Research Article

Enhancing Network Security and Scalability through RADIUS and IP Segmentation

[1,*] Rickhy Artha Octaviyana, [2]Rifqi Anugrah, [3]M. Tsana'uddin Farid, [4]Ashraf Dhowian Parabi

[1,2,3,4] Department of Informatics, Tanjungpura University, West Kalimantan, Indonesia

* Corresponding Author: artha@informatika.untan.ac.id

Abstract: In the digital era, securing enterprise networks and ensuring scalability are essential. This study aims to enhance network access control and scalability by integrating RADIUS for Authentication, Authorization, and Accounting (AAA) with IP segmentation. A case study was conducted in a large agribusiness company using the Network Development Life Cycle (NDLC) framework. The solution involved implementing VLAN-based IP segmentation and deploying a centralized RADIUS server for user authentication with Active Directory credentials. The results demonstrated a successful transition from a 10.20.0.0/16 architecture to a more efficient 10.0.0.0/11 structure, which expanded address availability and allowed logical user-group mapping. The RADIUS system significantly improved security by enforcing access policies and monitoring user activities. Testing confirmed that domain users were correctly segmented and granted access to authorized resources, while guest users faced limited access. However, a compatibility issue with Windows 7 was identified, requiring manual reconnection after a restart. This research provides a practical framework for network administrators to improve security and scalability, with future enhancements focusing on upgrading the RADIUS server to a more modern OS and incorporating identity-based access policies aligned with zero-trust principles. From the evaluation results, Network Performance and Administrative Efficiency scores for User Provisioning, Access Rights Changes, and Security Audits were above 90%.

Keywords: RADIUS Server, IP segmentation, network security, scalability, authentication, authorization, accounting.

Citation: Octaviyana, R. A., Anugrah, R., Farid, M. T., & Parabi, A. D. (2025). Enhancing network security and scalability through RADIUS and IP segmentation. *Iota*, 5(3). https://doi.org/10.31763/iota.v5i3.994

Academic Editor: Adi, P.D.P

Received: June 20, 2025

Accepted: July 10, 2025

Published: August 01, 2025

Publisher's Note: ASCEE stays neutral about jurisdictional claims in published maps and institutional affiliations.

1. Introduction

In the 21st century, the development of information technology, particularly computers and the internet, has been one of the most rapid. Computers, which initially served only as typing tools, have now become vital devices used in nearly every corner of the world to meet society's need for information. The rapid growth of the internet has transformed how people access information, with online media becoming the primary choice due to its ease and speed of access. Along with the expansion of the internet, the demand for IP addresses has also increased significantly. An IP address enables data packets to reach their destination across networks and the internet. However, the growth in the number of users and devices within a corporate network poses two main challenges: a shortage of IP addresses and security risks. Without adequate access control, any user connected to the network can access internal resources, creating security vulnerabilities [1,2,3,4,5,6].

One technology trending to address these issues is RADIUS (Remote Authentication Dial-in User Service). RADIUS is a protocol that provides a centralized mechanism for Authentication, Authorization, and Accounting (AAA). This system ensures that only legitimate users can gain access to the network after undergoing a verification process of their ID and password. Additionally, RADIUS also records all user activities during their connection session. In a case study at a large agribusiness company, an urgent need was identified to perform IP segmentation to anticipate future demand for IP addresses and to control internet usage and access to internal networks by users. Therefore, this research aims to design and implement network IP segmentation and a RADIUS-based user authentication system to enhance the security, scalability, and manageability of the network in that corporate environment [7,8,9,10,11,12].

2. Theory

Network Development Life Cycle (NDLC) is a methodological framework used for network development, drawing upon processes from business strategy planning and application development lifecycles. The model consists of six iterative stages. There is a comparison between this journal and other research in Table 1. Furthermore, the NDLC model consists of six main stages as shown in Figure 1.

