JURNAL RISET INFORMATIKA **P-ISSN: 2656-1743 |E-ISSN: 2656-1735**
Vol. 8, No. 4. September 2026 DOI: https://doi.org/10.34288/jri.v8i4.553
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

IMPLEMENTATION OF SOFTWARE DEFINED NETWORKING FOR SIMULATION AND ANALYSIS OF DDOS ATTACKS ON SCHOOL NETWORKS

Arif Maulana Yusuf[-1], Muhammad Edi Iswanto[-2], Joko Irawan[-3], Robi Robiyanto[-4], Willy Permana Putra[-5]

Computer Engineering Technology / Department of Informatics Engineering
Indramayu State Polytechnic
arif.my@polindra.ac.id, muhammad.edi@polindra.ac.id, joko_irawan@polindra.ac.id,
robiyanto@polindra.ac.id, willy_p@polindra.ac.id

Abstract

The development of digital services in school environments has increased the importance of network security, particularly in addressing Distributed Denial of Service (DDoS) attacks that can disrupt network service availability. This study aims to develop a school network security simulation based on Software Defined Networking (SDN) and analyze the characteristics of normal traffic and DDoS attack traffic. The research method employed is an experimental approach through network simulation using the Mininet emulator and Ryu Controller. The study began with identifying school network security requirements, followed by designing the SDN network topology, implementing the simulation environment, generating normal traffic, and simulating DDoS attacks using the TCP SYN Flood method. Data collection was conducted using Wireshark, tcpdump, and SDN controller logs to obtain traffic parameters such as throughput, packet loss, delay, jitter, and packet rate. The results showed that normal traffic had an average throughput of 320 Kbps with stable network conditions, while during DDoS attacks the throughput increased significantly to 9.8 Mbps, accompanied by substantial increases in packet loss, delay, and jitter. These findings indicate that DDoS attacks directly affect the quality of school network services. Furthermore, the SDN architecture provides centralized traffic monitoring capabilities, making it a promising approach for developing DDoS detection and mitigation systems in school networks.

Keywords: Software Defined Networking; DDoS; Mininet; Ryu Controller; Network Security

Abstrak

Perkembangan layanan digital pada lingkungan sekolah menyebabkan kebutuhan terhadap keamanan jaringan menjadi semakin penting, terutama dalam menghadapi ancaman serangan Distributed Denial of Service (DDoS) yang dapat mengganggu ketersediaan layanan jaringan. Penelitian ini bertujuan untuk membangun simulasi keamanan jaringan sekolah berbasis Software Defined Networking (SDN) serta menganalisis karakteristik trafik normal dan trafik serangan DDoS. Metode penelitian yang digunakan adalah eksperimen melalui simulasi jaringan menggunakan emulator Mininet dan Ryu Controller. Penelitian diawali dengan identifikasi kebutuhan keamanan jaringan sekolah, dilanjutkan dengan perancangan topologi jaringan SDN, implementasi lingkungan simulasi, pembangkitan trafik normal, serta simulasi serangan DDoS menggunakan metode TCP SYN Flood. Proses pengumpulan data dilakukan menggunakan Wireshark, tcpdump, dan log controller SDN untuk memperoleh parameter trafik seperti throughput, packet loss, delay, jitter, dan jumlah paket per detik. Hasil penelitian menunjukkan bahwa trafik normal memiliki throughput rata-rata sebesar 320 Kbps dengan kondisi jaringan yang stabil, sedangkan saat serangan DDoS terjadi throughput meningkat hingga mencapai 9,8 Mbps disertai peningkatan packet loss, delay, dan jitter secara signifikan. Hasil tersebut menunjukkan bahwa serangan DDoS berdampak langsung terhadap penurunan kualitas layanan jaringan sekolah. Selain itu, arsitektur SDN mampu memberikan kemudahan dalam monitoring trafik jaringan secara terpusat sehingga berpotensi digunakan sebagai dasar pengembangan sistem deteksi dan mitigasi serangan DDoS pada jaringan sekolah.

