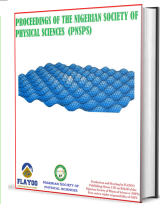
Published by Nigerian Society of Physical Sciences. Hosted by FLAYOO Publishing House LTD

Proceedings of the Nigerian Society of Physical Sciences

Journal Homepage: https://flayoophl.com/journals/index.php/pnspsc



Mitigating MAC flooding attacks using port security techniques

Shehu Ibrahim Gajo*

Department of Computer Engineering Technology, Katsina State Institute of Technology and Management, Katsina

A B S T R A C T

In today's interconnected digital landscape, network security is paramount, particularly for Local Area Networks (LANs) that are increasingly vulnerable to MAC flooding attacks. These attacks exploit vulnerabilities in network switches, compromising network integrity and privacy. This study aims to explore the effectiveness of port security mechanisms in mitigating MAC flooding threats through a practical simulation using Packet Tracer. The simulation setup includes a switch, two authorized computers, and one unauthorized computer, with a strict limit of one MAC address allowed per port. A shutdown violation is triggered whenever the switch port learns more than one MAC address, preventing MAC flooding. The findings reveal that the implementation of MAC address limiting effectively prevents the learning of additional MAC addresses, thereby safeguarding the network from potential flooding attacks. When the maximum MAC address limit is reached, the port is shutdown as set in the violation mode. This research underscores the critical importance of proactive security measures in maintaining network integrity and provides valuable insights for network administrators seeking to enhance their security protocols.

Keywords: MAC flooding attacks, Port security, Network security, MAC address limiting, Packet tracer.

DOI:10.61298/pnspsc.2025.2.162

1. INTRODUCTION

In today's digital landscape, Local Area Networks (LANs) are fundamental to organizational operations, enabling seamless communication, data sharing, and resource access. LANs are widely used in businesses, educational institutions, and government agencies. However, the security of these networks is constantly under attack from malicious actors looking to exploit vulnerabilities and gain unauthorized access to sensitive information [1].

MAC (Media Access Control) flooding attacks are one of the security threats that LAN faces by targeting network switches. MAC flooding attacks take advantage of the behaviour of the network switches, which are in charge of forwarding network traffic based on MAC addresses [2]. These attacks aim to overwhelm the switch's MAC address table, also known as a CAM (Content Addressable Memory) table, by flooding it with numerous fake or spoofed MAC addresses. When the table is full, the switch can enter either a fail-open or a fail-closed mode [3].

In fail-open mode, the switch acts like a hub, broadcasting all incoming traffic to all ports rather than forwarding it selectively based on the MAC address table. This threatens network privacy because unwanted devices can access sensitive data. In fail-closed mode, the switch becomes unresponsive and stops for-

*Corresponding Author Tel. No.: +234-703-8135-131.
e-mail: shehugajo2004@gmail.com (Shehu Ibrahim Gajo)

warding traffic until the MAC address table is cleaned. This results in a denial of service (DoS) situation, making the network inoperable.

Various methods have been explored by researchers and network administrators to mitigate this threat. Implementing port security features on network switches is one of the successful techniques. It allows network administrators to limit the number of MAC addresses per port, bind specific MAC addresses to ports, or automatically remove inactive MAC addresses from switch memory [1]. This technique is useful in organizational settings, where proper configuration is crucial to avoid potential issues.

This study aims to enhance the understanding of port security mechanisms within a simple LAN environment and assess their effectiveness in mitigating MAC flooding attacks using the Packet Tracer simulation tool. By designing a realistic network scenario, the research specifically examines the MAC address limiting mechanism, its configurations, and its impact on network security. The findings will offer valuable insights for network administrators, enabling them to strengthen security measures, maintain network integrity, and implement effective countermeasures to safeguard LAN infrastructures.

