



Network Security Analysis Using Switch Port Security CPT

^{1st}Nurfadilah Istiqamah , ^{2nd}Jumadi Mabe Parenreng 

^{1,2}Department of Computer Engineering, Universitas Negeri Makassar, Makassar 90222, South of Sulawesi, Indonesia

*Corresponding Author: jparenreng@unm.ac.id

Abstract:

The gradual advancement of information network technology has rapidly increased due to the growing demand for efficient, stable, and fast network connectivity, as well as reliable information security. One factor that influences network quality is network security, which encompasses various techniques to enhance network security, such as building firewalls, layer seven protocols, and port security. Port security utilizes existing ports to enable secure switching access. The switch can protect the local area network (LAN). Several types of switch port security are commonly used, including default/static port security, dynamic learning port security, and sticky port security.

Keywords: Switch Port Security, Port Security, Network Security, Sticky Port Security, Network Connectivity



Citation: N.Istiqamah, J.M.Parenreng " Network Security Analysis Using Switch Port Security CPT". *Iota*, 2023, ISSN 2774-4353, Vol.03, 04.
<https://doi.org/10.31763/iota.v3i4.614>

Academic Editor : Adi, P.D.P

Received : August, 06 2023

Accepted : September, 17 2023

Published : November, 07 2023

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



Copyright: © 2023 by authors. Licensee ASCEE, Indonesia. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution Share Alike (CC BY SA) license(<https://creativecommons.org/licenses/by-sa/4.0/>)

1. INTRODUCTION

The current technological advancements are rapidly progressing, especially in network security, which is crucial for Internet technology [1]. The need for computer networks is becoming increasingly important in education, work, and entertainment. Network security is one of the most critical aspects of managing a computer network [2]. With many network access points, there are also numerous opportunities for network criminals to engage in activities such as online data theft, disabling network resources for hacking purposes, and so on [3].

Network security has become a significant topic with the development of information technology [4]. It brings not only benefits but also negative aspects [5]. Nowadays, we can witness attacks on computer systems connected to the Internet. As a result of these attacks, many computer systems and networks are disrupted or even damaged [6]. A security system is needed to avoid and handle activities that disrupt the network system to prevent such incidents [7]. Various techniques can be employed to reduce cybercrime, and one commonly used method to secure a LAN is switch port security [8]. Switch port security is a technique that allows anyone with network access to connect to the network through available ports on the switch [9]. This research aims to obtain the results of network security system analysis using switch port security implemented with the Cisco Packet Tracer 7.3.0 application.

2. THEORY

In recent years, the gradual development of information network technology has rapidly progressed in the era of globalization to meet the increasing demand for efficient, stable, and fast access to information and reliable information security [10].

There has been continuous development to enhance computing power and data processing, especially in terms of technology, from personal computers (PCs) to computers. A computer network is a connection between two or more computers that are linked through data transmission media, either wired or wireless [11].

Network security is a system that prevents unwanted activities by identifying users who do not have network access rights [12]. Connecting your computer to other computers through wired or wireless networks allows others to access data, modify content, and even delete data online [13]. Vulnerabilities exist everywhere, from devices and data pathways to applications and users. Organizations, from small businesses to large corporations and service providers, require network security to protect critical assets and infrastructure from rapidly evolving attacks [14].

The task of network security elements is to detect and classify traffic [15]. Switch Port Security is a method that can be implemented on a switch to allow access only to clients whose MAC addresses are stored in the switch's MAC address table, thereby preventing unauthorized hosts from easily connecting to the network through any port on the switch [16]. Switch Port Security can also be referred to as a method that allows specific users to access the network through switch ports to protect the local network [17].