Kata kunci: Software Defined Networking; DDoS; Mininet; Ryu Controller; Keamanan Jaringan

INTRODUCTION

The development of computer network technology in educational environments continues to increase along with the growing complexity of digital service requirements(Addinillah and Sulianta 2024; Rozan et al. 2024; Yakub et al. 2025). Modern schools currently utilize computer networks to support learning processes, administration, internet access, data storage, and computer-based examination systems. Dependence on such network infrastructure makes network security an important factor that must be considered(Rivaldi and Purnama 2025; Syah et al. 2025). Threats to network security, particularly Distributed Denial of Service (DDoS) attacks, can disrupt network service availability and hinder school operational activities(M.Iqbal, Yuhandri Yunus, and Syafri Arlis 2024; Ridho, Yudhana, and Riadi 2018).

Distributed Denial of Service (DDoS) attacks are one of the most common forms of cyberattacks, carried out by flooding a target system with an excessive volume of traffic, thereby overwhelming network resources and preventing them from serving legitimate user request(Asyidiq and Fathoni 2025; Elvi Ningsih Telaumbanua et al. 2025; Kiswanto et al. 2025). The impact of such attacks may lead to network performance degradation, service access delays, and even complete network disconnection. In educational environments, these conditions can disrupt digital learning activities and hinder access to academic information systems(Mudzhaffar 2025; Pribadi Fitrian, Syah Putra, et al. 2025).

Traditional network approaches have limitations in network security management and monitoring because the control and forwarding functions are still integrated within the same network devices. Software Defined Networking (SDN) has emerged as a solution by separating the control plane from the data plane, enabling network management to become more flexible, centralized, and easier to develop(Fitrian et al. 2025; Pribadi Fitrian, Dwi Nurhikmah, and Taupik Anjana 2025). The SDN architecture also enables network administrators to perform real-time traffic monitoring and implement security mechanisms that are more adaptive to network threats(Lee et al. 2019; Oh, Shin, and Lee 2022).

Several previous studies have shown that the implementation of SDN is capable of improving network management efficiency and supporting the implementation of dynamic network attack detection systems(Harja, Rakhmatsyah, and Nugroho 2019; Hunaifi and Fauzan Akbar 2019; Sdn et al. 2025). In addition, the use of network emulators such as Mininet and SDN controllers such as Ryu or POX enables network simulations to be conducted realistically without requiring a large amount of hardware resources(Junediansyah and Basuki 2022; Nugroho, Basuki, and Akbar 2025). Such simulation environments can be utilized to build school network topologies, generate normal traffic, and simulate DDoS attacks in order to obtain diverse network traffic data.

However, most previous research still focuses on the implementation of Software Defined Networking (SDN) architecture to improve network management efficiency or develop attack detection mechanisms in public network environments (Radito, Trisnawan, and Amron 2020; Yakub et al. 2025). These studies generally use simple network topologies or public datasets, thus not fully representing the characteristics of school networks that have various services, such as academic servers, computer laboratories, learning internet access, and administrative systems. Furthermore, some studies focus more on the development of attack detection algorithms without providing an overview of the process of building a simulated environment that approximates real-world conditions as a source of traffic data.

Therefore, there is still a need for research that builds a comprehensive SDN-based school network simulation environment, starting from identifying network security needs, topology design, generating normal traffic, to simulating DDoS attacks in one integrated experimental scenario (Dwi Putri and Gunanto 2025; Ndun 2025). A representative simulation environment is expected to be able to produce more realistic network traffic variations so that it can be used as a basis for network performance analysis and as a dataset source for further research on DDoS attack detection and mitigation on SDN architecture.

Based on these conditions, this study aims to design and develop a school network security simulation based on Software Defined Networking (SDN) using a network emulator(Alssaheli et al. 2021; Amusan, Alade, and Alabi 2024). The research begins with identifying the security requirements of school networks, followed by the design of an SDN network topology, the generation of normal traffic, and the simulation of DDoS attacks to produce various network traffic conditions. The generated traffic data are expected to serve as a basis for network performance analysis and the

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v8i4.553
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

development of attack detection mechanisms within an SDN environment.

This research is expected to contribute to the development of a more adaptive, centralized, and efficient school network security system in dealing with the threat of cyber attacks, especially DDoS attacks in SDN-based network environments.