2. PORT SECURITY TECHNIQUES REVIEW

Port security is achieved through three key techniques: MAC address limiting, which restricts the number of allowed MAC addresses; MAC address sticky, which learns and bind MAC addresses; and MAC address aging, which removes inactive MAC addresses over time. Each technique offers its own advantages and considerations. Selecting the most suitable technique depends on your network's specific needs and security goals. It is recommended to assess your network's needs and constraints to determine the most suitable technique. Here is a brief comparison of these techniques [4]:

(i) MAC Address Limiting

- Advantages: Allows you to set a specific maximum limit on the number of MAC addresses per port, providing control over the number of allowed devices. It offers strong protection against MAC flooding attacks by preventing the switch from being overwhelmed with excessive MAC addresses.
- Considerations: Requires careful configuration and monitoring to ensure that the maximum limit is appropriate for the network's devices and potential growth.

(ii) MAC Address Sticky

- Advantages: Simplifies MAC address management by automatically binding MAC addresses to specific ports. It enhances network security by allowing only authorized devices with their respective MAC addresses to communicate through the associated ports.
- Considerations: Requires manual configuration or enabling sticky MAC address learning on each port. This may not be suitable for networks with frequently changing or dynamic devices.

(iii) MAC address aging

- Advantages: Automatically removes inactive MAC addresses from the switch's memory, helping to maintain an efficient MAC address table. It supports efficient resource allocation and prevents the table from being filled with unnecessary or out-dated entries.
- Considerations: Requires proper configuration of aging time to balance between removing inactive addresses and avoiding premature removal of legitimate devices. It may not provide direct protection against MAC flooding attacks but helps optimize MAC address table utilization.

Compared to sticky MAC addressing and MAC address aging, setting a limit on the number of MAC addresses allowed on a port is a more direct approach to preventing MAC flooding attacks because it prevents the switch from learning an excessive number of MAC addresses.

The research by Ref. [5] analysed the effectiveness of port security mechanisms in defending against MAC flooding attacks. They found that configuring MAC address limiting on switch ports significantly reduced the impact of such attacks by restricting the number of MAC addresses that can be learned on each port. (Sandi et al., 2022) demonstrated the benefits of MAC address limiting in restricting the impact of flooding attacks. It was demonstrated in Ref. [6] that by allowing network administrators to specify a maximum limit on the number of MAC addresses allowed per port, MAC address limiting provides a proactive approach to network security. This preventative approach decreases the possibility of MAC flooding attacks overwhelming the switch's MAC address table, and preventing unwanted access to network resources.

Furthermore, a comparative analysis conducted by Ref. [7] evaluated the effectiveness of different port security techniques in defending against MAC flooding attacks. The research demonstrated that limiting MAC addresses was highly effective in preventing MAC address flooding on the switch. This resulted in a more resilient network and reduced security vulnerabilities.

These findings are consistent with the recommendations provided by networking experts, Cisco Systems [8], who emphasize the significance of MAC address limiting as a robust defence mechanism against MAC flooding attacks. By establishing a predetermined maximum limit on MAC addresses per port, network administrators can exercise precise control over the number of connected devices, ensuring the network remains secure and accessible.

Based on the above studies, MAC address limiting emerges as the preferred port security technique due to its effectiveness in preventing MAC flooding attacks, preserving network segmentation, and offering good control over device connectivity [5]. Table 1 outline the pros and cons of the three key port security techniques.

Each technique offers unique advantages and potential drawbacks, and a combination of these techniques is often the best approach for securing network ports effectively. For example, using MAC address limiting in conjunction with MAC address sticky can offer a comprehensive approach to controlling the number of devices and ensuring only authorized devices are connected. Although, the best port security technique for a given

Table 1. Port security techniques comparison.

Technique	Pros	Cons
MAC Address Limiting	• Restricts the number of MAC addresses per port, preventing MAC flooding attacks. • Enhances security by ensuring only a limited number of devices can connect. • Prevents unauthorized devices from connecting.	• Requires manual configuration for optimal security. • Can block legitimate devices if the limit is too low.
MAC Address Sticky	• Automatically learns and stores MAC addresses, reducing administrative workload. • Persistent across reboots if saved in the running configuration.	• Can be a security risk if attackers gain access to the learned MAC addresses. • Requires manual clearing of old MAC addresses when devices are replaced.
MAC Address Aging	• Automatically removes inactive MAC addresses, allowing dynamic reassignment. • Helps maintain an updated list of active devices.	• If aging time is too short, legitimate devices may need to reauthenticate frequently. • Attackers can manipulate aging timers to prolong their presence in the network.

network will depend on factors such as network size, device dynamics, security requirements, and scalability considerations. It is recommended to conduct a thorough analysis of the network's needs to determine the most appropriate technique(s) for specific scenario.