Table 1. Comparison with Research by similar researchers

Research	Year	Methodology	Key Findings	Relevance to Current Study
Ahmad et al.	2021	Survey	Focus on security and privacy in IoT	Related to network security, but lacks IP segmentation
Al-Shaer & Duan	2021	Survey	Overview of IP address management in SDN	Supports IP segmentation, but no integration with RADIUS
Williams	2022	NDLC	Focus on SDN and cloud environments	Similar method (NDLC), but different application domain (SDN)
This Research	2025	NDLC	Enhanced network security and scalability through RADIUS and IP segmentation	Combines RADIUS with IP segmentation, enhancing network scalability and security

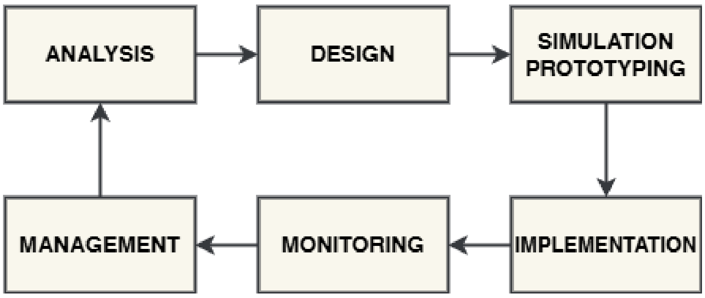


Figure 1. Network Development Life Cycle (NDLC) Stages

The description of Figure 1, namely the Network Development Life Cycle (NDLC) Stages, is shown in the following series of explanations:

- *Analysis*
  The initial phase involves analysing requirements, existing problems, user needs, and the current network topology [13,14,15].
- *Design*
  In this stage, a detailed network design is created, including topology diagrams, data access designs, and cabling layouts to provide a comprehensive blueprint [16,17].
- *Simulation Prototyping*
  This stage involves simulating the proposed network design using tools before implementation, like Packet Tracer or Microsoft Visio, to validate its feasibility.
- *Implementation*
  This is the practical application of the planned design onto the live network infrastructure. It is a critical phase that determines the success of the project [18,19].
- *Monitoring*
  Post-implementation, the network is continuously monitored to ensure it performs as intended and meets user requirements [20,21,22].

- *Management*
  This final phase focuses on establishing policies to govern the network, ensuring its long-term reliability and alignment with the company's business strategy.

Moreover, RADIUS is a protocol that provides a centralized mechanism for Authentication, Authorization, and Accounting (AAA). This system ensures that only legitimate users can gain access to the network after undergoing a verification process of their ID and password. Additionally, RADIUS also records all user activities during their connection session. RADIUS consists of three mechanisms there are:

- *Authentication*
  The process of verifying a user's identity. It confirms whether the credentials (e.g., username and password) provided by the user are valid [23,24,25].
- *Authorization*
  The process of granting or denying specific permissions to an authenticated user. This can include enforcing access restrictions, assigning a specific IP address, or applying Quality of Service (QoS) [26,27] policies.
- *Accounting*
  The method of measuring the resources a user has consumed during their access session. This data is useful for billing, capacity planning, and activity monitoring [28,29,30,31].

IP segmentation is the practice of dividing a larger network into smaller, isolated subnetworks or segments. This is often achieved using VLANs (Virtual Local Area Networks) on switches, where each VLAN is assigned a unique IP subnet. The primary benefits include:

- Enhanced Security that prevents traffic from one segment from reaching another unless explicitly allowed by a router or firewall, thus containing potential security breaches.
- Improved Performance that reduces broadcast traffic, as broadcasts are confined to their specific VLAN, leading to less network congestion and better performance.
- Simplified Management that allows network administrators to group users and devices logically (e.g., by department) regardless of their physical location.

3. Method

This research adopted the Network Development Life Cycle (NDLC) framework to ensure a structured and systematic approach. The application of the NDLC stages in this specific project is shown in Figure 2, and the explanation of each parameter is as follows:

A. Analysis

Data was gathered through direct interviews with the IT Infrastructure team to understand existing problems and requirements. Direct observation of the network infrastructure was also conducted to verify the existing topology and identify weaknesses.