RESEARCH METHODS

This research was conducted using an experimental method through Software Defined Networking (SDN)-based network simulation. The goal of this method was to build a simulated school network environment, generate normal traffic, and simulate DDoS attacks to obtain varying network traffic conditions.

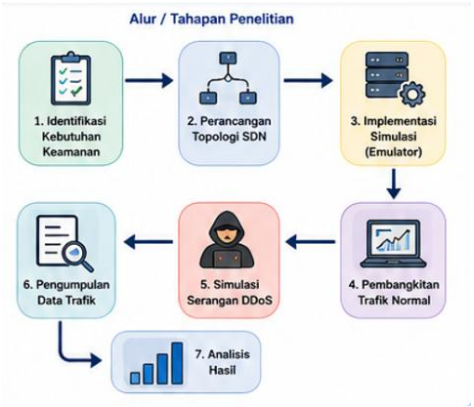

Figure 1. Research stages

Figure 1 above shows the research flow used to build a school network security simulation based on Software Defined Networking (SDN). Each stage is interconnected, from identifying security needs to analyzing the network simulation results(Agus and Sulistyo 2025; Putra and Lestariningati 2018; Sapu and Muis 2025).

1. Identify Security Needs

The first stage is to analyze the network and security needs of the school environment. This stage gathers information about the network services used, such as internet access, computer labs, administration servers, and digital learning systems.

Additionally, network security threats that could disrupt school services are identified, such as Distributed Denial of Service (DDoS) attacks, malware, and unauthorized access. The identification results are used as a basis for determining the network design and security mechanisms to be implemented.

2. SDN Topology Design

The next step is to design an SDN-based network topology. The topology is designed using the concept of separating the control plane and the data plane so that network management can be centralized by the SDN controller.

The design was performed using the Mininet network emulator with several virtual devices such as OpenFlow switches, user hosts, and school servers. Network segmentation was created to reflect the actual conditions of the school network.

3. Simulation Implementation

Once the topology is designed, the next step is to implement the simulation environment using a network emulator. The emulator used is Mininet with a Ryu Controller-based SDN controller.

In this phase, all virtual devices are configured, including switches, hosts, IP addresses, and connections between devices. This simulated environment is used to test both normal network traffic and DDoS attack traffic.

4. Generation of Normal Traffic

The normal traffic generation phase is conducted to simulate the daily activities of school network users. Normal traffic is generated through several network communication activities, such as:

- Pinging between hosts
- Accessing the school website
- File transfers
- Simple data streaming

The aim of this stage is to obtain the characteristics of normal network traffic as comparative data against traffic during an attack.

5. DDoS Attack Simulation

The next step is to simulate a Distributed Denial of Service (DDoS) attack. The simulation involves sending a large number of network packets from multiple attacker hosts to the target server.

The attack method used is TCP SYN Flood using tools such as hping3. This stage aims to create a network traffic flooding condition so that its impact on the school's network performance can be observed.

6. Traffic Data Collection

During the simulation, all network traffic activity is collected for analysis. Data collection is performed using network monitoring tools such as Wireshark, tcpdump, and logs from the SDN controller.

7. Analysis of Results

The final step is to analyze the obtained network traffic data. The analysis is performed by comparing the characteristics of normal traffic and DDoS attack traffic based on network performance parameters.

RESULTS AND DISCUSSION

This section presents the research results based on the stages that have been carried out, namely identifying school network security needs, designing a Software-Defined Networking (SDN)-based network topology, generating normal traffic, and simulating a Distributed Denial of Service (DDoS) attack. The research results are then analyzed to determine the characteristics of network traffic a

1. Identify School Network Security Needs

Identification is carried out through analysis of the main network services used in school activities, such as internet access for learning, e-learning systems, administration services, and school data storage servers.

The analysis results indicate that the school network faces several potential security threats, particularly DDoS attacks, which can slow down or even render network services inaccessible. Furthermore, other threats such as malware, brute force attacks, and sniffing can also impact the stability of the school network. The results of the identification of security needs and threats are shown in Table 1.