3. METHODOLOGY

Configuring MAC address limiting involves enabling port security, setting a MAC address limit per interface, and defining violation responses. The following configuration details will provide a practical guide to mitigate MAC address flooding:

(i) Identify the switch port to to apply the port security by MAC address limiting.

(ii) Enter the configuration mode of the switch by using configure terminal command. This command allows access the switch's configuration settings.

(iii) Select the specific interface by using the interface command <interface_number> e.g., FastEthernet0/2. This command allows access to the configuration mode for the specified interface.

(iv) Enable port security on the interface by using the command switchport port-security. This command activates port security on the selected interface.

(v) Set the maximum number of MAC addresses allowed on the port using the command switchport port-security maximum <max_number>. Replace <max_number> with the desired maximum limit of MAC addresses for the port.

This command specifies the maximum number of MAC addresses that the switch will allow on the specified port. Any additional MAC addresses beyond this limit will be blocked, preventing MAC flooding attacks and unauthorized access.

(vi) Configure port security violation modes (restrict, shutdown, or protect) using the switchport port-security violation command. This command specifies the violation mode when a security violation occurs, such as when the maximum number of MAC addresses is exceeded. The available options are:

- Shutdown: Switch interface will be shut-down and no traffic is allowed on that interface. This option sends an SNMP trap and a syslog message, and increments a violation counter when a port security violation occurs. The "shutdown" option is the highest port security option available and the default one.
- Restrict: Switch interface drops frames with an unknown source MAC address after the switch port reaches maximum number of allowed MAC addresses. This option also sends an SNMP trap and a syslog message and increments a violation counter when a port security violation occurs.
- Protect: Switch interface drops frames with an unknown source MAC address after the switch port reaches maximum number of allowed MAC addresses. No SNMP trap and a syslog message are generated. The "protect" option is the lowest port security option available.

(vii) Exit the interface configuration mode by using the command exit.

(viii) Save the configuration changes by using the command write.

By following these steps and configuring the MAC address limiting feature on the desired switch port, you can effectively restrict the number of MAC addresses allowed on the port and enhance the security of your network against MAC flooding attacks.

In this research, the following commands are used in the switch ports configurations and Figure 1 shows the network topology setup.

Switch0#**configure terminal**
Switch0(config)#**interface fastethernet0/2**
Switch0(config-if)#**switchport mode access**
Switch0(config-if)#**switchport port-security**
Switch0(config-if)#**switchport port-security maximum 1**
Switch0(config-if)#**switchport port-security violation shutdown**
Switch0(config-if)#**exit**
Switch0(config)#**exit**
Switch0#

4. RESULTS AND DISCUSSION

The configuration of MAC address limiting on the selected switch port was successfully implemented following the outlined steps. This section discusses the observed results and their implications in terms of network security and mitigating MAC flooding attacks.

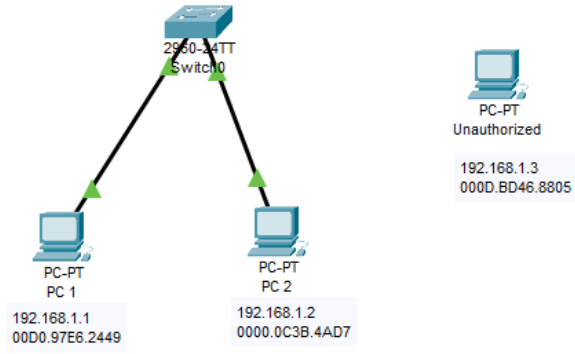


Figure 1. Network topology setup for port-security settings.

