Nusantara 1

Artikel Galleys Teknologi-Vol2.4-1914.pdf

Library - No Repository 38

Library B

Unidades Tecnológicas de Santander_DIE

Document Details

Submission ID
trn:oid:::1:3397043435

Submission Date
Nov 3, 2025, 9:58 AM GMT-5

Download Date
Nov 3, 2025, 9:59 AM GMT-5

File Name
Artikel_Galleys_Teknologi-Vol2.4-1914.pdf

File Size
328.9 KB

14 Pages

5,486 Words

33,872 Characters

19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

53 Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

11 Missing Quotations 2%
Matches that are still very similar to source material

13 Missing Citation 5%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

16% Internet sources
13% Publications
10% Submitted works (Student Papers)

Match Groups

- **53** Not Cited or Quoted 12%
  Matches with neither in-text citation nor quotation marks
- **11** Missing Quotations 2%
  Matches that are still very similar to source material
- **13** Missing Citation 5%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

16% Internet sources
13% Publications
10% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
www.journal.lembagakita.org		1%
2	Student papers	
Chester College of Higher Education		<1%
3	Student papers	
Wilmington University		<1%
4	Internet	
internationalpubls.com		<1%
5	Student papers	
Jose Rizal University		<1%
6	Internet	
ijritcc.org		<1%
7	Internet	
en.wikipedia.org		<1%
8	Student papers	
University of the Sunshine Coast		<1%
9	Student papers	
College of Natural Resources, RUB		<1%
10	Student papers	
Northcentral		<1%

11	Internet	
jurnal.umj.ac.id		<1%
12	Internet	
inass.org		<1%
13	Internet	
www.ijsce.org		<1%
14	Internet	
dergipark.org.tr		<1%
15	Student papers	
Central Queensland University		<1%
16	Publication	
Hailong Zhang, Enguo Zhu, Yi Ren, Ran Li, Guoquan Zheng, Shuai Hou. "The Opti...		<1%
17	Internet	
ejournal.bsi.ac.id		<1%
18	Internet	
jurnal.stmikroyal.ac.id		<1%
19	Internet	
pjlss.edu.pk		<1%
20	Internet	
www.ejournal.unma.ac.id		<1%
21	Publication	
"Proceedings of the 4th International Conference on Advances in Communication...		<1%
22	Internet	
journal.kawanad.com		<1%
23	Internet	
www.ijdcn.latticescipub.com		<1%
24	Internet	
link.springer.com		<1%

25 Internet
pmc.ncbi.nlm.nih.gov <1%

26 Internet
networkustad.com <1%

27 Internet
www.ixiacom.com <1%

28 Internet
www.gsconlinepress.com <1%

29 Student papers
University of Wales Institute, Cardiff <1%

30 Internet
accretivetechnologygroup.com <1%

31 Internet
repo.undiksha.ac.id <1%

32 Internet
repository.telkomuniversity.ac.id <1%

33 Student papers
Midlands State University <1%

34 Internet
lfac.cu.edu.tr <1%

35 Internet
threatcare.com <1%

36 Student papers
Middlesex University <1%

37 Publication
Sushil Kumar Singh, Rajendrasinh B. Jadeja, Ashish Khanna, Pushan Kumar Dutta,... <1%

38 Publication
Julvan Marzuki Putra Sibarani, Yuma Akbar, Sutisna, Kiki Setiawan. "Implementa... <1%

39 Internet
www.grafiati.com <1%

40 Internet
www.ijcsn.org <1%

41 Publication
"AI-Driven Transportation Systems: Real-Time Applications and Related Technolo... <1%

42 Publication
Ahmad Alalewi, Iyad Dayoub, Soumaya Cherkaoui. "On 5G-V2X Use Cases and Ena... <1%

43 Student papers
Ravensbourne <1%

44 Internet
abcxperts.com <1%

45 Internet
er.chdtu.edu.ua <1%

46 Internet
lembagakita.org <1%

47 Internet
pubs.ascee.org <1%

48 Internet
www.journals.latticescipub.com <1%

49 Internet
www.researchgate.net <1%

50 Publication
Norliza Katuk, Noradila Nordin, Adib Habbal. "From Smart Cities to the Metaverse... <1%

51 Publication
Yuzhen Wang, Guoxiao Zong, Qiang Wei. "Research on the Application of Decepti... <1%

52 Publication
Doug Cairns, Roberta Amendola, Dilpreet Bajwa, Cecily Ryan, Chris Ridgard, Jared... <1%

Technologia Journal: Jurnal Informatika
E-ISSN:3046-9163
Vol.2.No.4, November 2025
DOI : https://doi.org/10.62872/xe3zrt53

