DHCP Snooping ve Port Güvenliği Kullanılarak MITM Saldırılarına Karşı Switch Güvenliğinin İyileştirilmesi[1]

***

Improving Switch Security Against MITM Attacks Using DHCP Snooping and Port Security

DOI:10.33461/uybisbbd.1766477

Bashar ALHAJAHMAD[2]

Makale Bilgileri

Makale Türü: Araştırma Makalesi

Geliş Tarihi: 16.08.2025

Kabul Tarihi: 04.10.2025

Öz

Bu çalışma, Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) üzerindeki güvenlik açıklarını incelemekte ve saldırganların güvenilir portları kötüye kullanması durumunda DHCP Snooping tekniğinin sınırlılıklarına odaklanmaktadır. DHCP sahtekarlığı (spoofing) saldırılarını tespit ve engellemek amacıyla, DHCP Snooping ile Port Security'nin entegre edildiği geliştirilmiş bir yöntem önerilmektedir. Yazılım Tanımlı Ağ (SDN) veya makine öğrenmesi tabanlı çözümler ileri düzey altyapı gerektirirken, önerilen yöntem hafif, düşük maliyetli ve işletme ile eğitim ağlarında yaygın olarak kullanılan geleneksel Katman 2 anahtarlarında uygulanabilir niteliktedir. DHCP Snooping, anahtar portlarını güvenilir veya güvenilir olmayan olarak sınıflandıracak şekilde yapılandırılmış, Port Security ise MAC adresi doğrulamasına dayalı erişim kısıtlaması getirmiştir. Bu entegrasyon, özellikle geleneksel DHCP Snooping'in yetersiz kaldığı güvenilir portlar üzerinden gerçekleştirilen saldırıları etkili bir şekilde engellemiştir. Simülasyon sonuçları, DHCP Snooping ile Port Security'nin birlikte kullanımının, port düzeyinde MAC tabanlı kimlik doğrulama sağlayarak ağ güvenliğini önemli ölçüde güçlendirdiğini göstermektedir. Yöntem, yalnızca yetkili DHCP sunucularının istemci taleplerine yanıt vermesini garanti etmekte, güvenilir portların istismarını önlemekte ve ağ performansında herhangi bir düşüşe yol açmamaktadır. Bulgular, ek donanım veya karmaşık algılama sistemlerine gerek duymadan ağ bütünlüğünü artırmada yöntemin etkinliğini ve uygulanabilirliğini ortaya koymaktadır.

Anahtar Kelimeler: *MITM, DHCP Denetimi, Port Güvenliği, DHCP Sahteciliği, Ağ Güvenliği.*

Article Info

Paper Type: Research Paper

Received: 16.08.2025

Accepted: 04.10.2025

Abstract

This study investigates security vulnerabilities in the Dynamic Host Configuration Protocol (DHCP), focusing on the limitations of DHCP Snooping when attackers exploit trusted ports. We propose an enhanced detection and prevention mechanism that integrates DHCP Snooping with Port Security to counter DHCP spoofing attacks. Unlike approaches based on Software-Defined Networking (SDN) or machine learning which require advanced infrastructure our method is lightweight, cost-effective, and deployable on conventional Layer 2 switches commonly used in enterprise and educational networks. DHCP Snooping was configured to classify switch ports as trusted or untrusted, while Port Security restricted access through MAC address verification. This integration effectively mitigated DHCP spoofing attempts, including those launched through trusted ports, where traditional DHCP Snooping alone is insufficient. Simulation results show that combining DHCP Snooping with Port Security significantly strengthens network security by enforcing MAC-based authentication at the switch port level. The method ensures that only legitimate DHCP servers can respond to client requests, prevents the exploitation of trusted ports, and maintains network performance without introducing instability. The findings demonstrate the practicality and effectiveness of the proposed approach in enhancing network integrity without additional hardware or complex detection systems.

Keywords: *MITM, DHCP Snooping, Port Security, DHCP Spoofing, Network Security.*

Atıf/ to Cite (APA): Alhajahmad B. (2025). Improving Switch Security Against MITM Attacks Using DHCP Snooping and Port Security. International Journal of Management Information Systems and Computer Science, 9(2), 157-174. DOI: 10.33461/uybisbbd.1766477

[1] This study was presented as an oral presentation at the 11th International Computer and Instructional Technologies Symposium, held on May 24–26, 2017.

[2] Department of Computer Engineering, Faculty of Engineering, Siirt University, bashar.ahmad@siirt.edu.tr, Siirt, Türkiye.

1. INTRODUCTION

The Dynamic Host Configuration Protocol (DHCP) streamlines the acquisition of network configuration parameters, including IP addresses, from a designated DHCP server (Droms, 1997a). Unlike the manual management of IP addresses, which is labor-intensive and time-consuming in large-scale networks, DHCP automates this process by dynamically assigning IP addresses in response to host requests (Ahmad et al., 2021). This process hinges on robust communication between the client and the DHCP server within the network. In this interaction, the client operates as the "blind" party, lacking knowledge of network device addresses or the DHCP server's identity. During the discovery phase, the client initiates communication by sending a DHCP Discover message and subsequently receives IP configuration offers (DHCP Offers) from the server in response (Yan et al., 2016).

To counteract attacks targeting DHCP servers, particularly those involving rogue DHCP servers, various measures have been developed. One effective strategy is the activation of DHCP Snooping, which implements an authentication filter against unauthorized DHCP servers (Pradana & Budiman, 2021). This method can be further reinforced through the utilization of the DHCP Snooping Trusted Port technique within the network (Miftah, 2018).

Despite its effectiveness, DHCP Snooping is vulnerable to certain security flaws. One significant issue is the assumption that ports connected to DHCP servers are secure, leading to the acceptance of all DHCP ACK packets from these ports as legitimate. If an attacker gains access to a secured port, they can exploit this vulnerability to send DHCP ACK packets to clients, assigning false IP addresses and potentially intercepting their data undetected.

This research makes significant contributions by enhancing the DHCP Snooping process through the integration of Port Security techniques. Typically, once a switch port is secured, only DHCP ACK packets from the main DHCP server are expected to traverse through it. However, if a malicious attacker connects a rogue device to this ostensibly secure port, detecting such activity becomes challenging. This research illuminates an approach to address this vulnerability by integrating Port Security techniques with the DHCP Snooping process. The findings demonstrate an improved security posture for network infrastructures, particularly in mitigating sophisticated DHCP spoofing attacks.

While prior research has explored DHCP spoofing detection using SDN controllers, machine learning algorithms, and advanced inspection tools, these methods often require substantial infrastructure or complex configurations. In contrast, this study makes a novel contribution by leveraging existing switch-level features—DHCP Snooping and Port Security—within traditional Layer 2 environments. Our method addresses a specific weakness in current DHCP Snooping implementations by introducing MAC address-based filtering at the port level, offering a deployable, low-cost solution for enhanced security. This research aims to fill the gap between highly advanced frameworks and the practical needs of everyday enterprise or campus networks.