4.1. CONNECTIVITY TEST BEFORE SECURITY VIOLATION

The ping test results for the IP address 192.168.1.2 indicate a successful network connection. The four ping requests sent to the destination IP address received a reply without any packet loss. These results prove a reliable and efficient network connection between the source device and the destination device. The ping results are as follows:

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)**.

4.2. PORT SECURITY BEFORE SECURITY VIOLATION

During the testing phase, several scenarios were conducted to assess the impact of MAC address limiting. These scenarios involved connecting various devices to the configured switch port, attempting to exceed the defined MAC address limit, and monitoring the behaviour of the switch and network performance.

Switch0#show port-security interface fa0/2 command is used to display the following results.

Port Security: **Enabled**

Port Status: **Secure-up**

Violation Mode: **Shutdown**

Maximum MAC Addresses: **1**

Total MAC Addresses: **1**

Last Source Address: **0000.0C3B.4AD7**

Security Violation Count: **0**

The conducted port security test showed that the port security feature was enabled, ensuring a secure environment for the network. The port was in a secure-up state with a shutdown violation mode, allowing normal operation while promptly shutting down in case of security violations. The maximum allowed MAC address was set to 1. No security violations were detected during the test.

4.3. PORT SECURITY AFTER SECURITY VIOLATION

To test the port security violation effectiveness, PC2 with IP address 192.168.1.2 is removed from the configured port (fastethernet0/2) and connect the unauthorized computer, in this case with an IP address of 192.168.1.3 and MAC address of 000D.BD46.8805.

Port Security: **Enabled**

Port Status: **Secure-shutdown**

Violation Mode: **Shutdown**

Maximum MAC Addresses: **1**

Total MAC Addresses: **1**

Last Source Address: **000D.BD46.8805**

Security Violation Count: **1**

The successful implementation of port security is evident in the observed configuration, where the port is set to "Secure-shutdown" mode. The increment of a security violation count proved that a violation has occurred, and the port has appropriately shutdown to prevent unauthorized access.

4.4. CONNECTIVITY TEST AFTER SECURITY VIOLATION

Ping result from PC1 to unauthorized PC3 shows a total shutdown and disconnections.

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 **(100% loss)**.

The ping results indicate a complete loss of connectivity with the IP address 192.168.1.3. This outcome is due to the successful implementation of port security measures. The port security configuration is effectively preventing any communication with the IP address in question. As a result, all ping requests to 192.168.1.3 are timing out, indicating a 100% packet loss. This outcome demonstrates the effectiveness of the port security implementation in maintaining network integrity and protecting against unauthorized access.

Table 2. Result comparison.

Before Security Violation	After Security Violation
Port Security: **Enabled**	Port Security: **Enabled**
Port Status: **Secure-up**	Port Status: **Secure-shutdown**
Violation Mode: **Shutdown**	Violation Mode: **Shutdown**
Maximum MAC Addresses: **1**	Maximum MAC Addresses: **1**
Total MAC Addresses: **1**	Total MAC Addresses: **1**
Last S/Address: **0000.0C3B.4AD7**	Last S/Address: **000D.BD46.8805**
Security Violation Count: **0**	Security Violation Count: **1**

4.5. SUMMARY OF RESULTS

Switch0#show port-security interface fa0/2 command displays detailed port security information for FastEthernet 0/2 (fa0/2). The comparison results before and after violation is stated in Table 2.

When the number of connected devices reached the maximum limit, the switch successfully blocked any additional MAC addresses from being learned on the port. This behaviour validates the effectiveness of MAC address limiting in preventing MAC flooding attacks. Furthermore, the configured shutdown violation mode played a crucial role in handling security violations when the maximum MAC address limit was exceeded. Once the violation threshold is reached, the switch automatically shutdown the port by placing it into an **err-disabled (error-disabled)** state. This action prevents further communication through the compromised port. The port can be recovered by manually re-enable the port by executing the command: no shutdown after entering interface configuration mode or automatic recovery using the command: errdisable recovery cause psecure-violation.

