrypted packets [9]

2.2 Methodology

A. Research Flowchart

This flowchart discusses the method used for the author's research related to communication between PLCs using the internet-based Modbus TCP protocol. The main focus of this research is to analyze communication performance with TIPHON parameters. This research aims to test the performance of the communication system by involving two PLCs in different places and connected via the internet network.

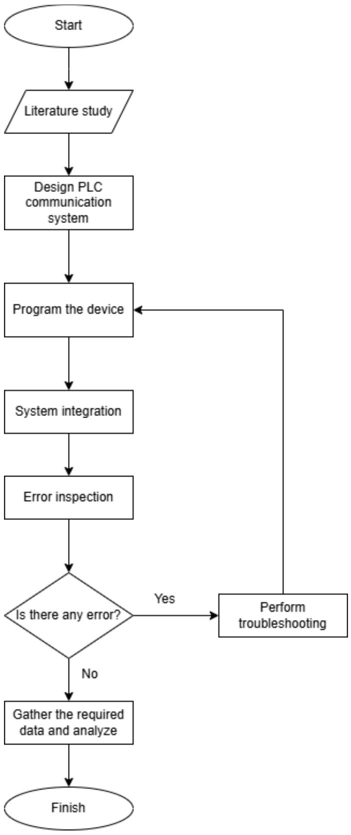


Figure 3. Research Flowchart

The flowchart represents the stages involved in the communication system testing process between PLCs using the Modbus TCP protocol. The process begins with the design of the communication system between the PLCs, followed by program configuration on each PLC. Once the system is configured, the next stage is system integration according to the design. After integration, error inspection is performed to ensure that the system is functioning as expected. If any errors are detected, the process will loop back to the appropriate stage for correction.Once the system is verified and functioning correctly, the final step involves data analysis.

B. Experiment Scenario

The design of the communication system between PLCs will be connected using the Modbus TCP protocol over the internet network. As can be seen in Figure 4 the two PLCs are connected to the internet through two different networks.

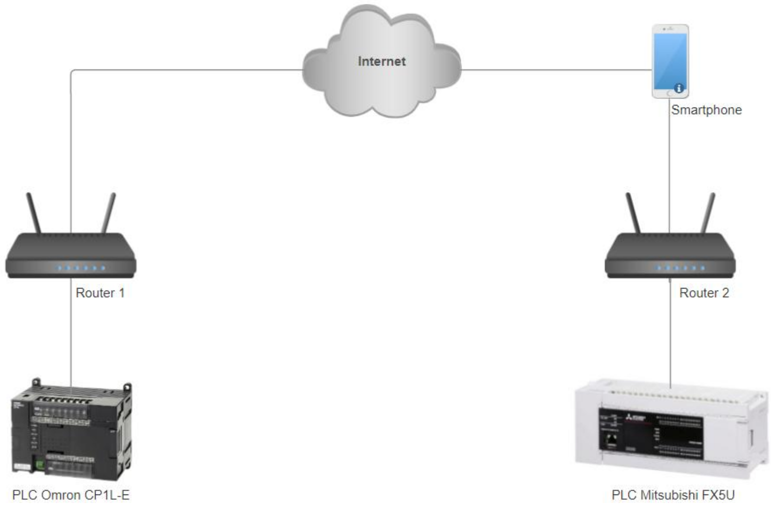


Figure 4. System Topology

It can be seen in Figure 4 that the design of the communication system that will be made using the Modbus TCP protocol via internet. The Omron CP1L-E PLC acts as a data storage device, which then sends the data to the Mitsubishi FX5U PLC. data transmission is carried out using the Modbus TCP communication protocol. The router is used as a connecting medium between devices in this system.

It should be noted that the internet connectivity for this system relies on two different network types, the Omron CP1L-E PLC is connected through a public IP network, while the Mitsubishi FX5U PLC is connected through a cellular data network. For the FX5U PLC, the Telkomsel network provider is used, utilizing a 4G cellular connection in Universitas Siliwangi 2, Kota Tasikmalaya. The average download speed is 37.3 Mbps, and the upload speed is 4.99 Mbps. However, it has been observed that the Telkomsel 4G network experiences fluctuating stability, leading to intermittent connectivity issues. This fluctuation was one of the key challenges mentioned in the paper. In contrast, the public IP network used by the Omron CP1L-E PLC offers a more stable and reliable connection, ensuring more consistent data transmission. This highlights the challenge of relying on mobile networks, which, despite their widespread coverage, may not always guarantee stable performance in certain areas.

TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) is a standard developed by the European Telecommunications Standards Institute (ETSI) to establish quality of service (Qos) in IP-based networks[13]. The TIPHON standard is used as a reference for measuring network quality parameters, namely delay, throughput, jitter, and packet loss in IP-based communication systems.

1. Delay

Delay is the time it takes for a data packet to travel from sender to receiver. In this research, the delay used is Round Trip Time (RTT) delay[13]. Because the Modbus TCP work system is request and response, the RTT delay can be used to assess how fast the total response of communication is. The average value of this delay can be found using equation 2.1.

$$\text{Rata} - \text{rata Delay RTT (ms)} = \frac{\text{Total Round Trip Time Delay}}{\text{Total request} - \text{response cycles}} \quad (1)$$

Delay must be minimized to ensure stable communication. The delay categories can be seen in Table 6.

Table 6. TIPHON Delay Index [14]

Category	Delay (ms)	Index
Excelent	< 150	4
Good	150 - 300	3
Poor	>300 - 450	2
Bad	> 450	1

2. Jitter

Jitter is the variation in the delivery time of data packets. If the total number of request and response cycles is N, then Jitter can be calculated using equation 2.2.

$$\text{Jitter (ms)} = \frac{\sum_{n=2}^{N} |\text{Delay RTT}_n - \text{Delay RTT}_{n-1}|}{N-1} \tag{2}$$

Jitter is the amount of delay variation in data communication. Jitter categories are shown in Table 7.

Table 7. TIPHON Jitter Index [14]

Category	Jitter (ms)	Index
Excelent	0	4
Good	>0 - 75	3
Poor	> 75 - 125	2
Bad	>125 - 255	1

3. Packet Loss

Packet loss is the percentage of data packets that are lost or fail to reach their destination during transmission. In the context of PLC communication, packet loss can cause errors in data transmission that could result in system failure.

$$\text{Packet loss (\%)} = \frac{\text{number of packets loss}}{\text{Total Packages sent}} \text{x}100\% \tag{3}$$

High packet loss can lead to decreased communication quality and decreased performance. Packet loss categories are shown in Table 8.

Table 8. TIPHON Packet Loss Index [14]

Category	Packet loss (%)	Index
Excelent	<3%	4
Good	3-15%	3
Poor	>15-25%	2
Bad	>25%	1

4. Throughput

Throughput is the amount of data successfully transmitted from sender to receiver in a unit of time. In this research, a high throughput ensures that the system can transmit a sufficient amount of data without any bottlenecks. Throughput uses units of bits per second (bps) or bytes per second (Bps). The categories of Throughput are described in Table 9.

Table 9. TIPHON Throughput Index [14]

Category	Throughput (kbps)	Index
Excelent	>2100	4
Good	>1200-2100	3
Poor	>338-1200	2
Bad	0-338	1

High throughput indicates stable network performance. Throughput testing can use the formula in equation 2.4.

$$\text{Throughput (bps)} = \frac{\text{Total transferred data}}{\text{Data collection period}} \tag{4}$$

From the above formula, the total data transferred is a measure of the data communicated from both request and response packets.

3. RESULT

The performance analysis of Modbus TCP communication between Mitsubishi FX5U PLC and Omron CP1L-E PLC over the internet is based on the TIPHON standard, which measures four parameters: throughput, delay, jitter, and packet loss. The test results show low throughput, caused by the small packet size of Modbus TCP data. This protocol is designed to transmit a limited amount of data, so the TIPHON standard, which is more suitable for big data applications such as video streaming or VoIP, is not suitable. Despite the low throughput, this is still in accordance with the design of Modbus TCP which prioritizes reliability and speed in small data transactions. The data will be analyzed further.