Implementation of Software Defined Networking (SDN) Technology in the Campus Network of Ichsan Sidenreng Rappang University

Baharuddin
Universitas Ichsan Sidenreng Rappang
e-mail:* baharanthyqu@gmail.com

Inputed : October 15, 2025 *Revised : October 29, 2025*
Accepted : October 20, 2025 *Published : November 03, 2025*

ABSTRACT

The development of information technology and the digitalization of higher education demand a more efficient, flexible, and secure network infrastructure. Software Defined Networking (SDN) offers a new paradigm in network management by separating the control plane and data plane, enabling more centralized and adaptive network management. This study aims to analyze the implementation of SDN in campus networks, specifically at Ichsan Sidenreng Rappang University, and identify its benefits, challenges, and implementation strategies. The method used is a systematic literature review of 15 scientific publications from 2020-2025 that discuss the implementation of SDN in the context of campus networks. The results show that SDN provides significant network performance improvements, with a decrease in latency from 37.7 ms to 18 ms, jitter from 40.3 ms to 2.7 ms, and an increase in throughput from 95 Mbps to 98.2 Mbps compared to conventional networks. SDN also increases flexibility through centralized management and automation, strengthens security with adaptive firewall integration, and improves service redundancy and availability. Key implementation challenges include the need for human resource training, the development of comprehensive security policies, and testing on more complex topologies. This study concludes that implementing SDN on campus networks is strategic for supporting the digitalization of higher education, with recommendations for thorough planning, ongoing human resource training, and the development of policies that holistically integrate technical and security aspects.

Keywords: *Software Defined Networking, Campus Network, Network Management, Network Security, QoS*.

INTRODUCTION

The digital transformation in higher education has transformed the way academic institutions manage and provide services to their academic communities. Modern universities now rely heavily on reliable information and communication technology infrastructure to support a wide range of activities, from online learning and academic information systems to digital libraries and collaborative research. The need for stable, fast, and secure connectivity is a fundamental prerequisite for higher education institutions to compete and provide quality services in the digital age.

However, conventional network architectures still widely used by educational institutions face various limitations in meeting these demands. Traditional networks tend to be static, with configurations scattered across multiple devices, making them difficult to manage efficiently, especially as the network grows more complex. Troubleshooting is time-consuming because administrators must access each device individually. Scalability is limited because adding or changing devices requires complex and error-prone manual configuration. Implementing security policies is also challenging, as they must be applied separately to each network device.

Software-Defined Networking (SDN) presents an innovative solution to overcome the limitations of conventional network architecture. SDN separates the control plane, which regulates decision-making logic, from the data plane, which handles packet forwarding. This separation allows for centralized network management through a controller that can dynamically program the behavior of all network devices. With this paradigm, administrators can set network policies, allocate bandwidth, and implement security from a single point of control, without the need to configure each device individually.

Implementing SDN in campus networks offers various strategic advantages. From a performance perspective, SDN has been shown to significantly reduce latency and jitter, which is crucial for real-time applications such as video conferencing and online learning (Fitrian et al., 2025; Gonzales & Pitogo, 2024). From a management perspective, SDN enables configuration automation, accelerating the deployment of new services and reducing human error (Chen et al., 2024; Mensah et al., 2024). From a security perspective, SDN facilitates the centralized implementation of firewalls and security systems with rules that can be dynamically adjusted based on real-time network conditions (Hariyadi et al., 2025; Saputra & Dalimunthe, 2021).

Ichsan Sidenreng Rappang University, as a growing higher education institution, faces the challenge of providing a network infrastructure capable of supporting the increasing demands of digitalization. The growing number of users, the diversification of digital services, and the demand for stable and secure connectivity require more modern and efficient network solutions. Implementing SDN is a strategic choice to transform the campus network infrastructure to be more responsive, adaptive, and able to accommodate future developments.

Although the benefits of SDN have been widely studied in various contexts, there is still a gap in the literature regarding the practical implementation of SDN in higher education institutions in Indonesia, especially mid-sized universities such as Ichsan Sidenreng Rappang University. This study attempts to fill this gap by comprehensively analyzing the implementation of SDN in the context of campus networks, identifying the benefits that can be obtained, challenges that need to be anticipated, and effective implementation strategies. The research questions that are the focus of this study are how SDN can improve campus network performance, what are

the advantages of SDN compared to conventional architectures in the context of higher education, what challenges are faced in implementing SDN, and what is the right implementation strategy to maximize the benefits of this technology.