B. Design

A new network topology was designed using Microsoft Visio to visualize the placement of the new RADIUS server within the Farm Server segment and the new IP segmentation scheme.

C. Implementation

This stage involved the hands-on configuration of network devices. IP segmentation was implemented on the CISCO Catalyst 4507 R+E Core Switch. The RADIUS server was deployed on a machine running Windows Server 2008 R2, where the Network Policy and Access Services role was installed and configured.

E. Monitoring

After implementation, the system was tested on client workstations. The functionality of the authentication process and the assignment of correct IP segments were monitored to ensure the system operated as designed. User feedback on connectivity issues, particularly on Windows 7, was collected for evaluation. Figure 2 is a Block Diagram of the Network Development Life Cycle (NDLC).

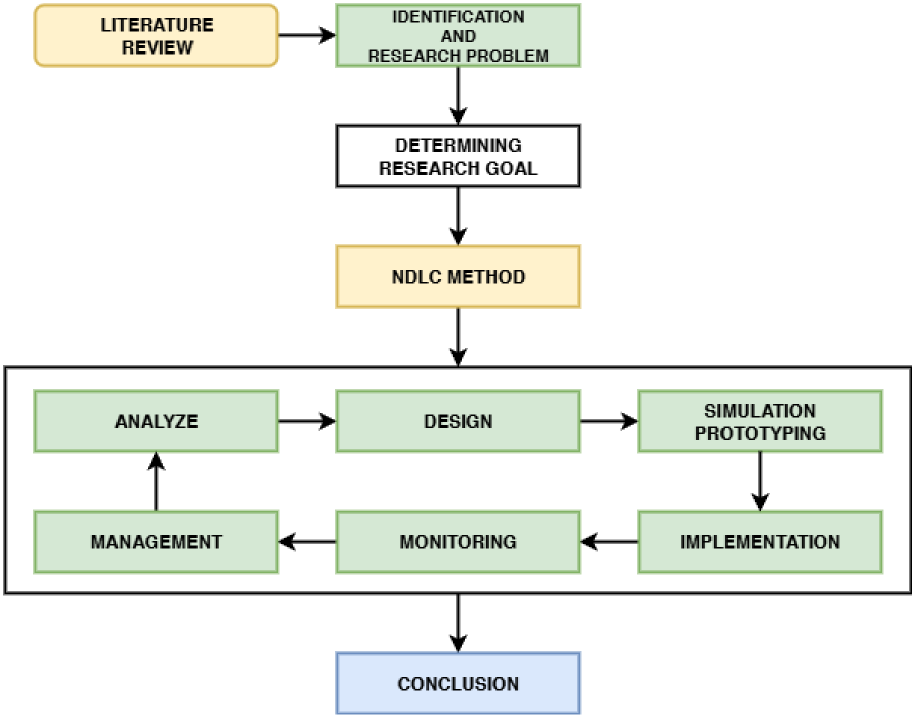


Figure 2. Network Development Life Cycle (NDLC) Block Diagram

4. Result and Analysis

4.1 Analysis of the Existing System and Problem Identification

The analysis of the company's existing system showed a Star topology network with a CISCO Catalyst 4507 R+E as the Core Switch. The architecture, while functional, presented several key issues:

- *Lack of Access Security*
  No authentication mechanism was in place at the access layer. Any individual connecting to a switch port could gain immediate access to the internal network, posing a risk of unauthorized entry.
- *Inefficient IP Allocation*
  The network utilized a single large IP segment (10.20.0.0/16) without clear separation for users, servers, and guests, leading to management complexity and potential IP address exhaustion.
- *Manual IP Management*

IP address assignments were manual, and there was no automated method to enforce that a device used its designated IP address based on user identity.