Table 1. School Network Security Service Needs and Threats

No	Network Services	Security Threats	Impact
1	Learning internet access	DDoS, Brute Force	Internet access disruption
2	E-learning system	DDoS, SQL Injection	The system cannot be accessed
3	Administration Server	DDoS, Malware	Administration service disruption
4	School file sharing	Sniffing, DDoS	Data leaks
5	School database server	DDoS, Data Leakage	Loss of critical data

Based on these identification results, a network architecture capable of centralized traffic management and monitoring is needed, allowing network administrators to detect traffic anomalies more quickly. Therefore, the Software-Defined Networking (SDN) approach was chosen because it separates the control plane and data plane, making network management more flexible and adaptive to network security threats.

2. SDN Network Topology Design

This study used a single Ryu Controller-based SDN controller to serve as the network's central control center. The controller is connected to several Open vSwitches, which act as virtual switches to regulate traffic flow between hosts.

The network topology consists of five OpenFlow switches and several user hosts divided into several network subnets. Network segmentation was implemented to create a more realistic simulation of the school environment and support the process of monitoring network traffic between segments according to the school's needs, as shown in Figure 2.

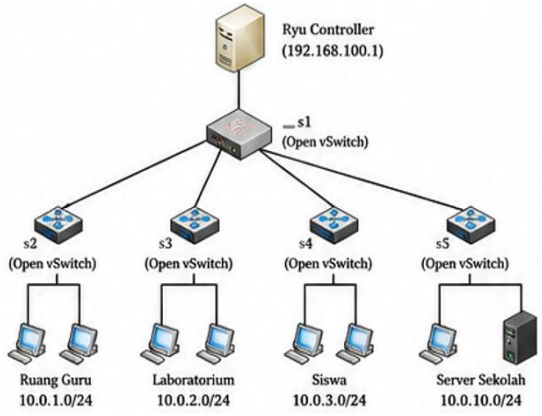

Figure 2. Network Topology of SDN School

Table 2. Device Configuration in Topology

Device	Amount	Function
Ryu Controller	1	SDN Controller as network controller
Open vSwitch	5	Virtual switch connected to Controller
User Host	12	User simulation in each segment (Teacher, Lab, Student)
School Server	1	Service server (Web/Database/Save File)

3. Generation of Normal Traffic

After the network topology was successfully established, normal traffic was generated to simulate the daily activities of school network users. Normal traffic was generated using several types of network communication, such as ICMP pings, TCP file transfers, and HTTP service access.

Traffic generation is performed between hosts within the network to create network conditions that mimic real-world school user activity, such as accessing learning websites, sending data, and communicating between devices. Normal traffic generation parameters are shown in Table 3.

Table 3. Normal Traffic Parameters

Traffic Type	Protokol	Source → Destination	Average traffic speed
Web Access	HTTP(TCP)	Host → Web server	150-300 Kbps
Transfer File	FTP (TCP)	Host → Server File	200-400 Kbps
Ping	ICMP	Host → Host	10-50 Kbps

Observations show that normal traffic has a relatively stable throughput pattern with low packet loss and delay rates. This indicates that the designed SDN network is capable of handling normal network communications well. The resulting normal traffic rate over 300 seconds is shown in Figure 3.

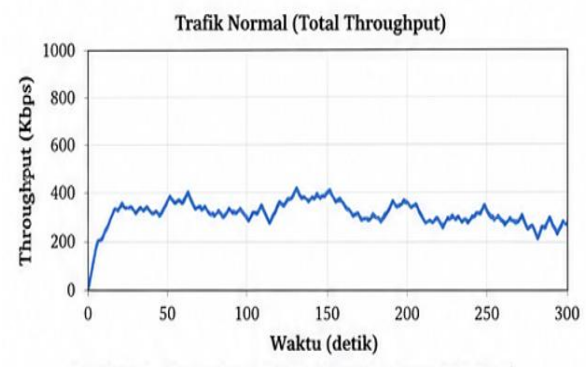

Figure 3. Normal Traffic Throughput for 300 Seconds

Figure 3 shows that normal traffic is relatively stable with an average throughput of around 320 Kbps and without significant traffic spikes.