The switch should correctly identify each device; through port security, each device's MAC address will be checked [18]. Switch security settings are divided into three types: Static, where MAC addresses allowed on the port are manually entered, and this information is still stored correctly even when the switch is powered off [19]. Another setting is Dynamic, where the switch automatically detects the first connected MAC address, but the drawback is that the MAC address is lost when the switch is turned off. And Sticky, where the switch automatically saves the first and subsequent connected MAC addresses and retains them even when the switch is powered off [20].

Identifying data characteristics promptly and isolating threats in real time is a major challenge for network security technology [20]. The penalty for devices or devices without registered MAC addresses in the switch is a penalty for violation, commonly known as a violation, which can be set in 3 modes: Protect, where the port is configured to suspend outgoing packets from the device or device, preventing them from reaching the network. If the port is configured, the device's packages are not stopped, only stored and not allowed on the network. Similar to Power Off, when you apply settings to a port, the port immediately shuts down, and the device or device cannot connect automatically [10].

3. METHOD

The method used in this research is port security, which aims to register and restrict which end devices, such as client computers or PCs, can connect to a specific port on a switch. Essentially, port security limits a designated port to only allow the registered MAC address of a specific end device, preventing any other unauthorized devices from connecting. The research process follows a systematic approach that relates to the studied factors using a problem-solving approach. The experimentation will be conducted using the Cisco Packet Tracer 7.3.0 (CPT) simulation.

A. System Architecture

1) *Default / static port security*

Port security is enabled by configuring the MAC address on the switch port. Once port security is activated, the port will not forward packets if the source

address is not the pre-defined address we specified. It allows us to manually determine the specific MAC address that is allowed to connect to that port.

2) *Port security dynamic learning*

Figure 1 is Switch Port Security, explaining that there are two users whose targets are the same switch port, one user who is allowed and one who is not. For those given permission, the user can immediately access it, while those not allowed will be denied access.

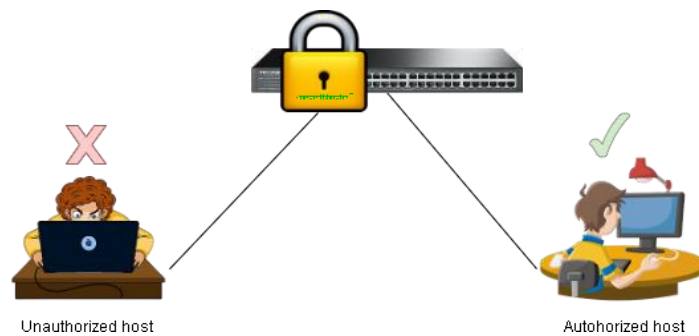


Fig.1. Switch Port Security

3) *Sticky port security*

Figure 2 is Sticky Port Security; the switch's capability to recognize each connected device's MAC address will block any MAC address that exceeds the registered number. The switch reads the MAC address of each connected device. Using Sticky Port Security, the switch can register the number of devices connected to that switch. For example, if only 2 MAC addresses are registered, when a third device tries to connect, the Sticky Port Security feature will automatically prevent (block) that MAC address. As a result, only the first two devices that have been registered will be allowed to connect, and the number of connected devices will remain limited to 2.

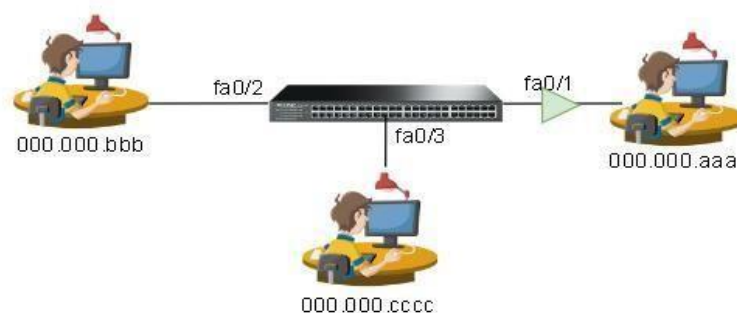


Fig.2. Sticky Port Security

B. Testing Stages

Figure 3 shows the stages carried out with the following phases:

1. Start
2. The configuration steps which include applying configuration to the switch.

3. If the switch configuration is completed, the next step is to access the PC. If unsuccessful, return to the switch configuration step, and if successful, proceed to the next step.
4. If the previous process is successful, the next step is to perform data retrieval.
5. Finished.