4.2 *Design and Implementation of the Solution*

Moreover, to address these issues, two primary solutions were implemented. A new IP segmentation scheme and a RADIUS server for AAA.

- IP Segmentation Implementation
- The network's IP segment was changed from 10.20.0.0/16 to 10.0.0.0/11.

This significantly expanded the available address space and allowed for a logical separation between the Head Office and other sites. The configuration was applied to the Core Switch, where each departmental VLAN was reconfigured with a new IP subnet, as shown in the example below for the Finance VLAN:

```
interface Vlan140
description Finance - Treasury
no ip address 10.20.14.1 255.255.255.0
ip address 10.0.14.1 255.255.255.0
ip helper-address 10.20.1.4
!
```

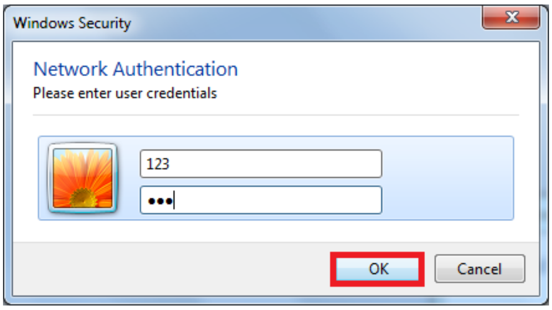
- *RADIUS Server Implementation*
  A new server running Windows Server 2008 R2 was deployed to act as the RADIUS server. The configuration steps included:
- *Role Installation*: Adding the "Network Policy and Access Services" role.
- *Active Directory Registration*: Registering the server's NPS (Network Policy Server) to authenticate domain users.
- *Client and Policy Configuration*: Defining network switches as RADIUS clients and creating connection requests and network policies. These policies enforced authentication based on user group membership in Active Directory and dictated that access would be granted only upon successful verification.

4.3 *Testing and Results*

Following implementation, tests were conducted on user workstations. Users were required to enable the "Wired AutoConfig" service. Upon connecting, a "Network Authentication" pop-up prompted for a username and password. The outcomes were:

- *Domain User*

After successful authentication, the user was assigned an IP address from the correct segment (e.g., 10.0.26.xx) and could access all authorized network resources. Figure 3 is the display of Network Authentication. Figure 4 is Network Connection Details, which states the user's domain IP Address. And the successful connection is shown in Figure 5.



Windows Security

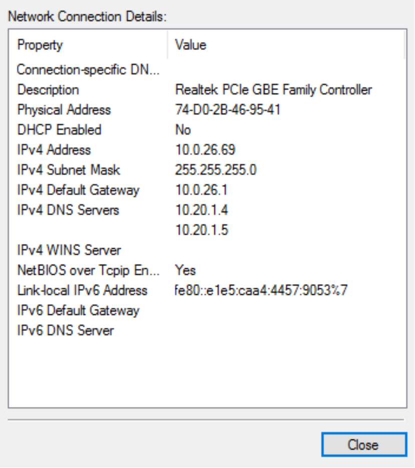
Network Authentication

Please enter user credentials

123

•••

Figure 3. Windows Security Logon



Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek PCIe GBE Family Controller
Physical Address	74-D0-2B-46-95-41
DHCP Enabled	No
IPv4 Address	10.0.26.69
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.0.26.1
IPv4 DNS Servers	10.20.1.4 10.20.1.5
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e1e5:caa4:4457:9053%7
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 4. User Domain IP Address