2. BACKGROUND

2.1. Dynamıc Host Confıguratıon Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) serves as a network management protocol designed to seamlessly assign IP addresses and essential network configuration parameters such as subnet mask, default gateway, and lease time to clients within a network automatically (Tripathi & Hubballi, 2018). The process of binding an IP address follows a structured protocol known as D.O.R.A, consisting of four essential steps detailed below (Droms, 1997b):

- **DHCP DISCOVER**: Initiated by the DHCP client, this step involves broadcasting a message across the network to locate a DHCP server capable of providing an IP address.
- **DHCP OFFER**: Triggered by the DHCP server upon receiving a DHCP discover message, this phase involves sending a unicast message back to the client, indicating the availability of the DHCP server and offering an IP address.
- **DHCP REQUEST**: Generated by the client, this broadcast message is a formal request to the DHCP server to allocate the offered IP address.
- **DHCP ACKNOWLEDGMENT**: In this final step, the DHCP server sends an acknowledgment message directly to the DHCP client, confirming the successful assignment of the requested IP address to the legitimate host.

Figure 1 illustrates the dynamic process of assigning binding information to a DHCP client:

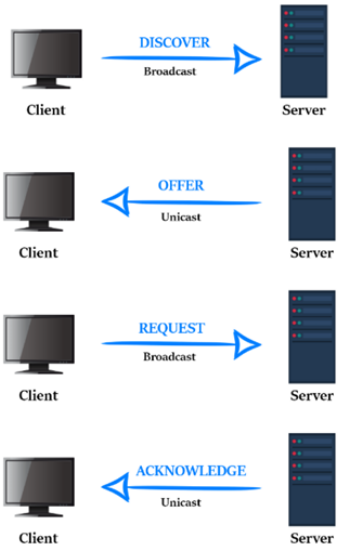

Figure 1. DHCP Process Operations (Mehran, 2022)

2.2 MITM Attack

A Man-in-the-Middle (MITM) attack is a form of unauthorized access where an attacker covertly intercepts and monitors unencrypted data exchanged between network devices and targeted computers. Operating at the Data Link layer of the OSI model, MITM attacks grant the attacker control over the traffic flow once successfully executed (Aldaoud et al., 2021; Kalkancı et al., 2019). Spoofing-based Man-in-the-Middle (MITM) attacks are among the most prevalent in cybersecurity. These encompass four primary types: ARP spoofing, DHCP spoofing, DNS spoofing, and IP spoofing (Bhushan et al., 2017).

2.3 DHCP Attacks

Rogue DHCP servers are frequently exploited by attackers to facilitate various network assaults, including Man-in-the-Middle, Sniffing, and Reconnaissance attacks. By deploying a rogue DHCP server within a network, attackers can furnish clients with falsified addresses and network configuration details.

Another form of assault targeting DHCP servers is known as a DHCP starvation attack. In this scenario, attackers inundate the network with a high volume of DHCP REQUEST messages, each containing spoofed source MAC addresses. If the legitimate DHCP server responds to these spurious requests, it rapidly depletes the available IP addresses within its scope. Subsequently, attackers can establish a rogue DHCP server and respond to new DHCP requests from network clients. Following a DHCP starvation attack and the deployment of a rogue DHCP server, the attacker gains the ability

to allocate IP addresses and manipulate TCP/IP configuration settings for network DHCP clients. These settings, which encompass crucial parameters like the Default Gateway and DNS Server IP addresses, can be tampered with by the attacker. By substituting the original legitimate Default Gateway and DNS Server IP addresses with their own, the attacker redirects network traffic to their designated system. As a consequence of this alteration, network clients inadvertently direct outbound traffic to the attacker's computer instead of the intended destinations. This maneuver allows the attacker to intercept sensitive user data and initiate a Man-in-the-Middle attack—a tactic known as DHCP spoofing. Additionally, the attacker may further exploit the compromised network by setting up a rogue DNS server, redirecting end-user traffic to counterfeit websites, thereby facilitating phishing attacks (Alsaadi & Abdul-Zahra, n.d.).

In Figure 2, we observe a network example where the client obtains its IP configuration from the DHCP server. This configuration is then utilized by the client to establish connectivity with the remote network.

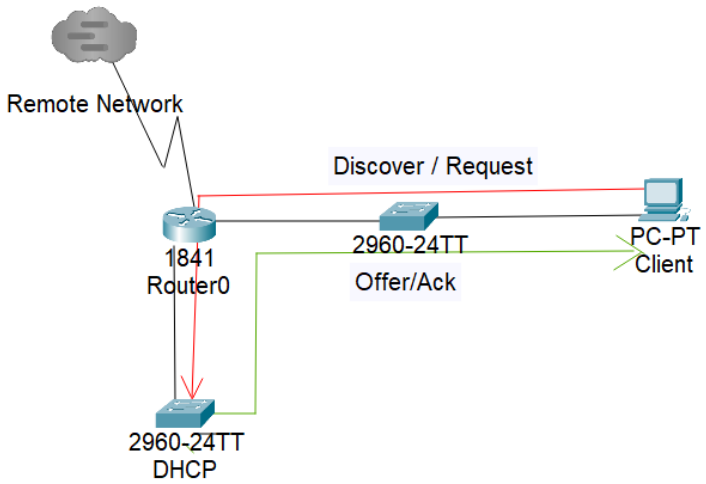

Figure 2. Acquiring IP Address Through DHCP Server

In Figure 3, we see the identical network scenario, with the distinction that the client now obtains its IP configuration from the attacker's DHCP server.

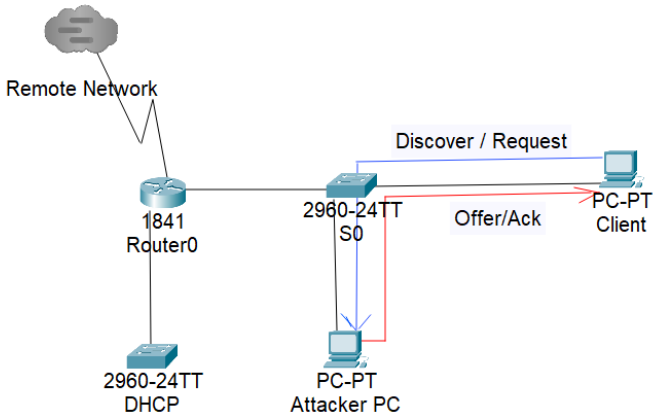

Figure 3. Performing DHCP Spoofing Using Attacker's PC

2.4 DHCP Snooping

DHCP Snooping serves as a vital security measure against DHCP attacks by categorizing ports as either 'trusted' or 'untrusted'. The port linked to the DHCP server is designated as 'trusted', while

the one connected to the DHCP client is labeled 'untrusted'. If a message intended to originate from the DHCP server, such as DHCPOFFER or DHCP ACK, arrives at an 'untrusted' port, it is immediately discarded. Consequently, ports not associated with the DHCP server are consistently configured as 'untrusted'.

Moreover, DHCP snooping offers additional protection by regulating the rate of DHCP traffic at the port level and dropping traffic in case of a MAC address mismatch between the Ethernet header and the 'chaddr' field of the DHCP message. These measures effectively combat DHCP flooding, DHCP starvation, and DHCP spoofing attacks. By controlling traffic rates and ensuring MAC address consistency, DHCP flooding and DHCP starvation attacks are mitigated, while the segregation of ports into trusted and untrusted categories acts as a barrier against DHCP spoofing (Syed et al., 2022).