METHODOLOGY

This study uses a systematic literature review approach to analyze the implementation of Software Defined Networking in campus networks. This method was chosen because of its ability to integrate findings from various studies, both theoretical and practical, to provide a comprehensive understanding of SDN technology in the context of higher education.

The data collection process was carried out through the identification and selection of scientific publications relevant to the research topic. The inclusion criteria included publications within the 2020 to 2025 timeframe to ensure the freshness of the information and relevance to the latest SDN technology developments. Selected articles must discuss the implementation of SDN in the context of campus networks or educational institutions, covering technical aspects such as network performance, management, security, and scalability. The study focuses on comparing SDN with conventional networks, routing protocols, SDN controllers, integration with security systems, and Quality of Service (QoS) implementation. A total of 15 scientific articles that met these criteria were used as primary data sources in this study.

Data analysis was conducted using a thematic approach that identified key categories related to SDN implementation. First, information was extracted from each article related to network performance metrics such as latency, jitter, and throughput, as well as aspects of management, security, and scalability. Second, the findings were grouped based on similar themes to form analysis categories covering network performance improvement, flexibility and automation, security and redundancy, and implementation challenges. Third, a cross-literature synthesis was conducted to identify consistent patterns, best practices, and implementation recommendations applicable to the context of Ichsan Sidenreng Rappang University.

To ensure the validity of the analysis, source triangulation techniques were used by comparing findings from various case studies of SDN implementations at different universities. The analysis also considered the implementation context, such as network scale, controller type, and network topology, to understand factors influencing implementation success. Data categorization and interpretation were conducted iteratively to ensure the consistency and accuracy of the analysis.

Limitations of this method include the focus on literature available in a specific database and possible differences in implementation context between the reviewed studies and the specific conditions of Ichsan Sidenreng Rappang University. However, by using 15 diverse sources from various geographical contexts and implementation scales, this study attempts to provide a representative picture of SDN implementation in campus networks that can

serve as a reference for planning and implementation at Ichsan Sidenreng Rappang University.

RESULTS AND DISCUSSION

The current network infrastructure at Ichsan Sidenreng Rappang University is still dominated by a conventional network architecture that relies on manual configuration of each device, such as routers, switches, and access points. This model presents a number of limitations in terms of scalability, management efficiency, and security. Based on internal observations and interviews with the campus information technology team, it was discovered that the annual increase in network users primarily due to the expansion of e-learning services, web-based academic information systems, and the digitization of administration has resulted in significant traffic loads during peak hours. This often leads to problems such as decreased access speeds, delays when using online learning applications, and difficulties in the troubleshooting process because device configurations are handled separately.

Furthermore, the static nature of network security management mechanisms makes updating firewall and access control policies time-consuming and prone to configuration errors. This situation indicates that UNISRI's network system lacks sufficient flexibility and automation to meet the dynamic demands of higher education digitalization. Therefore, implementing Software-Defined Networking (SDN) is a strategic solution for transforming the campus network into a more centralized, adaptive, and manageable one. With centralized controller-based management, SDN has the potential to reduce configuration time, improve connection stability, and strengthen security through real-time monitoring mechanisms and automated policy enforcement across all campus network devices.

Network Performance Improvement through SDN Implementation

The implementation of Software Defined Networking has been shown to provide significant network performance improvements across a variety of key metrics. One of the key advantages of SDN is its ability to dramatically reduce latency, or delay. Research shows that SDN can reduce latency from an average of 37.7 ms on conventional networks to just 18 ms, a nearly 52% reduction (Fitrian et al., 2025; Gonzales & Pitogo, 2024; Mahdiyah et al., 2021). This latency reduction is crucial for online learning applications that require real-time interaction, such as video conferencing, webinars, and virtual classrooms. Lower latency results in a more responsive user experience and reduces communication disruptions that often occur on high-delay networks.

In addition to latency, SDN also significantly reduces jitter. Jitter, which measures the variation in delay between data packets, can be reduced from 40.3 ms on conventional networks to just 2.7 ms on SDN networks (Fitrian et al., 2025; Gonzales & Pitogo, 2024; Mahdiyah et al., 2021). This jitter reduction of up to 93% provides a much more stable and consistent connection, which is crucial for video and audio streaming applications in online learning. High connection

stability ensures that learning materials can be delivered without buffering or dropouts that can disrupt the learning process.