3.1 Delay

In this test, the measured delay value is Round Trip Time (RTT). This delay is calculated because the Modbus TCP working system is based on the request and response mechanism. RTT measures the total time required from the time the request is sent until the response is received back. Data regarding delay from tests can be seen in Table 10.

Table 10. Delay Test Result

Variations	Observation Time (s)	Average Delay (s)	Bottleneck
10 ms	37213,53666	0,036891584	Yes
25 ms	48190,49942	0,046732402	Yes
50 ms	48871,24026	0,036761036	Yes
70 ms	80026,853998	0,045354945	Yes
75 ms	91001,87931	0,040054844	No
80 ms	90994,72547	0,049632729	No
100 ms	91337,57493	0,061718532	No

From Table 10, it is known that the value of adding delay to the experiment does not linearly affect the average RTT delay. This can be seen in the experiment with 10 ms which is worth 0.036891584 s and 50 ms which is worth 0.036761036. The RTT delay value in these experiments is less than the other experiments. This can occur because the load conditions on the network are different in each test.

3.2 Jitter

Jitter is a measure of the time variation in Round Trip Time (RTT) delay that occurs in different data packets. In other words, jitter shows how consistent the communication time is in each transmission cycle. Data regarding jitter obtained from previous tests can be seen in Table 11.

Table 11. Jitter Test Result

Variations	Observation Time (s)	Average Jitter (s)
10 ms	37213,53666	0,010120984
25 ms	48190,49942	0,069631497
50 ms	48871,24026	0,071144308
70 ms	80026,853998	0,033893682
75 ms	91001,87931	0,068227009
80 ms	90994,72547	0,052160053
100 ms	91337,57493	0,086793105

The data shows that the jitter variation increases as the delay increases. At a delay of 10 ms, the jitter of 0.0101 indicates good communication performance with small fluctuations. As the delay increases to 25 ms and 50 ms, the jitter increases to 0.0696 and 0.0711, indicating slight instability. However, at a delay of 70 ms, the jitter drops to 0.0339, indicating the influence of network load. Jitter rose again at delays of 75 ms and 100 ms, with the highest value of 0.0867. Overall, although the jitter varied, the values remained within acceptable limits.

3.3 Packet Loss

Packet loss is a condition when data packets sent over a network are not received by the receiver. The high number of packet loss indicates that communication is not going well because the communicated data packets are lost in the communication process. The results of packet loss testing can be seen in Table 12.

Table 12. Packet Loss Test Result

Variations	Observation Time (s)	*Packet loss* (%)
10 ms	37213,53666	0.1
25 ms	48190,49942	0.1
50 ms	48871,24026	0
70 ms	80026,853998	0
75 ms	91001,87931	0
80 ms	90994,72547	0
100 ms	91337,57493	0

The packet loss test results show a low percentage. At time lags of 10 ms and 25 ms, with a percentage of 0.1%, indicating the stability of Modbus TCP communication. At time lags of 50 ms to 100 ms, the percentage of packet loss remained 0%.

3.4 Quality of Service (QoS)

After the analysis of all tests is carried out, the next step is to summarize the results of all previous tests for QOS analysis using the Tiphon standard. This is done to provide an overview of the communication performance between the Mitsubishi FX5U PLC and Omron CP1L-E using the Modbus TCP protocol via the internet in several parameters tested. A summary of the overall test results is contained in Table 13.

Table 13. Overall Test Result

Variations	Parameters		
	Delay (ms)	Jitter (ms)	Packet loss (%)
10 ms	36,891584	10,120984	0.1
25 ms	46,732402	69,631497	0.1
50 ms	36,761036	71,144308	0
70 ms	45,354945	33,893682	0
75 ms	40,054844	68,227009	0
80 ms	49,632729	52,160053	0
100 ms	61,718532	86,793105	0
Average	45,306582	55,995805	0
Index	4	3	4

Based on the results in Table 13, the TIPHON Qos index for delay reaches 4, which indicates that the communication system runs with a fast response. Communication system performance for response time is considered optimal for industrial applications that require real-time communication. The average jitter value reaches 56 ms. The system gets a TIPHON Qos index with a value of 3 which indicates good jitter performance, although there is instability in certain variations. With an almost zero packet loss value, the TIPHON Qos index for this parameter gets a value of 4, indicating no data is lost during the communication process. Overall, the TIPHON Qos analysis shows that the inter-PLC communication system with Modbus TCP protocol has excellent performance. With the highest indexes in delay and packet loss. The index for jitter is also within the acceptable range so the system is considered optimal.