The images shown in figure 4 and figüre 5 illustrate the functioning of DHCP snooping, depicting how it selectively permits or blocks DHCP messages:

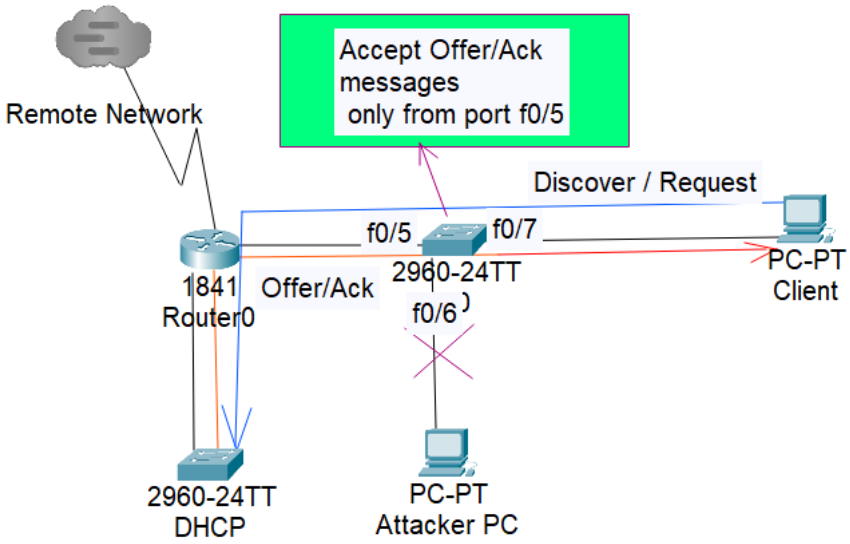

Figure 4. Mitigating DHCP Spoofing Through DHCP Snooping Protocol

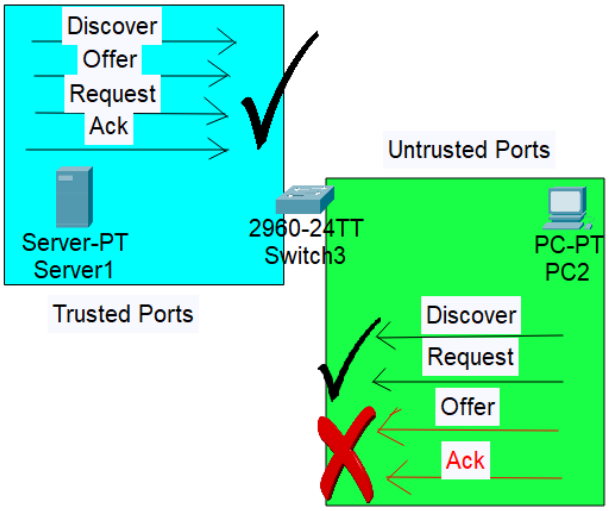

Figure 5. Trusted and Untrusted Ports in Snooping Process

2.5 Port Securıty

Cisco's implementation of port security serves as a stringent control applied directly to one or more edge interfaces (Cisco Systems, 2007a). Originally designed to counter Content Addressable

Memory (CAM) overflow attacks, port security is now recommended for mitigating MAC address spoofing attacks. This feature restricts input to an interface by comparing source MAC addresses against learned or configured MAC addresses in the switch's address table (Cisco Systems, 2007b).

When port security is activated on an interface, the switch designates that interface as secure and associates it with secure MAC addresses, thereby altering the typical learning process. This secure learning mechanism creates a (usually non-aging) 1-M (interface-MAC relationship) secure entry, where M represents the maximum number of secure MAC addresses allowed. In the address table, secure MAC address entries take precedence over non-secure entries (Buhr et al., 2011).

If a port is restricted to a single instance of authorized MAC addresses, only one device will be able to connect to the port and utilize its full bandwidth. A security breach occurs when a device with a different MAC address attempts to connect to the port after the maximum number of protected MAC addresses has been reached. In response to detecting such a breach, the switch automatically shuts down the port. The switch can be configured to either protect or restrict access to the port to enhance security measures (Sandhya, 2023). We need to specify the action to be taken in the event of a security violation. Three possible modes are available: Protect, Restrict and Shutdown.

3. LITERATURE REVIEW

In a recent paper, the authors proposed a technique to mitigate Address Resolution Protocol (ARP) spoofing-based Secure Socket Layer (SSL) stripping in a Local Area Network (LAN) by employing both Dynamic Host Configuration Protocol (DHCP) snooping and ARP inspection techniques. This mitigation strategy comprises both detection and prevention modules. The detection module utilizes an analytical tool and an algorithm designed to capture and analyze ARP packets (Adjei et al., 2021).

In another study, the authors investigated the security of the DHCP service provided by Software-Defined Networking (SDN) controllers, aiming to prevent DHCP starvation attacks targeting the SDN controller. They designed and implemented a DHCP security module, DHCPguard, on the POX controller. This module utilizes DHCP snooping, rate limiting, and IP pool recovery functions. The findings demonstrate that DHCPguard effectively blocks malicious DHCP messages, recovers the IP address pool, and mitigates the negative impacts of DHCP-related attacks on the network without incurring significant overhead (Tok & Demirci, 2021).

Another paper provides a comprehensive analysis of DHCP vulnerabilities, explaining how DHCP operates and summarizing various DHCP attacks. The paper details how these attacks occur and compromise network security. The authors propose and implement several effective countermeasures against DHCP attacks, successfully mitigating their impact and enhancing network security (Ali & Shareef, 2021).

A different paper summarizes various potential Layer 2 attacks with a focus on security issues at this layer. The paper covers examples such as VLAN hopping, MAC flooding, and DHCP attacks, highlighting the security vulnerabilities resulting from insufficient Layer 2 hardening. Additionally, it discusses how these vulnerabilities increase the susceptibility of a Local Area Network (LAN) to attacks. The paper also demonstrates efficient switch configuration techniques to mitigate these attacks (Banitalebi Dehkordi et al., 2021).

In another study, researchers propose a machine learning-driven framework for detecting MQTT (Message Queuing Telemetry Transport) Denial of Service (DoS) attacks within IoT platforms. Their approach relies on a custom-designed DoS attack model. They develop an attack detection testbed specifically designed to capture both normal and malicious traffic, with a focus on statistical flow features derived from traffic counts. To evaluate the effectiveness of their proposed feature set, the researchers validate it using three distinct machine learning algorithms: Attribute-

Oriented Data Evaluation (AODE) employing Naive Bayes, C4.5 utilizing Decision Trees, and Multilayer Perceptron (MLP) based on Artificial Neural Networks (Syed et al., 2020).

Using the Python Programming Language, a recent study illuminated the simplicity of executing DHCP attacks through scripts and outlined methods for their detection within network environments. To emulate real network infrastructures, the research leveraged Python, Scapy, and GNS3 to explore the ramifications of DHCP flooding and Rogue DHCP. The paper introduces a novel approach for identifying DHCP Starvation attacks in any network, utilizing the Offer packet inherent to the DHCP protocol (Shrestha & Sherpa, 2023).