4. DDoS Attack Simulation

A DDoS attack simulation on a built SDN network was conducted by generating a large amount of continuous traffic to the target server using the TCP SYN Flood protocol.

The attack was conducted from multiple attacker hosts to the school server to create a network traffic flood. The simulation process aimed to determine changes in network traffic characteristics during a DDoS attack. The attack parameters are shown in Table 4.

Table 4. DDoS attack simulation parameters

Parameter	Value	Description
Number of Attackers	5 Host	H1, h2, h3, h4, h5 (Student segment)
Target	Web Server (10.0.10.2)	School's primary service
Protokol	TCP SYN	SYN Flood
Attack Duration	300 seconds	Simulation time
Packet Rate	1000 packets/second/host	Total ~5000 packets/second

Simulation results show a significant increase in network throughput during the attack. Furthermore, delay, jitter, and packet loss values increased compared to normal traffic conditions. These conditions indicate that DDoS attacks can impact school network performance and cause a decrease in network service quality. The results of the increased traffic during a DDoS attack can be seen in Figure 4.

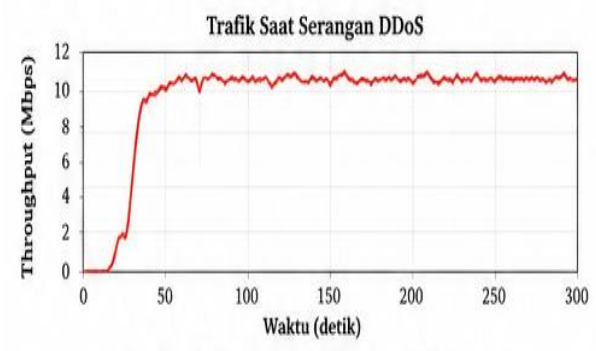

Figure 4. Throughput during a DDoS Attack

It can be seen that when the attack began (around the 30th second), throughput spiked drastically, reaching an average of 9.8 Mbps. This indicates a flood of traffic to the server.

5. Comparison of Normal Traffic and DDoS Traffic

A comparison between normal traffic and DDoS attack traffic was conducted to determine changes in network performance during the simulation. The parameters compared included throughput, packet count, packet loss, delay, and jitter.

The analysis shows that DDoS traffic contains a significantly larger number of packets than normal traffic. Furthermore, packet loss increases significantly due to the influx of traffic to the target server. Delay and jitter also increase, degrading network communication quality.

Table 5. Comparison of Normal Traffic and DDoS Traffic

Metrics	Normal Traffic	DDoS Traffic	Increase (%)
Througput	320 Kbps	9,8 Mbps	2962%
Number of packets per second	350 pkt/s	5200 pkt/s	1386 %
Packet Loss	1,2 %	28,6 %	-
Average Delay	12 ms	145 ms	1108 %
Average Jitter	3 ms	38 ms	1167 %

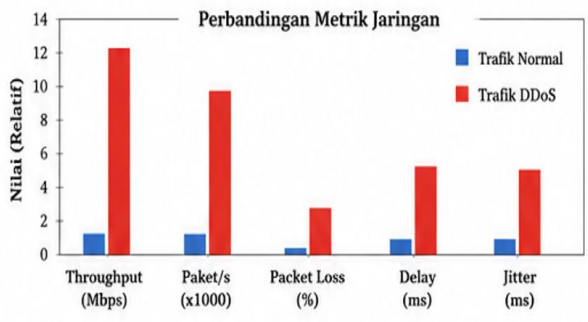

Figure 5. Comparison of Normal and DDoS Traffic Metrics

Based on Table 5 and Figure 5, DDoS attacks cause a significant increase in traffic, high packet loss, and increased delay and jitter. This impacts the quality of school network services. The results will form the basis for developing attack detection and mitigation mechanisms in SDN-based network environments.

The SDN architecture simplifies network traffic monitoring because all traffic flows can be centrally monitored through the SDN controller. Thus, SDN has the potential to support the development of DDoS attack detection and mitigation systems in school networks.