Despite its effectiveness, the MAC address limiting technique presents certain limitations that must be acknowledged:

(i) MAC address limiting is not a comprehensive security measure, as it primarily mitigates MAC flooding attacks. However, it does not address more sophisticated attack vectors, particularly those targeting higher layers of the OSI model, such as ARP spoofing, man-in-the-middle (MITM) attacks, or application-layer exploits. As a result, reliance on MAC address limiting alone may leave networks vulnerable to multifaceted cyber threats.

(ii) The findings presented in this study are based on simulated network environments, which may not fully capture the complexities and dynamic nature of real-world network infrastructures. Factors such as diverse traffic patterns, varying attack methodologies, and hardware-specific behaviors could influence the practical effectiveness of MAC address limiting. Therefore, further research in live, operational networks is necessary to comprehensively evaluate its robustness and adaptability in real-world scenarios.

5. CONCLUSION

The primary goal of this paper is to mitigate MAC flooding attacks by limiting the number of MAC addresses that can be learned on a given port. A switch port is configured to allow one

maximum number of secure MAC addresses. This limit is set to prevent the switch from learning an excessive number of MAC addresses, which can indicate malicious activity or unauthorized devices. Upon enabling MAC address limiting and setting a maximum number of MAC addresses allowed on the port, the switch effectively restricted the number of MAC address that could be learned on that specific interface. Any attempts to exceed the configured limit were prevented, thereby mitigating the risk of MAC flooding attacks. This measure enhances network security by ensuring that the switch's MAC address table does not become overwhelmed with excessive MAC addresses. By implementing MAC address limiting, organizations can enhance the security posture of their networks and safeguard against MAC flooding threats effectively. It is important to note that the effectiveness of MAC address limiting may vary depending on the specific network environment and the network's size and dynamics. Network administrators should consider factors such as the number of authorized devices, future scalability requirements, and potential device mobility when configuring the maximum MAC address limit. Exploring emerging technologies such as machine learning for predictive analysis and proactive security measures could further strengthen MAC address limiting mechanisms, enabling organizations to stay ahead of evolving threats in an increasingly complex cybersecurity landscape.

DATA AVAILABILITY

The data will be available on request from the corresponding author.

References

[1] M. Sandhya, "Empirical investigations on the security and threat mitigation of campus switches", 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India: IEEE, Jan. 2023, pp. 1–8. [Online]. http://dx.doi.org/10.1109/ICCCI56745.2023.10128280.

[2] Y. Tzang, H. Chang & C. Tzang, "Enhancing the performance and security against media-access-control table overflow vulnerability attacks", Security Comm. Networks **8** (2015) 1780 https://doi.org/10.1002/sec.1142.

[3] A. ElShafee & W. El-Shafai, "Design and analysis of data link impersonation attack for wired LAN application layer services", J Ambient Intell Human Comput **14** (2023) 13465. https://doi.org/10.1007/s12652-022-03800-5.

[4] CISCO press, "Cisco networking academy's introduction to basic switching concepts and configuration", in *Routing and switching essentials companion guide*, Cisco Press, 2014. [Online]. https://www.ciscopress.com/articles/article.asp?p=2181836&seqNum=7.

[5] T. A. A. Sandi, F. Firmansyah, S. Dewi, E. K. Pratama & R. D. Astuti, "Comparison of port security switch layer 2 mac address dynamic with mac address static sticky", J. inspir. **12** (2022) 65. https://doi.org/10.35585/inspir.v12i2.8.

[6] N. Juniper, "Configuring MAC limiting". [Online]. Accessed: Jul. 08, 2023. https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/topic-map/configuring-mac-limiting.html.

[7] F. Semperboni, "Protecting against MAC flooding attack", CiscoZine. [Online]. Accessed: Jul. 08, 2023. https://www.ciscozine.com/protecting-against-mac-flooding-attack/.

[8] Cisco, "MAC address limiting on service instances and bridge domains". [Online]. Accessed: Feb. 01, 2025. https://www.cisco.com/c/en/us/td/docs/ios/cether/configuration/guide/ce_mac-addlmt-bdsin.html.