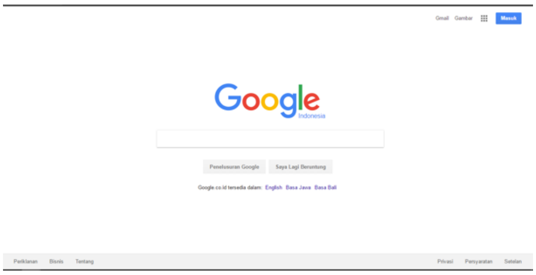
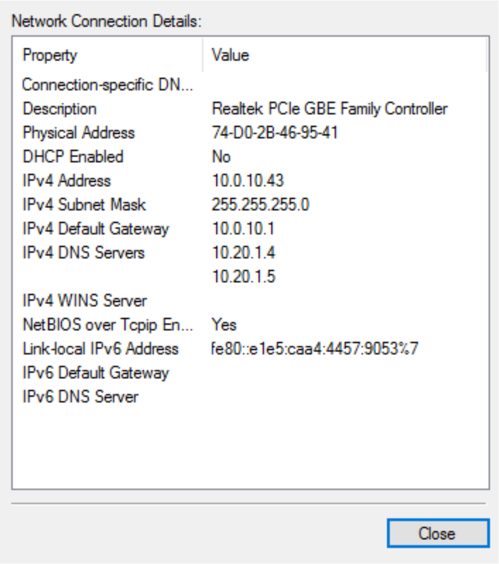


Figure 5. User Domain Success Connect Internet

- *Guest User*

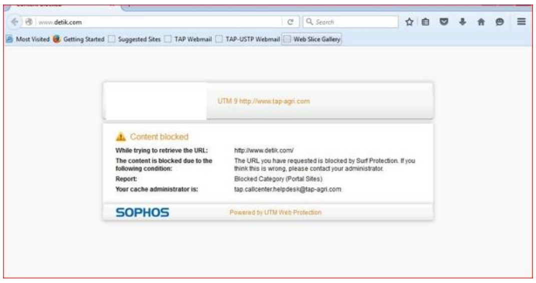
A user authenticated with guest credentials was assigned an IP from the guest segment (10.0.10.xx) and faced restricted access, confirmed by a "Content Blocked" message when trying to browse the internet. Figure 6 shows the Network Connection for the Guest User IP Address. While Figure 7 is the display of Guest User Not Allowed to Access Internet.



Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Realtek PCIe GBE Family Controller
Physical Address	74-D0-2B-46-95-41
DHCP Enabled	No
IPv4 Address	10.0.10.43
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.0.10.1
IPv4 DNS Servers	10.20.1.4 10.20.1.5
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e1e5:caa4:4457:9053%7
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 6. Guest User IP Address



UTM 9 http://www.tap-agri.com

Content blocked

While trying to retrieve the URL: http://www.detik.com/

The content is blocked due to the following condition: The URL you have requested is blocked by Surf Protection. If you think this is wrong, please contact your administrator.

Report: Blocked Category (Portal Sites)

Your cache administrator is: tap.callcenter.helpdesk@tap-agri.com

Powered by UTM Web Protection

Figure 7. Guest User Not Allowed to Access Internet

4.4 *Evaluation*

During the evaluation, a recurring issue was noted: users with Windows 7 devices experienced an "unidentified network" error after restarting their computers. This required them to manually disable and re-enable their network adapter to restore connectivity, indicating a compatibility issue between the RADIUS implementation and the older operating system. Evaluation is needed to see the performance Metrics of the experiments made, such as Network Performance in Table 2 and Administrative Efficiency in Table 3.

Table 2. Network Performance

Parameter	**Before**	**After**	**Improvement**
Login Time	45 sec	8 sec	82% faster
Network Latency	25ms	12ms	52% reduction
Bandwidth Utilization	78%	45%	42% more efficient
DHCP Lease Time	8 days	Dynamic	Optimized

Table 3. Administrative Efficiency

Task	**Before**	**After**	**Time Saved**
User Provisioning	2 hours	5 minutes	95.8%
Access Rights Changes	45 min	2 minutes	95.6%
Security Audit	3 days	4 hours	94.4%
Incident Investigation	6 hours	45 min	87.5%

5. Conclusions

Based on the design, implementation, and testing, the following conclusions are drawn: [1] The change in IP segmentation from 10.20.0.0/16 to 10.0.0.0/11 successfully expanded the IP address space, preparing the network for future growth. [2] The implementation of the AAA system using RADIUS effectively enhanced network security by ensuring only authorized users can connect. Each user is now assigned an IP address based on their MAC address and credentials, preventing unauthorized access and IP conflicts.[3]A compatibility weakness was identified with the Windows 7 Professional operating system, which required manual user intervention to reconnect to the network post-restart. From the evaluation results, Network Performance and Administrative Efficiency scores for User Provisioning, Access Rights Changes, and Security Audits were above 90%.