CONCLUSIONS AND SUGGESTIONS

Conclusion

The implementation of a Software Defined Networking (SDN)-based network using a network emulator was successfully built and was able to realistically represent the school network conditions. The research began with the identification of school network security needs which showed that Distributed Denial of Service (DDoS) attacks were one of the main threats to the availability of school network services. The SDN network topology was successfully designed using Mininet and Ryu Controller with network segmentation representing the school environment, including the teacher's room, computer laboratory, student room, and school server. The developed simulation environment was able to run normal network communications and support the centralized traffic monitoring process through the SDN controller.

The results of generating normal traffic indicate that the network has stable performance with consistent throughput values and low delay and packet loss. In contrast, the DDoS attack simulation using the TCP SYN Flood method produces a significant traffic spike, causing an increase in delay, jitter, and packet loss, which impacts the quality of network service. These results indicate that the simulation environment is able to clearly depict the differences in characteristics between normal network conditions and conditions during an attack.

The development of a comprehensive SDN-based school network simulation environment, starting from identifying security needs, designing a topology that represents the school infrastructure, generating normal traffic, to simulating DDoS attacks in one integrated experimental scenario. Unlike previous research that generally focused on SDN implementation or developing attack detection algorithms, this research produces a simulation environment that is able to provide network traffic data that is more representative of school operational conditions. This environment can be used as a medium for evaluating network performance as well as a source of datasets for developing detection and mitigation methods for attacks based on machine learning and Intrusion Detection Systems (IDS).

Thus, this research contributes to the provision of an adaptive, centralized, and realistic

simulation platform to support the research and development of SDN-based school network security systems. In the future, this simulation environment can be expanded by implementing various types of cyberattacks, integrating automated mitigation mechanisms, and utilizing artificial intelligence algorithms to enhance real-time attack detection capabilities.

Suggestion

Based on the results of the research that has been conducted, there are several suggestions that can be developed in further research, including:

1. Develop an automatic DDoS attack detection system using machine learning or deep learning methods on the SDN controller.
2. Adding variations in network attack types such as UDP Flood, ICMP Flood, HTTP Flood, and botnet attacks to make the simulation results more complex.
3. Implement automatic mitigation mechanisms on the SDN controller to block suspicious traffic in real-time.
4. Perform network performance testing using more Quality of Service (QoS) parameters, such as latency, availability, and bandwidth utilization.

REFERENCES

Addinillah, Naila Aura, and Feri Sulianta. 2024. "ANALISIS MANAJEMEN RISIKO MENGGUNAKAN METODE NIST 800-30 PADA LAB KOMPUTER SEKOLAH (Studi Kasus : SMP Negeri 1 Ciniru)." *Jurnal Teknologi Dan Informasi* 14(1).

Agus, Yulius Manahil Hendrawan, and Wiwin Sulistyo. 2025. "Simulasi Traffic Dan Performa Jaringan SDN Menggunakan ONOS Controller Dan Standar TIPHON." *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi* 4(2). doi: 10.24246/itexplore.v4i2.2025.pp196-210.

Alssaheli, Omran M. A., Z. Zainal Abidin, N. A. Zakaria, and Z. Abal Abas. 2021. "Implementation of Network Traffic Monitoring Using Software Defined Networking Ryu Controller." *WSEAS Transactions on Systems and Control* 16. doi: 10.37394/23203.2021.16.23.

Amusan, Elizabeth A., Oluwaseun M. Alade, and John J. Alabi. 2024. "Secure Network Monitoring Using Software Defined Networking (SDN) with Ryu Controller." *FUOYE Journal of Engineering and Technology* 9(2). doi: 10.4314/fuoyejet.v9i2.12.

Asyidiq, Mursalat, and Azhar Fathoni. 2025. "Analisis Efektivitas LLM Dalam Deteksi Serangan DDoS Pada Jaringan Komputer." *Prosiding Seminar Kecerdasan Artifisial, Sains Data, Dan Pendidikan Masa Depan* 3(1).

Dwi Putri, Pelita, and Sigit Gunanto. 2025. "Perancangan Dan Implementasi Infrastruktur Jaringan Hotspot Berbasis Koneksi Point To Point Protocol Over Ethernet (PPPoE) Dan Implementasi Web Proxy Dengan Mikrotik Di Kantor Desa Abung Jayo." *Sienna* 5(2). doi: 10.47637/sienna.v5i2.1394.