Increased throughput is also a tangible benefit of SDN implementation. Throughput, which measures the amount of data successfully transmitted per unit of time, increased from an average of 95 Mbps on conventional networks to 98.2 Mbps on SDN (Fitrian et al., 2025; Gonzales & Pitogo, 2024; Mahdiyah et al., 2021). Although the increase is around 3.4%, the consistency and stability of throughput on SDN are significantly improved, which is crucial for supporting large data transfers such as downloading course materials, uploading student assignments, and accessing digital libraries. This improvement also supports the use of Learning Management Systems (LMS), which require stable bandwidth for optimal operation.

This superior performance is also confirmed by comparative studies between various SDN controllers. Research shows that RYU and POX controllers in an SDN architecture with OSPF routing provide superior performance compared to conventional networks in terms of response time and packet forwarding efficiency (Shodiq & Prihanto, 2021). The implementation of the Border Gateway Protocol (BGP) routing protocol in SDN also shows better performance in terms of convergence time and routing stability compared to implementations in traditional networks (Mahdiyah et al., 2021; Yaqin, 2020).

SDN also facilitates more effective bandwidth management through the implementation of Quality of Service (QoS). With QoS, administrators can prioritize network traffic based on application type, ensuring that critical services such as academic information systems, e-learning, and video conferencing receive adequate bandwidth allocation even during network congestion (Fitrian et al., 2025). This capability is particularly important in a campus context where multiple applications with varying bandwidth requirements run concurrently. With better bandwidth management, institutions can maximize the utilization of existing infrastructure while ensuring consistent quality of service for priority applications.

Analysis of SDN network performance using the Random Early Detection (RED) algorithm also shows that SDN can manage network congestion more effectively, reducing packet loss and increasing bandwidth utilization (Manuputty & Widiasari, 2024). This algorithm helps maintain optimal network performance even when the load increases, which often occurs during peak hours in campus environments. SDN's ability to dynamically adapt to network conditions ensures that service quality is maintained across a variety of usage scenarios.

SDN Flexibility, Automation, and Scalability

One of the fundamental advantages of SDN is the separation of the control plane and the data plane, enabling centralized network management (Sarmiento et al., 2021). This architecture transforms the way administrators manage network infrastructure from a device-by-device approach to a network-wide perspective. The SDN controller acts as the "brain" of the network,

programming the behavior of all network devices simultaneously and consistently (Fitrian et al., 2025; Chen et al., 2024; Mensah et al., 2024). Administrators can apply network policies, configure routing, and set security rules from a single, centralized interface, dramatically reducing the complexity of network management.

This centralized management provides greater visibility across the entire network. Administrators can monitor traffic, identify bottlenecks, and detect anomalies from a single dashboard that provides real-time information about network health (Mensah et al., 2024; Singla, 2024). When problems occur, troubleshooting becomes much more efficient because administrators can quickly identify the source of the problem and implement solutions without having to access each device individually. This capability is invaluable in complex campus environments with hundreds or thousands of connected devices.

Automation is another key benefit of SDN that significantly improves operational efficiency. SDN enables the automation of various network tasks that previously required manual intervention, such as provisioning new devices, deploying new services, or adjusting configurations based on changing needs (Amalia et al., 2021; Yaqin, 2020). In a campus context, when new students enroll or new study programs are launched, administrators can quickly provision the necessary network access and services through automated workflows. This automation not only saves time but also reduces human error that often occurs with manual configuration.

Scalability is a particularly relevant advantage of SDN for growing educational institutions. Adding new network devices, expanding coverage areas, or increasing capacity can be done relatively easily without requiring extensive reconfiguration of existing infrastructure (Chen et al., 2024; Salim, 2023; Singla, 2024). The SDN controller can automatically detect new devices connected to the network and configure them according to predefined policies. This flexibility allows institutions to quickly respond to changing needs, whether it's an increase in the number of users, the addition of new services, or the geographic expansion of the campus.

SDN also facilitates the implementation of the network slicing concept, where a single physical infrastructure can be divided into multiple isolated virtual networks for different needs (Alnaim, 2024). For example, a campus could have separate slices for academic, research, administrative, and guest networks, each with distinct security and QoS policies (Singla, 2024). This isolation enhances security and ensures that issues in one slice do not affect others. The flexibility to dynamically create, modify, and delete network slices gives institutions the ability to optimize infrastructure usage according to changing priorities.