In a different article, authors put forth a holistic multi-stage strategy for identifying and mitigating DHCP attacks within a Software-Defined Networking (SDN) framework, dubbed "DHCPWatcher." These attacks have repercussions spanning the SDN network, controller, DHCP service, and clients. The study's findings revealed that DHCPWatcher exhibits superior performance when integrated with external DHCP servers, particularly in terms of the speed at which it detects and neutralizes attacks (Aldaoud et al., 2023).

In another study, authors proposed DHCP Snooping to enhance network security. DHCP, being a target for attacks, faces threats like DHCP Rogue attacks, where hackers create fake DHCP servers to distribute IPs. DHCP Snooping addresses such vulnerabilities by distinguishing Trusted and Untrusted Ports, enhancing data security. Results show DHCP Snooping prevents clients from obtaining IPs from rogue DHCP servers, safeguarding network integrity (Purnomo, 2024).

In different study, the authors developed HybridDAD, a framework aimed at detecting various DDoS attacks, including TCP, UDP, ICMP, and DHCP flooding attacks. By harnessing emerging programmable switches, HybridDAD extracts relevant features from network traffic and employs ML algorithms to distinguish between benign and malicious traffic. The paper outlines key IP traffic features associated with these DDoS attacks and introduces a two-step attack classification approach for early detection. Despite handling multiple attack types concurrently, the ML models consistently achieved high performance, with accuracy, F1 score, precision, and recall metrics exceeding 90% in most cases (Roshani & Nobakht, 2022).

4. METHODOLOGY

This research specifically targets DHCP spoofing attacks, presenting an improved approach for their detection and prevention. Our proposed method aims to address the limitations of DHCP Snooping by integrating it with port security techniques, thereby enhancing protection against these threats. To validate our approach, we simulated network topologies using the Packet Tracer simulation tool, providing a clear demonstration of our methodology.

4.1. Network Topology

We employed Packet Tracer simulation software to establish the necessary connections between various devices and servers within our network. This software allowed us to evaluate the system's functionality and provided a visual representation, offering a comprehensive perspective of the proposed system (Madakam et al., 2015). Additionally, Packet Tracer supports a wide range of networking protocols and accommodates both logical and physical workplace environments. Its seamless integration of real-time and simulation modes enhances its versatility and practicality. Packet Tracer enables researchers to easily construct their own network topologies, offering detailed visualizations of procedures and processes. It allows users, including students, to intuitively drag, place, and connect all required devices, facilitating hands-on learning experiences (Adesemowo & Gerber, 2014). For this study, we created the network topology illustrated in Figure 6, which includes 2 PCs, a router, a DHCP server, and a DHCP attacker server.

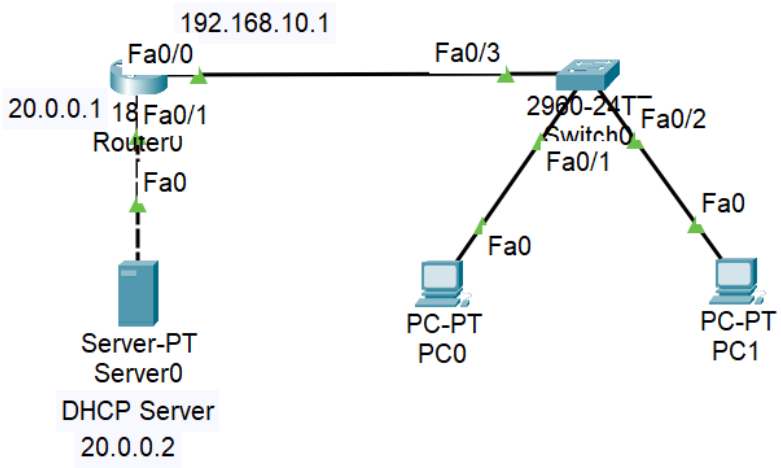

Figure 6. Proposed Network Topology

The router and DHCP setup were configured as follows:

- The Fa0/0 interface of Router 0 was assigned the IP address 192.168.10.1/24, serving as the default gateway for all devices within the network.
- Router 0's Fa0/1 interface was assigned the IP address 20.0.0.1/8.
- Fa0/0 interface of the router was set to forward all DHCP requests to the DHCP Server.
- A DHCP pool comprising 50 IP addresses was established specifically for the local network connected to the Switch.
- All PCs within the local network were configured as DHCP clients.

When the DHCP server is properly configured, DHCP clients automatically receive IP addresses upon setting their IP configuration to DHCP. Figure 7 illustrates the IP configuration obtained by both PC0 and PC1 from the DHCP server.

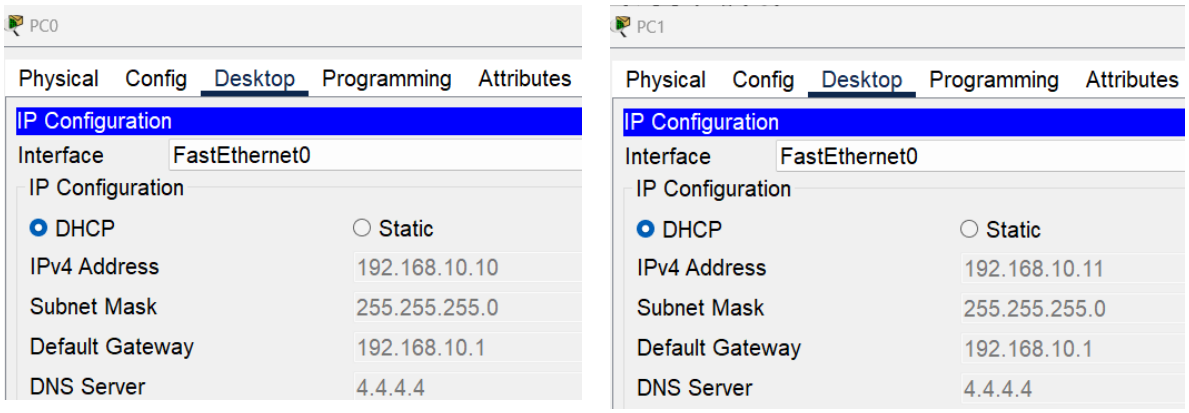

Figure 7. IP Configuration for Client PCs

The settings shown in Figure 7 were recorded before the DHCP attacker server was introduced into the network. To examine the functionality of the DHCP spoofing process, we incorporated a DHCP hacker server, as depicted in Figure 8.