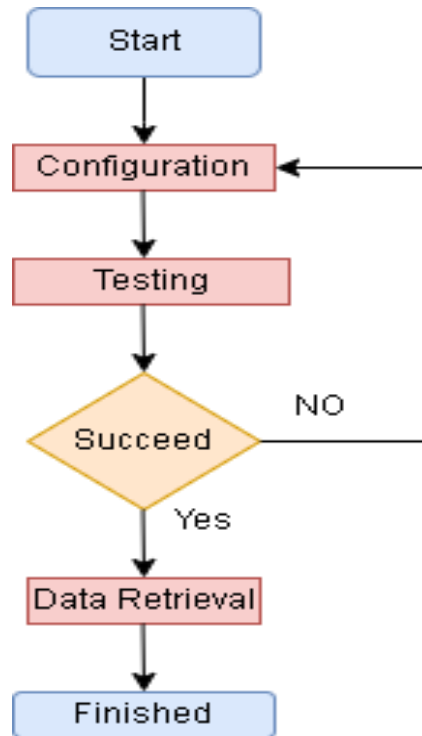


Fig.3. Testing Stage

Furthermore, the Testing Environment for Evaluating the Success of this System with Hardware and Software Specifications is shown in Table 1.

Table 1. System Requirement

ASUS Notebook	
Hardware	Intel(R) Core(TM)i3-5005U CPU @ 2.00GHz (4CPUs), ~2.0GHz
	4096MB GB
	Windows 10 Pro 64-bit (10.0, Build 19045) Version DirectX 12
Software	Cisco Packet Tracer 7.3.0 (64-bit)

4. RESULT AND DISCUSSION

The topology in Figure 4 used for implementing Port Security is shown. We are using a Type 2960-24TT switch and connecting all PCs using straight cables to the switch. PC0 is connected to port fa0/1, PC1 is connected to port fa0/2, and PC2 is connected to port fa0/3 on the switch.

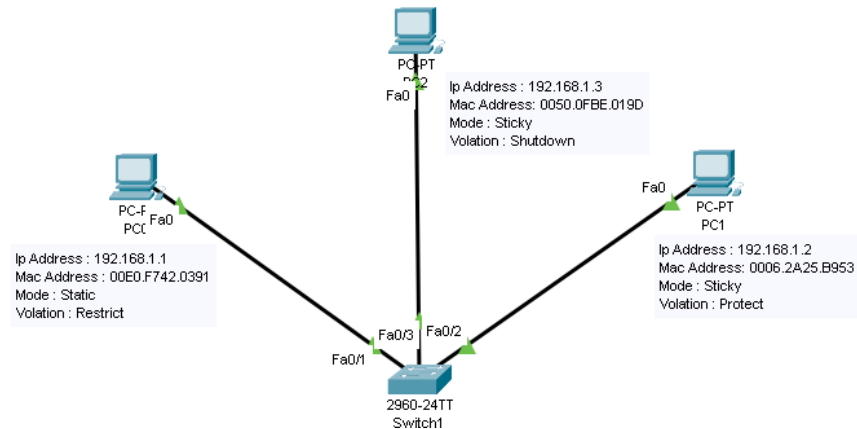


Fig.4. Cisco Switch Port Security Topology

Figure 5 shows the process of assigning an IP address to PC0 by adding the IP address 192.168.1.1 using a straight cable to connect to the switch. Similarly, in PC1 and PC2, each PC is assigned different IP addresses to connect to the switch, as seen in Figures 6 and 7.