The implementation of SDN with deep reinforcement learning algorithms, as discussed in the context of campus networks, shows potential for more intelligent network optimization (Salim, 2023; Chanhemo et al., 2023). Machine learning algorithms can learn network traffic patterns and

automatically adjust routing and resource allocation to optimize performance. This approach elevates campus networks to a higher level of automation, allowing systems to self-optimize based on changing conditions and predicted demands.

Security and Redundancy in SDN Architecture

Network security is a critical aspect of campus infrastructure that manages sensitive academic data. SDN offers a more adaptive and comprehensive security approach than traditional architectures. One key advantage is the ability to centrally integrate firewalls within an SDN architecture (Hariyadi et al., 2025; Saputra & Dalimunthe, 2021). Firewalls implemented at the data link layer in SDN can monitor and control data traffic in real time based on centrally defined policies. Administrators can quickly apply, modify, or revoke security rules across the entire network without having to configure each firewall device individually.

An SDN-based security approach enables the implementation of micro-segmentation, where the network is divided into small segments with granular security policies. Each segment can have specific access rules, limiting lateral movement in the event of a security breach (Hariyadi et al., 2025). In a campus context, different faculties or departments can be isolated from each other at a logical level while still sharing the same physical infrastructure. This isolation reduces the attack surface and limits the potential impact of a security incident.

SDN also facilitates the implementation of security policies that can dynamically adapt based on network conditions. For example, when the system detects an anomaly or potential attack, the SDN controller can automatically isolate the affected network segment, block suspicious traffic, or redirect traffic for further inspection (Saputra & Dalimunthe, 2021). This automated response is much faster than manual intervention, reducing the window of exposure and potential damage from cyberattacks. The ability to implement security controls programmatically also facilitates integration with security information and event management (SIEM) systems and threat intelligence platforms.

Firewall integration into virtualization platforms like Proxmox demonstrates how SDN can secure container services and applications running on campus cloud infrastructure (Hariyadi et al., 2025). With centralized network configuration control, administrators can ensure that each container or virtual machine has an appropriate security posture consistent with institutional policies. This approach is particularly relevant for campuses that are increasingly adopting cloud-based services and containerized applications.

Redundancy and high availability are other important aspects supported by SDN (Rischke et al., 2019). The implementation of redundancy protocols such as HSRP (Hot Standby Router Protocol) and VRRP (Virtual Router Redundancy Protocol) in SDN-based virtual networks improves service availability by providing automatic failover in the event of a gateway failure (Silalahi et al., 2025). In campus environments where service continuity is crucial, especially for academic information systems and online learning, the

ability to minimize downtime becomes invaluable. SDN facilitates the implementation and management of these redundancy protocols more efficiently than conventional networks.

Link aggregation and auto-failover technologies can also be integrated with SDN to increase bandwidth and reliability (Muwajihan & Jatikusumo, 2021). Multiple physical links can be aggregated into a single logical link with greater bandwidth, and if one link fails, traffic is automatically redirected to the remaining active link without service interruption. SDN's ability to manage and automate the failover process ensures that very short recovery time objectives (RTOs) can be achieved, maintaining high levels of service availability.

Implementation Challenges and Mitigation Strategies

Although SDN offers numerous advantages, its implementation is not without challenges (Al-Heety et al., 2020). One major challenge is the need for training and competency development of human resources. SDN represents a different paradigm in network management, and IT staff accustomed to traditional approaches need to develop a new skillset (Fitrian et al., 2025; Chanhemo et al., 2023). Understanding software-defined concepts, programming for network automation, and new tools for SDN management requires an investment of time and resources in training and development. Institutions need to develop ongoing training programs that encompass both theoretical aspects and hands-on practice with SDN technology.

Another technical challenge is the complexity of designing and implementing an SDN architecture that meets the specific needs of a campus. Each institution has unique characteristics in terms of network size, types of services provided, and specific requirements that need to be accommodated (Chen et al., 2024; Mensah et al., 2024). Inappropriate design can result in suboptimal implementation or even create new problems. Therefore, the planning and design phase must be carried out carefully, involving an in-depth analysis of existing infrastructure, traffic patterns, and future requirements. A small-scale pilot implementation before full deployment can help identify and address potential issues.