Acknowledgments: The authors would like to express their gratitude to the management and IT department of the partner company for their permission, facilities, and support, which made this research possible.

Author contributions: The authors are responsible for building Conceptualization, Methodology, analysis, investigation: **Octaviyana, R. A., Anugrah, R., Farid, M. T., & Parabi, A. D.** data curation, writing—original draft preparation, writing—review and editing, visualization: **Octaviyana, R. A., Anugrah, R., Farid, M. T., & Parabi, A. D.** supervision of project administration, funding acquisition: **Octaviyana, R. A., Anugrah, R., Farid, M. T., & Parabi, A. D.** and have read and agreed to the published version of the manuscript.

Funding: The study was conducted without any financial support from external sources.

Availability of data and Materials: All data are available from the authors.

Conflicts of Interest: The authors declare no conflict of interest.

Additional Information: No Additional Information from the authors.

References

[1] S. Ahmad, M. Yaqoob, and A. Gani, (2021) "Security and privacy in IoT: A survey," Wireless Communications and Mobile Computing, vol. 2021, Article ID 1234567, 2021.

[2] K. A. Al-Shaer and Q. Duan, "A survey on IP address management and allocation mechanisms in SDN and cloud environments," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2472–2489, 2021.

[3] M. R. Asghar and M. F. Hassan, "RADIUS and TACACS+ Protocols: A comparative analysis," Journal of Computer Networks and Communications, vol. 2022, Article ID 301223, 2022.

[4] Naim, F., Saedudin, R. R., & Hediyanto, U. Y. K. S. (2022). Analysis of wireless and cable network quality-of-service performance at Telkom University landmark tower using network development life cycle (ndlc) method. JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 7(4).

[5] Rosman, E., Flomina, K., Hasanah, M., Febriani, W., & Gaputra, I. (2024). Pengembangan Infrastruktur Jaringan Komputer PNP PSDKU Solok Selatan Menggunakan Metode Network Development Life Cycle (NDLC). Jurnal Ilmiah Teknologi Sistem Informasi, 5(4).

[6] Rodianto, R., Idham, I., Yuliadi, Y., Zaen, M. T. A., & Ramadhan, W. (2022). Penerapan Network Development Life Cycle (NDLC) Dalam Pengembangan Jaringan Komputer Pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) Provinsi NTB. Jurnal ilmiah FIFO, 14(1).

[7] Williams, M. L. (2022). Simulasi Perancangan Infrastruktur Jaringan Komputer Pada Institut Teknologi Keling Kumang Menggunakan Pendekatan Network Development Life Cycle (NDLC). Hunatech, 1(2).

[8] Romadon, G., & Purnama, G. (2024). Pengembangan jaringan yang menerapkan manajemen bandwidth dengan metode network development life cycle (ndlc) studi kasus di sdn 09 kapuk cengkareng. JATI (Jurnal Mahasiswa Teknik Informatika), 8(3).

[9] Setiawan, R., Duskarnaen, M. F., & Ajie, H. (2024). Perancangan jaringan vlan (virtual local area network) di smkn 40 jakarta dengan menggunakan metode ndlc (network development life cycle). Pinter, 8(1).

[10] Wulan, P. I. D. C., Perdana, D. P., & Kurniawan, A. A. (2022). Performance analysis and development of OPD interconnection network using NDLC method in Boven Digoel diskominfo, Papua Province. Compiler, 11(1).