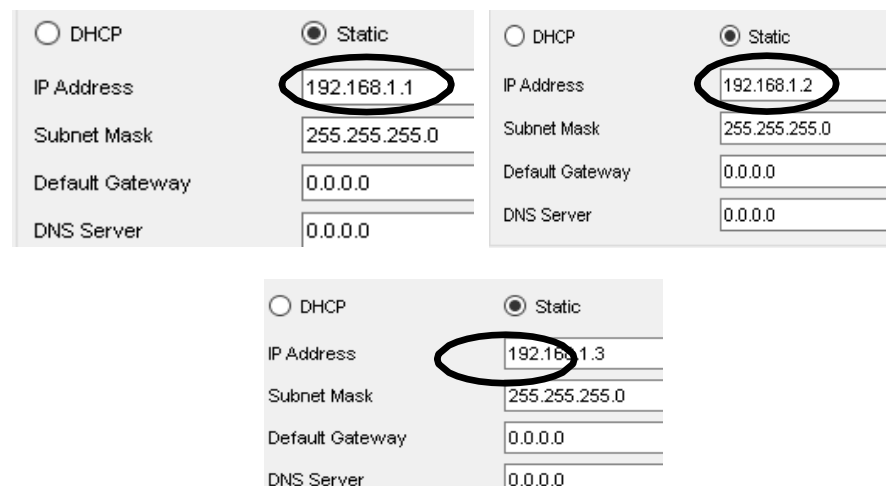


Fig.5. PC0, PC1, and PC2 IP Address

After assigning IP addresses to the PCs, the next step is configuring the ports on the switch to apply different security settings according to the created topology. Configure fa0/1 with Static mode and restrict security mode using the MAC address of PC0, which is 00E0.F742.0391, as shown in Figure 8. When this port is configured with these settings,

the device packets will not be stopped but will be logged, and they will not be allowed to enter the network.

```
Switch(config)#int fa0/1
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0000.R742.0391
Switch(config-if)#switch port-security violation restrict
```

Fig.6. Configuration of Restrict violation mode on fa0/1

```
Switch#show port-security interface fa0/1
Port Security : Enabled
Port Status : Secure up
Violation Mode : Restrict
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Fig.7. Result of configuring Restrict violation mode on fa0/1

Port fa0/2 is set to Sticky mode with Protect security, as seen in Figure 8. If this port is configured, packets from the device will be blocked and unable to connect.

```
Switch#show port-security interface fa0/2
Port Security : Enabled
Port Status : Secure up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Fig.8. Result of configuration with Protect violation mode on fa0/2

Fa0/3 is configured with Sticky mode and Shutdown security, as shown in Figure 9. With this configuration, the port will be immediately shut down, and the device or equipment cannot connect automatically.

```
Switch(config)#int fa0/3
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-address 0006.2A25.B953
Switch(config-if)#switch port-security violation shutdown
```

Fig.9. Configuration of Shutdown violation mode on fa0/3

```

Switch#show port-security interface fa0/3
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

```

Fig.10. Result of configuration with Shutdown violation mode on fa0/3

Moreover, to check each port, we can look at the overall configuration of each Switch port. When port security policy is violated, what action will be taken? Figure 11 shows whether the port will be disabled or given a warning.

```

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
Fa0/1    1          1          0          Restrict
Fa0/2    1          1          0          Protect
Fa0/3    2          1          0          Shutdown

```

Fig.11. shows the view of port security.

The VLAN (Virtual Local Area Network) ID is associated with MAC addresses. VLAN is used to separate network traffic within a single physical switch logically. MAC address refers to the list of MAC addresses learned by the switch. This includes the MAC addresses of devices connected to the switch through specific ports. The port type associated with the MAC address can be an access or trunk port. This helps track network traffic flow, identify MAC addresses connected to specific ports, and ensure that invalid or unwanted MAC addresses do not enter the network. In Figure 15, we can see the registered MAC addresses.

```

Switch#show mac-address-table
                Mac Address Table
-----

```

Vlan	Mac Address	Type	Ports
1	0006.2a25.b953	STATIC	Fa0/3
1	0050.0fbe.019d	STATIC	Fa0/2
1	00e0.f742.0391	STATIC	Fa0/1

Fig.12. Displays the view of MAC addresses.