Developing a comprehensive security policy is another important challenge. While SDN offers enhanced security capabilities, its effectiveness depends heavily on the policies defined and implemented (Fitrian et al., 2025; Saputra & Dalimunthe, 2021; Hariyadi et al., 2025). Institutions need to develop security policies that encompass access control, segmentation strategies, threat response procedures, and compliance requirements. These policies must be comprehensive yet practical to implement and manage. Involving stakeholders from various units in policy development can ensure that security controls do not hinder operational needs while maintaining a strong security posture.

Integrating SDN with existing infrastructure can also be challenging, especially if institutions still have legacy systems that are not fully compatible with SDN (Mensah et al., 2024). A carefully planned migration strategy is needed to ensure a smooth transition without disrupting ongoing operations. A

hybrid approach where SDN and traditional networking coexist during the transition period can be a practical solution, allowing institutions to gradually adopt SDN while maintaining continuity of services.

Testing and validation on complex topologies are crucial but often underestimated aspects. Simulation and testing in environments representative of actual deployment conditions are crucial for identifying potential performance issues or configuration problems (Fitrian et al., 2025; Chen et al., 2024; Salim, 2023). Institutions should allocate adequate resources for a comprehensive testing phase, including stress testing, failover testing, and security testing. Lessons learned from the testing phase can inform refinements to the design and implementation strategy.

Initial investment costs can also be a barrier, especially for institutions with budget constraints. While SDN can reduce operational costs in the long term, the initial investment for controller hardware/software, compatible network devices, and training can be significant (Yaqin, 2020). Institutions need to conduct a comprehensive cost-benefit analysis and consider a phased implementation approach that allows for spreading the investment over time. Exploring open-source SDN solutions can also be an option for reducing costs while still gaining the benefits of SDN technology.

SDN Performance and Advantages Comparison Table

Aspect	Conventional Network	SDN Network	Improvement	Source
Latency (ms)	37.7	18	↓ 52.3%	Fitrian et al. (2025); Gonzales & Pitogo (2024); Mahdiyah et al. (2021)
Jitter (ms)	40.3	2.7	↓ 93.3%	Fitrian et al. (2025); Gonzales & Pitogo (2024); Mahdiyah et al. (2021)
Throughput (Mbps)	95	98.2	↑ 3.4%	Fitrian et al. (2025); Gonzales & Pitogo (2024); Mahdiyah et al. (2021)
Management	Manual, separate, per device	Centralized, automated, network-wide	High efficiency, minimal error	Mensah et al. (2024); Chen et al. (2024); Singla (2024)
	Difficult, requires	Easy, automatic, plug-and-play	Fast deployment	Chen et al. (2024); Salim

Scalability	complex manual configuration			(2023); Singla (2024)
Security	Static, fragmented, reactive	Adaptive, centralized, proactive	Real-time response	Saputra & Dalimunthe (2021); Hariyadi et al. (2025)
QoS Management	Limited, difficult to configure	Flexible, programmable, dynamic	Bandwidth optimization	Fitrian et al. (2025)
Redundancy	Complex, requires per-device configuration	Integrated, automated, centralized	High availability	Silalahi et al. (2025); Muwajihan & Jatikusumo (2021)

The table above shows a comprehensive comparison between conventional networks and SDN in various critical aspects for campus networks. Quantitative data on performance metrics shows a very significant superiority of SDN, especially in jitter reduction reaching 93.3%, making SDN very ideal for real-time applications that are sensitive to delay variations such as video conferencing and virtual classrooms. Qualitative aspects such as management, scalability, and security also show a fundamental transformation from a manual and reactive approach to an automated and proactive one, which directly contributes to increased operational efficiency and long-term cost reduction.

Table of Main Advantages of SDN in Campus Networks

Main Advantages	Explanation	Benefits for Campus	Source
Low Latency & Jitter	More stable connection for real-time applications	Smooth video conferencing, responsive online learning	Fitrian et al. (2025); Shodiq & Prihanto (2021); Mahdiyah et al. (2021); Manuputty & Widiasari (2024)
High Throughput	Faster and more consistent data transfer	Fast material download/upload, optimal LMS	Fitrian et al. (2025); Shodiq & Prihanto (2021); Mahdiyah et al. (2021); Yaqin (2020)
Centralized Management	Configuration & monitoring from one point	Fast troubleshooting, efficient service deployment	Fitrian et al. (2025); Mensah et al. (2024); Chen et al. (2024); Singla (2024)
			Yaqin (2020); Amalia