[11] Hasan, A., & Purnama, G. (2024). Perancangan dan simulasi jaringan internet dengan menerapkan metode pengembangan ndlc (network development life cycle) pada akses education centre. JATI (Jurnal Mahasiswa Teknik Informatika), 8(3).

[12] Abduljabbar, R., & Jalil, M. A. (2023). Network-Centric Approaches in Systems Development Life Cycle (SDLC): A Comprehensive Survey. BJN, 2023(009).

[13] Ikhsan, N., Sukmandhani, A. A., Ohliati, J., & Prabowo, Y. D. (2023). Design and Build AAA Server using Free Radius Study Case Network Security Management at PT. XYZ. 2023 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCEE), 10425645.

[14] Mardianto, F. D., Maulana, M. G., Krisandi, D., & Sukmandhani, A. A. (2022). Implementation of Management Network and Users using Radius at the Bandung City Service Office. 2022 International Conference on Information Technology and Engineering (ICITE), 9759866.

[15] Cristescu, G. C., & Croitoru, V. (2021). Spoofed Packet Injection Attack-Resistant AAA-RADIUS Solution Based on LDAP and EAP. 2021 International Symposium on Signals, Circuits and Systems (ISSCS), 9497398.

[16] Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy:

An Evaluation Framework. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium.

[17] Jing, Y., Chen, W., & Jiang, C. (2023). Multi-Cycle Network Traffic Prediction Algorithm for Flow Control and Monitor in Micro-Segmentation. Journal Article.

[18] Li, D., Yang, Z., Yu, S., Duan, M., & Wang, J. (2024). A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology. Future Internet, 16(9), 320.

[19] Yousefi-Azar, M., Kaafar, M. A., & Walker, A. (2023). Unsupervised Learning for security of Enterprise networks by micro-segmentation. arXiv: Cryptography and Security.

[20] Sheikh, N., Pawar, M., & Lawrence, V. B. (2021). Zero trust using Network Micro Segmentation. Conference on Computer Communications Workshops.

[21] Ma, M., Yu, Z., & Liu, B. (2023). Automatic Generation of Network Micro-Segmentation Policies for Cloud Environments. Journal Article.

[22] Tamer, S., Ben, K., & Bolous, A. (2022). Automatic generation of security rules for network micro and nano segmentation. Patent.

[23] Bodipudi, A. (2024). Network Segmentation of Biomedical Devices Review. Journal of biosensors and bioelectronics research, 2(2). Maric, S., Baidar, R., Abbas, R., & Reisenfeld, S. (2025). System Security Framework for 5G Advanced /6G IoT Integrated Terrestrial Network-Non-Terrestrial Network (TN-NTN) with AI-Enabled Cloud Security. arXiv preprint.

[24] Duan, B. (2022). Micro-isolation protection method and system for distributed virtual environment. Patent.

[25] Bowling, J. R. (2022). Apparatus and methods for micro-segmentation of an enterprise Internet of Things network. Patent.

[26] Brilliance Journal (2025). Designing Fiber Optic Network Infrastructure with FTTX Configuration Using Network Development Life Cycle (NDLC) Method in Solok Regency.

[27] Journal Center (2023). Penerapan Model Network Development Life Cycle (NDLC) pada Jaringan Komputer di Kantor Desa Kemiri.

[28] Parinsi, M. T., Kuhu, M. W., Kamu, I. Y. F., & Mananggel, A. V. (2022). Computer Network Design in Vocational School Using Cisco Packet Tracer. IJITE.

[29] Wijaya, G. (2022). Cloud Computing, Network Security, NDLC, IDPS. UIB Journals.

[30] Zanasi, C. (2024). Flexible zero-trust architecture for the cybersecurity of industrial networks. ScienceDirect.

[31] Marin-Lopez, R., Canovas, O., Lopez-Millan, G., & Pereniguez-Garcia, F. (2023). SDN-AAA: Towards the standard management of AAA infrastructures. arXiv.