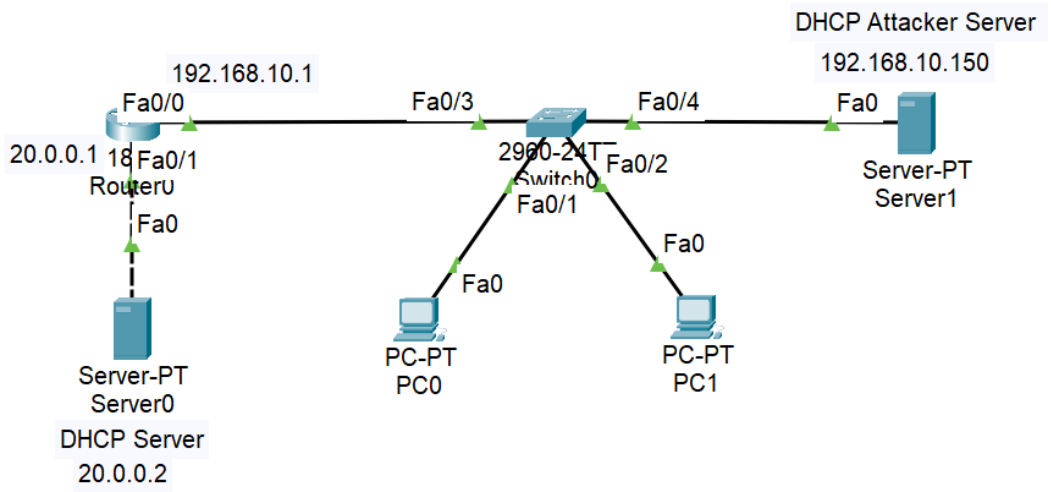

Figure 8. Network Toppology with Attacker Server

Figure 9 illustrates how both PC0 and PC1 acquire a new IP configuration from the attacker's DHCP server instead of the designated DHCP server when requesting a new IP configuration.

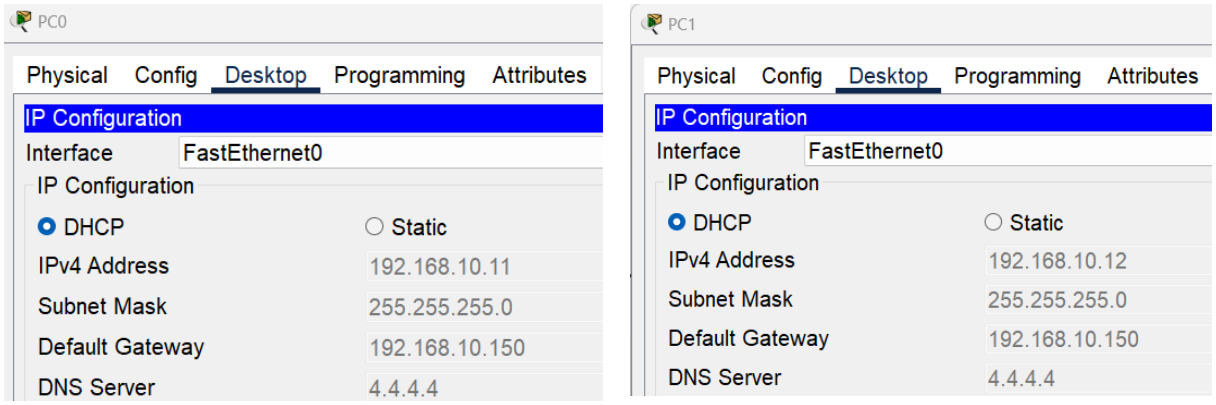

Figure 9. IP Configuration Obtained from Attacker Server

The attacker's DHCP server is positioned within the local network to intercept DHCP requests from clients before they reach the legitimate DHCP server. By preempting the original server's response, the attacker's DHCP server is the first to respond, providing the client with an IP configuration directly from the attacker's server.

4.2. DHCP Snooping Configuration On Switch

Upon enabling DHCP snooping, only the DHCP server connected to the trusted interface (specifically, f0/11 in our setup) is authorized to provide IP configurations. The configuration commands required to enable DHCP snooping on the switch in our network are exemplified in Figure 10:

```
Switch>enable
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface fa0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

Figure 10. DHCP Snooping Enable Configuration

To validate this configuration, we will obtain a new IP configuration for a PC within the local network. Figure 11 demonstrates how both PC0 and PC1 receive a fresh IP configuration from the original DHCP server.

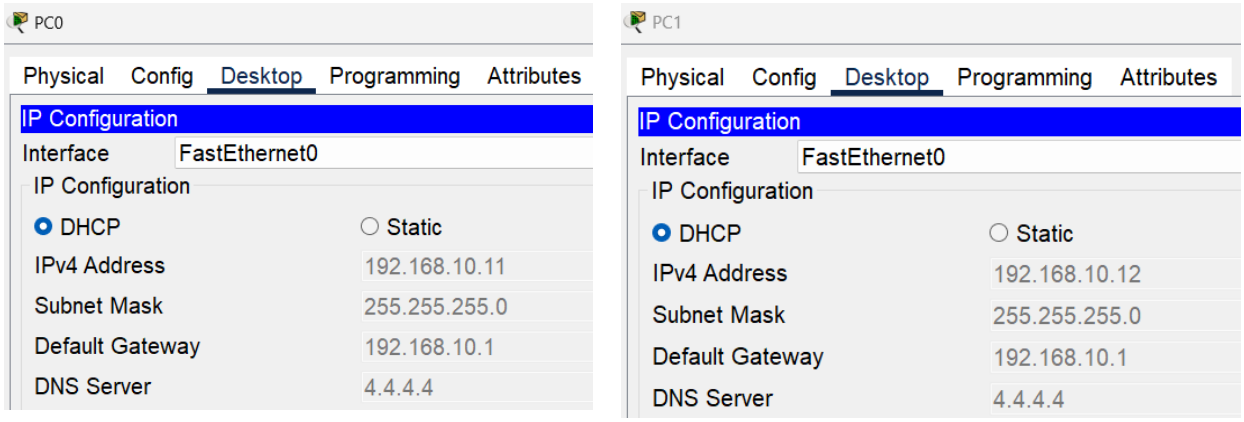

Figure 11. IP Configuration Acquired from DHCP Server with DHCP Snooping Implemented

To access the DHCP snooping configuration and statistics, the command 'show ip dhcp snooping' was employed, as demonstrated in Figure 12.

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/4            no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/3            yes        unlimited
```

Figure 12. Statistics for DHCP Snooping Configuration

Furthermore, essential information was obtained by employing the 'debug ip dhcp snooping event' and 'debug ip dhcp snooping packet' commands, which are specifically designed to debug DHCP snooping events and packets. This process is illustrated in Figure 13.

```
Switch#debug ip dhcp snooping event
Switch#debug ip dhcp snooping pac
Switch#debug ip dhcp snooping packet
Switch#00:50:21: DHCP_SNOOPING: received new DHCP packet from input interface
(FastEthernet0/2)
00:50:21: DHCP_SNOOPING: process new DHCP packet, message type: DHCP REQUEST, input
interface: Fa0/2, MAC da: FFFF.FFFF.FFFF, MAC sa: 0060.70DA.474B, IP da: 255.255.255.255,
IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.12, DHCP siaddr: 20.0.0.2,
DHCP giaddr: 192.168.10.1, DHCP chaddr: 0060.70DA.474B
00:50:21: %DHCP_SNOOPING: add binding on port FastEthernet0/2
00:50:21: DHCP_SNOOPING: add relay information option.
00:50:21: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:50:21: DHCP_SNOOPING: binary dump of relay info option, length: 20  data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x0 0x2 0x2 0x8 0x0 0x6 0x00 0x03 0xE4 0x5A 0x6D 0x22
00:50:21: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/2
00:50:21: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
00:50:21: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input
interface: Fa0/4, MAC da: FFFF.FFFF.FFFF, MAC sa: 00E0.8F24.93E9, IP da: 255.255.255.255,
IP sa: 192.168.10.150, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.12, DHCP siaddr:
192.168.10.150, DHCP giaddr: 192.168.10.150, DHCP chaddr: 0060.70DA.474B
00:50:21: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/3)
00:50:21: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input
interface: Fa0/3, MAC da: FFFF.FFFF.FFFF, MAC sa: 0001.C7E0.9601, IP da: 255.255.255.255,
IP sa: 192.168.10.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.12, DHCP siaddr:
20.0.0.2, DHCP giaddr: 192.168.10.1, DHCP chaddr: 0060.70DA.474B
00:50:21: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/3
```

Figure 13. IP DHCP Snooping Debugging Process

In Figure 13, a DHCP request packet is generated by the PC connected to interface fa0/2. This packet contains all the necessary information to request a new IP address from the DHCP server, including its MAC address (referred to as MAC SA in Figure 13). Although the packet originates from an untrusted port (interface), the switch processes and forwards it because it is a DHCP Request, not a DHCP Acknowledgment.