Elvi Ningsih Telaumbanua, Darwis Setiawan Waruwu, Kevin Rewardi Harefa, Christine Jenny Puspita Zega, Ivataro Laoli, and Ofelius Laia. 2025. "Simulasi Analisis Serangan DDoS Pada Beberapa Alamat Website Untuk Evaluasi Ketahanan Sistem." *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)* 4(1). doi: 10.62712/juktisi.v4i1.405.

Fitrian, Harry Pribadi, Adkia Adkia, Sindi Rahmadani, Raisya Puspa Kencana, and Ihsan Tafaquh Fiddin. 2025. "Analisis Peningkatan Kinerja Jaringan Melalui Reduksi Delay, Jitter, Dan Peningkatan Throughput Pada Infrastruktur Software-Defined Networking Di Digitech University." *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)* 8(1). doi: 10.32672/jnkti.v8i1.8627.

Harja, Danaswara Prawira, Andrian Rakhmatsyah, and Muhammad Arief Nugroho. 2019. "Implementasi Untuk Meningkatkan Keamanan Jaringan Menggunakan Deep Packet Inspection Pada Software Defined Networks." *Indonesian Journal on Computing (Indo-JC)* 4(1):133. doi: 10.21108/indojc.2019.4.1.286.

Hunaifi, Nanang, and Rovi Fauzan Akbar. 2019. "Analisis Kinerja Jaringan Berbasiskan Software Definition Network Dengan Protokol Openflow Di Rri Bandung." *Infotronik : Jurnal Teknologi Informasi Dan Elektronika* 4(1):24. doi: 10.32897/infotronik.2019.4.1.172.

Junediansyah, Ariefanda, and Achmad Basuki. 2022. "Penerapan Algoritme Prim Dan Floyd-Warshall Sebagai Algoritme Routing Pada Arsitektur Software Defined Network." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* 6(6).

Kiswanto, Dedy, Fanny Ramadhani, Nurul Maulida Surbakti, and Nadrah Afiati Nasution. 2025. "Pengembangan Dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest." *Bulletin of Information Technology (BIT)* 6(3).

Lee, Kilho, Minsu Kim, Taejune Park, Hoon Sung Chwa, Jinkyu Lee, Seungwon Shin, and Insik Shin. 2019. "MC-SDN: Supporting Mixed-Criticality Real-Time Communication Using Software-Defined Networking." *IEEE Internet of Things Journal* 6(4). doi: 10.1109/JIOT.2019.2915921.

M.Iqbal, M. Iqba., Yuhandri Yunus, and Syafri Arlis. 2024. "Audit Keamanan Jaringan Komputer Server Dari Serangan DDoS Menggunakan Snort Intrusion Detection System." *The Indonesian Journal of Computer Science* 13(5). doi: 10.33022/ijcs.v13i5.4391.

Mudzhaffar, M. F. 2025. "… Kualitas Jaringan Hotspot Menggunakan Metode Quality of Service (QoS) Dalam Mendukung Kegiatan Belajar Mengajar Di Sekolah Menengah Kejuruan Negeri 1 …." *Jurnal Dinamika Informatika*.

Ndun, Yosef Junior. 2025. "PENERAPAN VLAN (VIRTUAL LOCAL AREA NETWORK) UNTUKMENINGKATKAN KEAMANAN DAN EFISIENSI JARINGAN APLIKASI DAPODIK DI SDN OESUSU KABUPATEN KUPANG." *Jurnal Informatika Dan Teknik Elektro Terapan* 13(3). doi: 10.23960/jitet.v13i3.6851.

Nugroho, Farras Athallah, Achmad Basuki, and Sabriansyah Rizqika Akbar. 2025. "Pengembangan Backend Laboratorium Virtual Dengan IPMininet Untuk Pembelajaran Routing Jaringan Komputer." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* 9(9).