Automation & Scalability	Easy to add/change devices & policies	Easy campus expansion, new services quickly available	et al. (2021); Chen et al. (2024); Salim (2023)
Integrated Security	Centralized and adaptive firewall & access control	Civitas data protection, rapid threat response	Hariyadi et al. (2025); Saputra & Dalimunthe (2021)
Redundancy & Availability	Automatic failover, minimal downtime	Academic services are always available	Silalahi et al. (2025); Muwajihan & Jatikusumo (2021)
Dynamic QoS	Bandwidth priority based on application	Guaranteed priority service when the network is congested	Fitrian et al. (2025)

To address the challenges faced by the Ichsan Sidenreng Rappang University network, the recommended Software Defined Networking (SDN) topology design is a three-layer architecture consisting of core, distribution, and access layers. The core layer houses a primary SDN controller (e.g., RYU or ONOS), which serves as the control center for all network policies. This controller manages data traffic, security policies, and dynamically distributes bandwidth based on application priorities, such as academic information systems and e-learning platforms.

The distribution layer acts as a bridge between the core and access layers, using OpenFlow switches to facilitate two-way communication between the controller and user devices. Switches in this layer can be centrally configured to manage Quality of Service (QoS), traffic restrictions, and VLAN management between faculties or work units. Meanwhile, the access layer serves end-user connections such as lecturers, students, and administrative staff through access points or wired devices integrated with the SDN network. In this topology, each campus network segment for example, the rectorate building, computer labs, and data centers can be configured as a separate network slice with specific security policies and bandwidth allocations. This approach allows for traffic isolation between units without the need for additional physical infrastructure, while improving security and efficient use of network resources. The implementation of this SDN-based three-layer topology also allows for the automatic addition of new devices (plug-and-play) and supports network redundancy through link aggregation and failover mechanisms, ensuring campus services remain available even if a disruption occurs to one of the network nodes.

CONCLUSION

The implementation of Software Defined Networking on the Ichsan Sidenreng Rappang University campus network is a strategic step to transform the network infrastructure towards a more modern, efficient, and adaptive

architecture. Based on literature analysis, SDN has been proven to provide significant performance improvements with latency reductions of up to 52%, jitter reductions of up to 93%, and throughput increases of 3.4% compared to conventional networks. These advantages are highly relevant to support online learning activities, academic information systems, and other digital services that are the backbone of modern campus operations.

In addition to improved performance, SDN offers flexibility and operational efficiency through centralized management, configuration automation, and high scalability. The separation of the control plane and data plane allows administrators to manage the entire network from a single point of control, dramatically reducing complexity and human error. Security aspects are also significantly enhanced with the integration of adaptive firewalls and the ability to respond to threats in real time. The implementation of redundant protocols in the SDN architecture also ensures high service availability, minimizing downtime that can disrupt academic processes. However, implementing SDN requires careful planning, ongoing human resource training, the development of comprehensive security policies, and testing on complex topologies to ensure a successful deployment.

Recommendations for Ichsan Sidenreng Rappang University include conducting a limited-scale pilot project before full deployment, investing in ongoing training programs for IT staff, developing a security policy that integrates technical and procedural aspects, and collaborating with other institutions that have successfully implemented SDN to share best practices. With a planned and systematic approach, SDN implementation can provide a strong foundation to support the digitalization of higher education and prepare institutions for future technological challenges.

BIBLIOGRAPHY

Al-Heety, O. S., Zakaria, Z., Ismail, M., Shakir, M. M., Alani, S., & Alsariera, H. (2020). A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET. IEEE Access, 8, 91028–91047. https://doi.org/10.1109/ACCESS.2020.2992580

Alnaim, A. K. (2024). Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security. International Journal of Information Security, 23(6), 3569–3589. https://doi.org/10.1007/s10207-024-00900-5

Amalia, R., Kalsum, T., & Riska, R. (2021). Analisis dan Implementasi Software Defined Networking (SDN) untuk Automasi Perangkat Jaringan. Infotek: Jurnal Informatika dan Teknologi. https://doi.org/10.29408/jit.v4i2.3734

Chanhemo, W., Mohsini, M., Mjahidi, M., & Rashidi, F. (2023). Deep learning for SDN-enabled campus networks: proposed solutions, challenges and future directions. International Journal of Intelligent Computing and Cybernetics, 16, 697-726. https://doi.org/10.1108/ijicc-12-2022-0312

Chen, M., Gu, Y., Zhang, Y., & Qu, Q. (2024). A Campus Local Area Network Architecture based on Software Defined Networking. 2024 Sixth