This DHCP request packet is distributed to all devices connected to the switch, including both the legitimate DHCP server and the hacker DHCP server. Consequently, the DHCP attacker server, connected to interface fa0/4, responds with a DHCP Acknowledgment message, including the MAC address of the DHCP server, indicating its capability to offer IP addresses to the requesting client. However, since the attacker is connected to an untrusted port and the message is a DHCP Acknowledgment, the switch does not forward this message to other ports.

Subsequently, a DHCP Acknowledgment message is also observed originating from the legitimate server connected to port f0/3. In this case, the switch permits the passage of this message, as it originates from a trusted port. This process consistently repeats for all requests originating from devices within the network whenever a device requires an IP address. By monitoring the requests from all devices, the data for each packet was meticulously recorded.

Although the DHCP snooping process functions effectively, a potential vulnerability exists if the DHCP attacker server connects to f0/3 (our secured port) as depicted in Figure 14, and attempts to send DHCP Acknowledgment messages from the same port used by the legitimate DHCP server (int f0/3 in this scenario).

In this situation, the switch will treat these messages as legitimate, as they appear to come from the trusted server. Consequently, it will block all messages from the legitimate DHCP server, incorrectly treating them as illegitimate requests from an unsecured port.

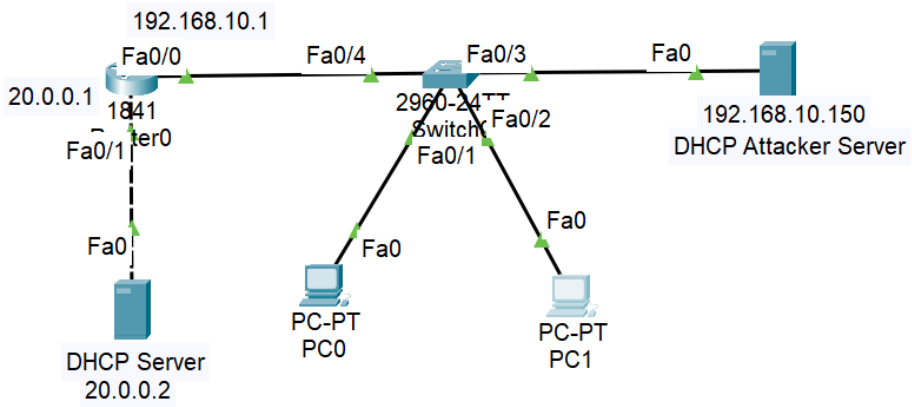

Figure 14. DHCP Attacker Acting as Legitimate DHCP Server

Figure 15 demonstrates how both PC0 and PC1 acquire again a new IP configuration from the attacker's DHCP server connected to f0/3, instead of the designated DHCP server connected to f0/4, when requesting a new IP configuration.

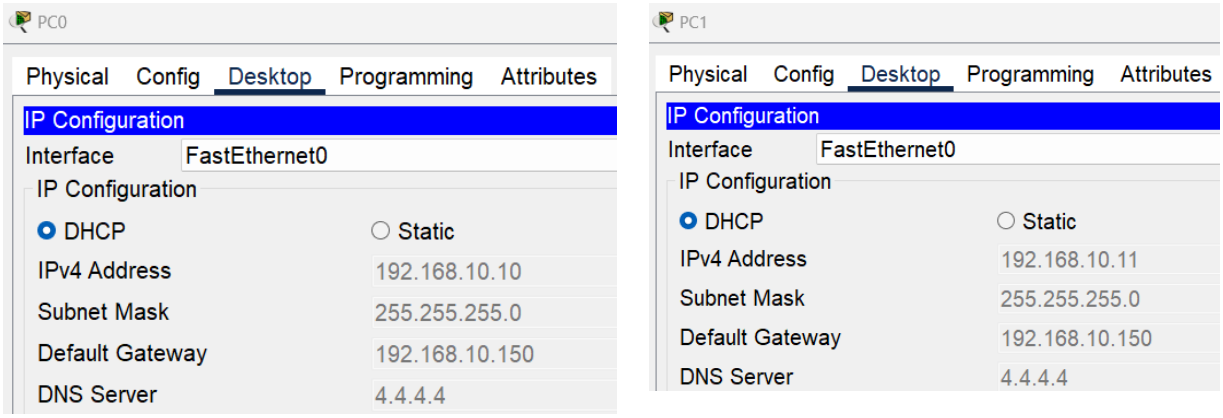

Figure 15. PC0 and PC1 Configuration Gained From Attacker Server

Upon examining the output of the DHCP Snooping debug process depicted in Figure 16, it becomes apparent that the switch initiates the forwarding of DHCP ACK packets originating from the DHCP attacker, while simultaneously inhibiting the transmission of DHCP ACK packets originating from the authentic DHCP server.

```
Switch>
Switch>01:07:48: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/2)
01:07:48: DHCP_SNOOPING: process new DHCP packet, message type: DHCP REQUEST, input interface: Fa0/2, MAC da: FFFF.FFFF.FFFF, MAC
sa: 0060.70DA.474B, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.10, DHCP siaddr:
192.168.10.150, DHCP giaddr: 192.168.10.150, DHCP chaddr: 0060.70DA.474B
01:07:48: %DHCP_SNOOPING: add binding on port FastEthernet0/2
01:07:48: DHCP_SNOOPING: add relay information option.
01:07:48: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
01:07:48: DHCP_SNOOPING: binary dump of relay info option, length: 20  data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x0 0x2 0x2 0x8 0x0 0x6 0x00 0x03 0xE4 0x5A 0x6D 0x22
01:07:48: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/2
01:07:48: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/3)
01:07:48: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input interface: Fa0/3, MAC da: FFFF.FFFF.FFFF, MAC sa:
00E0.8F24.93E9, IP da: 255.255.255.255, IP sa: 192.168.10.150, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.10, DHCP siaddr:
192.168.10.150, DHCP giaddr: 192.168.10.150, DHCP chaddr: 0060.70DA.474B
01:07:48: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/3
01:07:48: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
01:07:48: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input interface: Fa0/4, MAC da: FFFF.FFFF.FFFF, MAC sa:
0001.C7E0.9601, IP da: 255.255.255.255, IP sa: 192.168.10.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.10.10, DHCP siaddr:
20.0.0.2, DHCP giaddr: 192.168.10.1, DHCP chaddr: 0060.70DA.474B
```

Figure 16. DHCP Snooping Debug Process After Attacking

4.3 Using Port Security

To mitigate this vulnerability, an additional security layer using the port security technique has been proposed. Port security restricts network access by limiting which devices can connect and how they can connect, allowing only specific devices or MAC addresses to access the network. In our scenario, this technique was applied to the f0/3 port connected to the legitimate DHCP server.