This test pings all PCs where the expected result is "Reply" or "Connected." The test is conducted three times. In Figure 16, the first test is from PC0 to PC1, where when we ping, the expected result is a reply or connection. The same request is also tested with other IP addresses, such as from PC1 to PC2, where the expected result is also a reply.

```

Packet Tracer PC Command Line 1.0
C: >ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Fig.13. Ping on PC0

When PC0/PC1/PC2 switch ports are changed, those PCs will not be connected to other PCs. Similarly, if other PCs are connected to the switch, they will also not be connected. This is because the ports will detect unknown MAC addresses, or the maximum number of MAC addresses is limited. The test is conducted three times. In Figure 14, the first test is from PC0 to PC1, where when we ping, the result is "request timed out." The same request is also tested with other IP addresses, such as from PC2 to PC3, where the result is also "request timed out."

```

Packet Tracer PC Command Line 1.0
C: >ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Fig.14. Ping on PC0

5. CONCLUSION

Based on the experimental implementation using Cisco Packet Tracer simulation, it can be concluded that a Default/static port security is used for blocking one specific port. Regarding security capabilities, it is considered minimal because static port security can only register one MAC address. Port security dynamic learning can learn MAC addresses up to 132 MAC addresses. However, it has a drawback on the network administrator's side, as it can be challenging to register the MAC addresses allowed to use the network. Sticky port security is highly efficient because it can learn and register MAC addresses dynamically.

6. ACKNOWLEDGMENTS

Thanks are given to organizations or institutions that assist in research, directly or indirectly, in thinking and funding.