4. CONCLUSION

Communication between the Mitsubishi FX5U PLC and the Omron CP1L-E via the Modbus TCP protocol on the internet network worked well, showing fast performance with an average delay of 45 ms, an average jitter of 56 ms, and a packet loss of mostly 0%, making a time delay of 75 ms the optimal choice for speed, reliability, and system integrity.

During the research, the main obstacle encountered was the fluctuating internet network connection, especially when using mobile phone hotspots. This affected the stability of communication between PLCs, compromising the speed and reliability of data exchange. To solve this problem, it is recommended to use a more stable network such as fiber optic or 5G. In addition, although Modbus TCP/IP proved to be optimal, the use of alternative communication protocols such as OPC UA is recommended to test better performance in communication between PLCs, especially under different network conditions.

REFERENCES

[1] J. F. S. R. S. F. S. U. Birgit Vogel-Heuser, “Challenges for Maintenance of PLC-Software and Its Related Hardware for Automated Production Systems: Selected Industrial Case Studies,” 2015. http://dx.doi.org/10.1109/ICSM.2015.7332487

[2] S. Jaloudi, “Communication protocols of an industrial internet of things environment: A comparative study,” *Future Internet*, vol. 11, no. 3, 2019, doi: 10.3390/fi11030066.

[3] Y. Li and L. Yao, “Research on Ethernet Communication and Remote Control of PLC and PC,” 2016. http://dx.doi.org/10.2991/icmemtc-16.2016.156

[4] Frank Petruzella, “Programmable Logic Controllers,” 2017.

[5] Mitsubishi Electric, “MELSEC iQ-F FX5U User’s Manual (Hardware),” 2016. Available: www.mitsubishifa.co.th

[6] Mitsubishi Electric, “MELSEC iQ-F FX5 User’s Manual (Ethernet Communication),” 2016. Available: dl.mitsubishielectric.com

[7] Omron Corporation, *OPERATION MANUAL SYSMAC CP Series*. 2014. Available: www.ia.omron.com

[8] Mitsubishi Electric, “MELSEC iQ-F FX5 User’s Manual (MODBUS Communication),” 2016. Available: dl.mitsubishielectric.com

[9] L. Xuan and L. Yongzhong, “Research and Implementation of Modbus TCP Security Enhancement Protocol,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jun. 2019. doi: 10.1088/1742-6596/1213/5/052058.

[10] S. O. Wilson, A. Chancsig, R. Gamboa, D. Tipn, and S. Elizabeth, “Control and Monitoring of Electrical Variables of a Level Process using Modbus RTU-TCP/IP Industrial Communication,” *Indian J Sci Technol*, vol. 11, no. 32, pp. 1–12, Aug. 2018, doi: 10.17485/ijst/2018/v11i32/131113.

[11] A. B. Pratomo DEVELOPING A FIREWALL SYSTEM ON A COMPUTER NETWORK BASED ON MIKROTIK ROUTEROS,” vol. 1, no. 2, 2023, doi: 10.59688/bufnets.

[12] X. Zou *et al.*, “Pixel-level Bayer-type colour router based on metasurfaces,” *Nat Commun*, vol. 13, no. 1, Dec. 2022, doi: 10.1038/s41467-022-31019-7.

[13] R. Wulandari, “ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON-LIPI),” 2016. https://dx.doi.org/10.28932/jutisi.v2i2.454

[14] I. S. N. Nisa, Rahmat Miyarno Saputro, Tegar Fatwa Nugroho, and Alfirna Rizqi Lahitani, “Analisis Quality of Service (QoS) Menggunakan Standar Parameter Tiphon pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya,” *Teknomatika: Jurnal Informatika dan Komputer*, vol. 17, no. 1, pp. 1–9, Apr. 2024, doi: 10.30989/teknomatika.v17i1.1307.