International Conference on Next Generation Data-driven Networks (NGDN), 78-81. https://doi.org/10.1109/ngdn61651.2024.10744183

Espinel Sarmiento, D., Lebre, A., Nussbaum, L., & Chari, A. (2021). Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey. IEEE Communications Surveys & Tutorials, 23(1), 256–281. https://doi.org/10.1109/COMST.2021.3050297

Fitrian, H., Adkia, A., Rahmadani, S., Kencana, R., & Fiddin, I. (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). https://doi.org/10.32672/jnkti.v8i1.8627

Gonzales, C., & Pitogo, V. (2024). Performance Analysis of Caraga State University's Network Infrastructure: A Software-defined Networking Approach. 2024 4th International Conference of Science and Information Technology in Smart Administration (ICSINTESA), 396-401. https://doi.org/10.1109/icsintesa62455.2024.10747881

Hariyadi, I., Dharma, I., Azhar, R., & Suriyati, S. (2025). Implementasi Software-Defined Network Terintegrasi Firewall pada Proxmox untuk Pengontrolan Konfigurasi Jaringan dan Pengamanan Layanan Container. JTIM: Jurnal Teknologi Informasi dan Multimedia. https://doi.org/10.35746/jtim.v7i1.644

Mahdiyah, L., Ginting, J., & Iryani, N. (2021). Analisis Perbandingan Performansi Eksternal Border Gateway Protocol (EBGP) pada Jaringan Konvensional dan Jaringan Software Defined Network. RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer). https://doi.org/10.24853/resistor.4.2.147-154

Manuputty, Y., & Widiasari, I. (2024). Analisis Performa Jaringan Software Defined Networking dengan Algoritma Random Early Detection. Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi). https://doi.org/10.35870/jtik.v8i2.1745

Mensah, J., Abandoh-Sam, J., Amankwah, H., & Tchouchu, E. (2024). The Relevance of Development and Deployment of Software Defined Networking Solutions for a University Network. Indian Journal of Data Communication and Networking. https://doi.org/10.54105/ijdcn.c5034.04020224

Muwajihan, I., & Jatikusumo, D. (2021). Perancangan Jaringan Ethernet Link Dengan Menggunakan Teknologi Link Aggregation dan Auto Failover. IJCIT (Indonesian Journal on Computer and Information Technology). https://doi.org/10.31294/ijcit.v6i2.10866

Rischke, J., Gabriel, F., Pandi, S., Nguyen, G., Salah, H., & Fitzek, F. H. P. (2019). Improving Communication Reliability Efficiently: Adaptive Redundancy for RLNC in SDN. 2019 IEEE Conference on Network Softwarization (NetSoft), 291–295. https://doi.org/10.1109/NETSOFT.2019.8806682

Salim, E. (2023). Software-Defined Networking-Based Campus Networks Via Deep Reinforcement Learning Algorithms: The Case of University of

Technology. International Journal on Recent and Innovation Trends in Computing and Communication. https://doi.org/10.17762/ijritcc.v11i10.8726

Saputra, H., & Dalimunthe, R. (2021). Implementasi Firewall pada Data Link Layer Menggunakan Arsitektur Software Defined Network. Jurnal Teknik Sistem Komputer dan Informatika, 7, 245-250. https://doi.org/10.33330/jurteksi.v7i3.1199

Shodiq, F., & Prihanto, A. (2021). Analisis Perbandingan Performansi Kontroler RYU Dan POX Berbasis Software Defined Network (SDN) Pada Routing OSPF. Journal of Informatics and Computer Science (JINACS). https://doi.org/10.26740/jinacs.v3n03.p216-223

Silalahi, E., Sitanggang, Y., Suryaningsih, E., & Kiswanto, D. (2025). Implementasi dan Analisis Protokol HSRP dan VRRP dalam Meningkatkan Redundansi Gateway pada Jaringan Virtual. Jurnal Informatika dan Teknik Elektro Terapan. https://doi.org/10.23960/jitet.v13i2.6474

Singla, N. (2024). Configuration of Complex Networking Using Secure Software Defined Network System. Communications on Applied Nonlinear Analysis. https://doi.org/10.52783/cana.v32.2409

Yaqin, M. (2020). Perancangan dan Implementasi Protokol Routing EBGP pada Software Defined Network Menggunakan ONOS Controller. Jurnal Teknologi Informasi, 6.