AUTHOR CONTRIBUTIONS

All Author is responsible for building Conceptualization, Methodology, analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision of project administration, funding acquisition, and have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. N. Ishak, S. Hamza, and M. Hamid, "Analisis Keamanan Jaringan Menggunakan Switch Port Security Padawarnet Gramit Kelurahan Sasa Ternate Selatan," vol. 7, no. 1, pp. 611–618, 2023.
2. J. Guan, Y. Zhang, S. Yao, and L. Wang, "AID shuffling mechanism based on group-buying auction for identifier network security," *IEEE Access*, vol. 7, no. Cid, pp. 123746–123756, 2019, doi: 10.1109/ACCESS.2019.2936043.
3. A. D. Putra, M. Thorriq, and R. Bey, "Analisis dan Implementasi Keamanan Jaringan File Transfer Protocol (FTP) Menggunakan Intrusion Prevention System (IPS) pada Mikrotik".
4. Y. C. Dara, F. Hariadi, P. Alfa, and R. Leo, "Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp-Snooping Dan Switch- Port-Security (Implementation Analysis of Network Security Systems Using the DHCP Snooping and Switch Port Security Methods)," vol. 01, no. 03, pp. 187–196, 2022.
5. Y. Yang, C. Yao, J. Yang, and K. Yin, "A Network Security Situation Element Extraction Method Based on Conditional Generative Adversarial Network and Transformer," *IEEE Access*, vol. 10, no. September, pp. 107416–107430, 2022, doi: 10.1109/ACCESS.2022.3212751.
6. A. D. Maneka, L. Lapu, and K. Marak, "AnalisisKeamananJaringan Local Area Network PerpustakaanUniversitas Kristen WiraWencana SumbaMenggunakan DHCP server Berbasic Cisco," vol. 2, no. 1.
7. F. Liu, W. Huo, Y. Han, S. Yang, and X. Li, "Study on Network Security Based on PCA and BP Neural Network under Green Communication," *IEEE Access*, vol. 8, pp. 53733–53749, 2020, doi: 10.1109/ACCESS.2020.2981490.
8. K. NUGROHO and D. P. SETYANUGROHO, "Analisis Kinerja RouteFlow pada Jaringan SDN (Software Defined Network) menggunakan Topologi Full-Mesh," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 7, no. 3, p. 585, 2019, doi: 10.26760/elkomika.v7i3.585.
9. Sonny Rumalutur, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong Sonny Rumalutur," *Tek. Elektro*, vol. 19, no. 100, pp. 48–60, 2014.
10. S. Arlis and Sahari, "Analisis Firewall Demilitarized Zone dan Switch Port Security pada Jaringan Universitas Putra Indonesia YPTK," *J. KomtekInfo*, vol. 6, no. 1, pp. 29–29, 2019, doi: 10.35134/komtekinfo.v6i1.39.
11. H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.
12. Y. Tan, R. Gu, Y. Ji, D. Wang, and H. Li, "Adaptability Analysis for IP Switching and Optical Switching in Geographically Distributed Inter- Datacenter Networks," *IEEE Access*, vol. 6, pp. 56851–56861, 2018, doi: 10.1109/ACCESS.2018.2873621.
13. M. R. Yahya, N. Wu, Y. Gaizhen, T. Ahmed, Yasir, and J. Zhang, "An Algorithmic Framework to Construct Optical Switch via Scaling from N-to-2N Ports for Optical Network on Chip," *IEEE Access*, vol. 7, pp. 101427–101440, 2019, doi: 10.1109/ACCESS.2019.2930754.
14. N. Terzenidis et al., "End-to-End 1024-Port Optical Packet Switching with 25 Gb/s Burst-Mode Reception for Data Centers," *IEEE Photonics J.*, vol. 13, no. 3, 2021, doi: 10.1109/JPHOT.2021.3082642.
15. R. Faraji, L. D.Ing, T. Rahimi, M. Kheshti, and M. R. Islam, "Soft-Switched Three-Port DC-DC Converter with Simple Auxiliary Circuit," *IEEE Access*, vol. 9, pp. 66738–66750, 2021, doi: 10.1109/ACCESS.2021.3076183.

16. R. Mentang, A. A. E. Sinsuw, X. B. N. Najoan, and J. T. Elektro-ft, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *J. Tek. Elektro dan Komput.*, vol. 4, no. 7, pp. 35–44, 2015.
17. N. H. Ramadhan Dwi Putra, Arip Solehudin, "Penerapan Digital Security Untuk Analisis Serangan Keamanan Jaringan Voip Dengan Metode Penetration Testing," *Front. Neurosci.*, vol. 14, no. 1, pp. 1–13, 2021.
18. S. S. Zara, A. M. Elhanafi, and D. Handoko, "Pemodelan Jaringan Wan Dengan Teknologi Frame Relay Dengan Memanfaatkan Switch Port Security Sebagai Sistem Keamanan Jaringan," *Snastikom*, pp. 1–6, 2020, [Online]. Available: <http://prosiding.snastikom.com/index.php/SNASTIK OM2020/article/view/66>
19. Tommi Alfian Armawan Sandi, F. Firmansyah, S. Dewi, E. K. Pratama, and R. D. Astuti, "Comparison of Port Security Switch Layer 2 MAC Address Dynamic With MAC Address Static Sticky," *Inspir. J. Teknol. Inf. dan Komun.*, vol. 12, no. 2, pp. 65–75, 2022, doi: 10.35585/inspir.v12i2.8.
20. R. Faraji, L. Ding, T. Rahimi, H. Farzanehfard, H. Hafezi, and M. Maghsoudi, "Efficient Multi-Port Bidirectional Converter with Soft-Switching Capability for Electric Vehicle Applications," *IEEE Access*, vol. 9, pp. 107079–107094, 2021, doi: 10.1109/ACCESS.2021.3097750.