Oh, Sangeun, Insik Shin, and Kilho Lee. 2022. "RT-SDN: Adaptive Routing and Priority Ordering for Software-Defined Real-Time Networking." *IEEE Systems Journal* 16(2). doi: 10.1109/JSYST.2021.3120539.

Pribadi Fitrian, Harry, Anisa Dwi Nurhikmah, and Muhamad Taupik Anjana. 2025. "DESAIN DAN IMPLEMENTASI JARINGAN SOFTWARE-DEFINED NETWORKING (SDN) UNTUK JARINGAN KAMPUS YANG EFISIEN." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9(2). doi: 10.36040/jati.v9i2.12995.

Pribadi Fitrian, Harry, Fernanda Syah Putra, Amelia Nazelina Kusmana, Neng Tisha Nur Anggraeni Sapitri, and Sinta Nurhaliza. 2025. "TINJAUAN LITERASI MENGENAI TEKNOLOGI 5G: IMPLIKASI TERHADAP PERFORMA DAN KEAMANAN JARINGAN KOMPUTER DI SEKOLAH MENENGAH PERTAMA DAN SEKOLAH MENENGAH AKHIR." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9(2). doi: 10.36040/jati.v9i2.12873.

Putra, Himawan Eka, and Susmini Indriani Lestariningati. 2018. "Penerapan Arsitektur Software-Defined Networking Berbasis Openflow Pada Simulasi Jaringan Virtual." *Jurnal Teknik Komputer Unikom – Komputika* 7(1).

Radito, Raihan, Primantara Hari Trisnawan, and Kasyful Amron. 2020. "Implementasi Pencarian Jalur Berdasarkan Bandwidth Dengan Menggunakan Algoritme Dijkstra Pada Arsitektur Jaringan Software- Defined Networking (SDN)." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya* 4(5).

Ridho, Faizin, Anton Yudhana, and Imam Riadi. 2018. "Analisis Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS)." *Annual Research Seminar 2016* (December 2016).

Rivaldi, Kamaludin, and Giri Purnama. 2025. "Perancangan Dan Penerapan Monitoring Infrastruktur Perangkat Jaringan Komputer Pada Pusat Data Dan Sarana Informatika Melalui Pengaplikasian Zabbix Network Engineering." *ADIJAYA Jurnal Multidisiplin* 3(3).

Rozan, Muhammad Afrian, Muhlis Tahir, Ayu Putri Qirani, Nabila Rizqiullah, Mareta Veranda, Renny Puji, and Abd Ghaffar. 2024. "IMPLEMENTASI WEB PROXY PADA MIKROTIK UNTUK MENGOPTIMALKAN KEAMANAN JARINGAN WIRELESS LAN DI LINGKUNGAN SEKOLAH MAN 1 GRESIK." *Jurnal Pendidikan Teknologi Informasi (JUKANTI)* 7(1). doi: 10.37792/jukanti.v7i1.1280.

Sapu, Asnawati, and Ichwan Muis. 2025. *Penerapan Teknologi Software Defined Networking Untuk Mendukung Failover, Redundansi Dan Manajemen Jaringan Terintegrasi Dalam Infrastruktur Topologi Star Di SMK Tira Rantetayo*.

Sdn, Networking, Untuk Jaringan, Kampus Yang, Harry Pribadi Fitrian, Anisa Dwi Nurhikmah, and Muhamad Taupik Anjana. 2025. "Desain Dan Implementasi Jaringan Software-Defined." 9(2):2268–73.

Syah, Efrizal, Hermawan Weharima, Tarsius Susilo, Tedy Basuki, and Andy Mustafa Akad. 2025.

"Serangan Siber Terhadap Infrastruktur Kritis." *JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial Dan Pendidikan* 6(2). doi: 10.54543/syntaximperatif.v6i2.678.

Yakub, Riki, Muhlis Tahir, Esti Paramita Dewi, Bidari Husnul Khotimah, Adelia Noer Afidha, and Muhammad Yafi' Bahytsany. 2025. "IMPLEMENTASI KEAMANAN JARINGAN WIRELESS MENGGUNAKAN WEB PROXY PADA MIKROTIK DI SMP NEGERI 1 LABANG." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9(4). doi: 10.36040/jati.v9i4.14127.