Consequently, only DHCP ACK packets received from the legitimate DHCP server's MAC address will be accepted. Any DHCP ACK request from a trusted port will be rejected if the MAC address does not match that of the legitimate DHCP server. Additionally, the trusted port will be closed to prevent further requests from this port**.** To view the MAC addresses of the devices connected to the switch, the "show mac-address-table" command is used as shown in Figure 17:

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c7e0.9601    DYNAMIC     Fa0/3
   1    000d.bd81.cb0a    DYNAMIC     Fa0/1
   1    0060.70da.474b    DYNAMIC     Fa0/2
   1    00e0.8f24.93e9    DYNAMIC     Fa0/4
```

Figure 17. "show mac-address-table" Command Result

To implement the port security technique on port f0/3, the following commands are executed as illustrated in Figure 18:

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#exit
Switch(config)#
```

Figure18. Port Security Activation Process

As shown in Figure 18, and to meet our requirements, we limited the number of hosts that can be associated with an interface. This limit can be set anywhere from 1 to 132. In our case, we set the limit to 1 using the switchport port-security maximum value command. We also need to specify the action to be taken in the event of a security violation. In our scenario, we applied the "Shutdown" mode, where the switch generates a violation alert and disables the port. The only way to re-enable the port is to manually enter the "no shutdown" command.

Upon re-examining the MAC address table on the switch, a noteworthy observation is the address type. Although the switch learns this address dynamically, it is displayed as STATIC. This behavior is a result of the "sticky" option used with the port security command. The "sticky" option automatically converts dynamically learned addresses into static addresses. TO show the status of each port after applying port security technique, we used the "show mac-address-table" command as depicted in Figure 19:

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c7e0.9601    STATIC      Fa0/3
   1    000d.bd81.cb0a    DYNAMIC     Fa0/1
   1    0060.70da.474b    DYNAMIC     Fa0/2
   1    00e0.8f24.93e9    DYNAMIC     Fa0/4
```

Figure 19. "show mac-address-table" Command Result

Figure 20 illustrates that the switch deactivated port f0/2 upon receiving a DHCP ACK response from a MAC address that differed from the legitimate DHCP server's MAC address, despite the response originating from a trusted port. Notably, Packet Tracer visually represented this event by changing the color of the port connected to the DHCP attacker's server to red, signifying the disconnection.

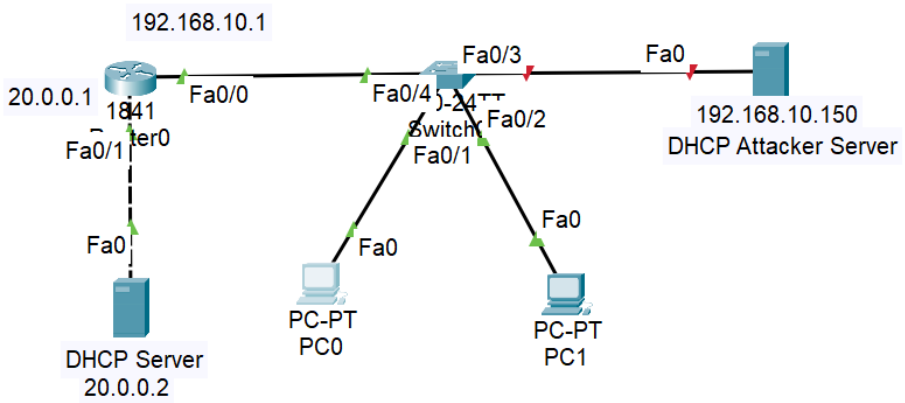

Figure 20. Blocking Packets From Attacker Server After Activating Port Security

Conversely, with the disconnection of the DHCP attacker server, no IP addresses will be assigned to any device within the network. Consequently, if any host requests a logical address, the switch will be unable to locate a DHCP server. As a result, the Automatic Private IP Addressing (APIPA) protocol will be activated on the host device, indicating the failure to obtain an IP address from any DHCP server as shown in Figure 21.

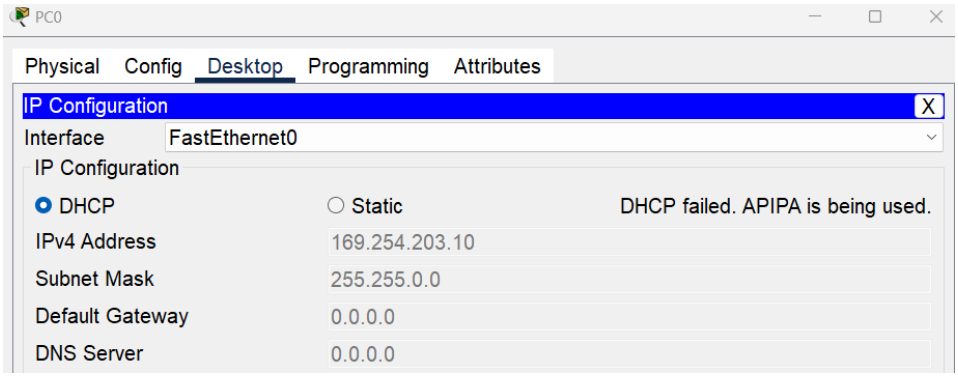

Figure 21. Activating APIPA Protocol After Failing Process of Obtaining IP Address

Even if we attempt to reconnect the legitimate DHCP server to the f0/3 port, it remains in a down state due to a port security violation. To reactivate the port and restore it to its normal operational state, we must follow the instructions provided in Figure 22:

```
Switch(config)#int f0/3
Switch(config-if)#sh
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
administratively down
Switch(config-if)#
Switch(config-if)#no shu
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state to up
```

Figure 22. Reactivating Port Using "no shutdown" Command

5. RESULTS AND DISCUSSIONS

The integration of DHCP Snooping with Port Security was tested in a simulated environment using Cisco Packet Tracer, as described in the methodology section. The network topology included both legitimate and rogue DHCP servers to evaluate the effectiveness of the combined security mechanisms. The results from the simulations validate the proposed approach, demonstrating significant improvements in mitigating DHCP spoofing attacks and preventing unauthorized network access.

5.1 Mitigation Of DHCP Spoofing Attacks

During the initial phase of the simulation, DHCP spoofing was successfully carried out when only DHCP Snooping was enabled. The rogue DHCP server, connected to an untrusted port, managed to respond to DHCP requests from client devices, leading to a successful Man-in-the-Middle (MITM) attack. This vulnerability aligns with previously reported issues where DHCP Snooping alone fails to protect against attacks when the intruder gains access to a secured or trusted port.

However, once Port Security was applied in conjunction with DHCP Snooping, the attack was effectively neutralized. The switch rejected DHCP ACK packets originating from the rogue server, based on the MAC address filtering implemented through Port Security. This result highlights the crucial role of Port Security in addressing the limitations of DHCP Snooping by adding an additional layer of verification. Only the legitimate DHCP server was able to provide IP addresses, ensuring the integrity of network configurations.

5.2 Impact On Network Stability

In scenarios where multiple devices attempted to access the network simultaneously, the combination of DHCP Snooping and Port Security proved to be stable. The rate-limiting feature of DHCP Snooping effectively managed DHCP traffic, preventing excessive DHCP requests from overwhelming the network. Port Security's dynamic learning of MAC addresses ensured that only authorized devices were granted network access, while maintaining a smooth operation for legitimate devices. No noticeable delays in IP address allocation were observed, confirming that the added security mechanisms did not degrade network performance.

5.3 Limitations Of The Current Approach

Despite the significant improvement in mitigating DHCP-based attacks, certain limitations were observed. The simulation revealed that if an attacker gains physical access to the trusted port, the effectiveness of both DHCP Snooping and Port Security can be compromised. Although Port Security can filter MAC addresses, an attacker with access to a trusted port may still be able to manipulate traffic if they clone the MAC address of a legitimate device. This highlights the need for

additional security measures, such as 802.1X authentication, to further protect trusted ports from unauthorized access.

5.4 Scientific Novelty and Comparative Evaluation

The novelty of this research lies in the practical and lightweight integration of DHCP Snooping and Port Security within traditional Layer 2 switch environments. This approach specifically addresses a key weakness of DHCP Snooping—its inability to protect against rogue DHCP servers when they are connected to trusted switch ports.

While several existing methods have been proposed to counter DHCP spoofing attacks, most focus on advanced environments such as Software-Defined Networking (SDN) or require machine learning-based detection mechanisms. For example:

- **DHCPGuard on SDN Controllers** [19] introduces IP pool recovery and rate-limiting but requires centralized SDN infrastructure.
- **DHCPWatcher** [24] employs multi-stage SDN defenses but lacks native compatibility with legacy or resource-constrained networks.
- **HybridDAD** [26] applies machine learning to programmable switches, offering strong detection but at a cost of higher computational requirements and complexity.

These techniques, while powerful, are not always practical for smaller enterprises, educational labs, or environments where only traditional switching infrastructure is available.

In contrast, the proposed method:

- Requires **no additional hardware** or external controllers.
- Leverages existing **Cisco IOS features**, making it easily deployable.
- Uses **MAC-based filtering and sticky learning** via Port Security to address the critical vulnerability of trusted ports in DHCP Snooping.

A comparative evaluation against common alternatives, such as ARP Inspection and VLAN separation, also reinforces this point. While ARP Inspection prevents address resolution spoofing, it does not mitigate DHCP-based attacks. VLAN segmentation helps contain threats but cannot prevent internal DHCP spoofing within the same VLAN. Thus, combining DHCP Snooping and Port Security delivers a more targeted and effective defense.

Table 1. Comparison with Existing Methods

Feature	Existing Methods ([19], [24], [26])	Proposed Approach
SDN/ML Requirements	Yes	No
Infrastructure Dependency	High (Controllers, ML agents)	Low (Switch CLI configurations only)
Real-time Attack Simulation	Often Theoretical	Demonstrated in Packet Tracer
Protection at Trusted Port	Partially addressed or ignored	Explicitly addressed with Port Security
Ease of Deployment	Moderate to Complex	Easy, CLI-based deployment
Performance Impact	May require resource tuning	Minimal, with no observed performance lag

This comparative analysis, along with the focus on practical deployability, underlines the unique contribution of this study to the field of Layer 2 network security.

6. CONCLUSION

In conclusion, this study successfully demonstrated the integration of DHCP Snooping and Port Security as a robust defense mechanism against DHCP spoofing attacks. By addressing the limitations of DHCP Snooping alone, which can be vulnerable when attackers gain access to trusted ports, the addition of Port Security provides an essential layer of protection. The results showed a significant improvement in mitigating Man-in-the-Middle (MITM) attacks by restricting unauthorized access to network resources and ensuring that only legitimate DHCP servers can assign IP addresses.

Furthermore, the solution maintained network stability, even under scenarios involving multiple devices, without introducing any performance degradation. While this approach greatly enhances network security, it also highlighted certain limitations. Specifically, the method could still be compromised if an attacker gains physical access to a trusted port, emphasizing the need for further research into additional security measures such as 802.1X authentication.

This study lays the groundwork for future explorations into combining other security technologies, like Network Access Control (NAC) and real-world testing on larger and more complex networks, to strengthen network defenses and scalability.

REFERENCES

Adesemowo, A. K., & Gerber, M. (2014). E-skilling on fundamental ICT networking concepts–Overcoming the resource constraints at a South African university. Proceedings of e-Skills Knowledge Production and Innovation Conference, 1–16.

Adjei, H. A., Shunhua, M. T., Agordzo, G. K., Li, Y., Peprah, G., & Gyarteng, E. S. (2021). SSL stripping technique (DHCP snooping and ARP spoofing inspection). 2021 23rd International Conference on Advanced Communication Technology (ICACT), 187–193.

Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

Alsaadi, R. R., & Abdul-Zahra, D. S. (n.d.). Security DHCP server on LAN network. Turkish Journal of Physiotherapy and Rehabilitation, 32, 3.

Ali, S. M., & Shareef, A. A. (2021). Designing a secure network solution against DHCP attacks. Iraqi Journal of Information & Communication Technology, 1(1), 45–57.

Aldaoud, M., Al-Abri, D., Al Maashri, A., & Kausar, F. (2021). DHCP attacking tools: An analysis. Journal of Computer Virology and Hacking Techniques, 17, 119–129.

Aldaoud, M., Al-Abri, D., Al Maashri, A., & Kausar, F. (2023). Detecting and mitigating DHCP attacks in OpenFlow-based SDN networks: A comprehensive approach. Journal of Computer Virology and Hacking Techniques, 19(4), 597–614.

Banitalebi Dehkordi, A., Soltanaghaei, M., & Boroujeni, F. Z. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. Journal of Supercomputing, 77(3), 2383–2415.

Bhushan, B., Sahoo, G., & Rai, A. K. (2017). Man-in-the-middle attack in wireless and computer networking—A review. 2017 3rd International Conference on Advanced Computing, Communication and Automation (ICACCA) (Fall), 1–6.

Buhr, A., Lindskog, D., Zavarsky, P., & Ruhl, R. (2011). Media access control address spoofing attacks against port security. Proceedings of the 5th USENIX Workshop on Offensive Technologies (WOOT 11).

Cisco Systems. (2007a). Configuring port-based traffic control. Catalyst 3550 Multilayer Switch Software Configuration Guide. Cisco Systems.

Cisco Systems. (2007b). Cisco Catalyst 3750 series switches: Layer 2 security features on Cisco Catalyst layer 3 fixed configuration switches configuration. Cisco Systems.

Droms, R. (1997a). RFC2131: Dynamic host configuration protocol.

Droms, R. (1997b). Dynamic host configuration protocol. Network Working Group, Internet Requests for Comments. RFC Editor.

Kalkancı, G., Ahmet, E. F. E., D. O. N. K., Cihangir, S., & Uysal, Z. A. (2019). A hidden hazard: Man-in-the-middle attack in networks. Computer Science, 4(2), 96–116.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), 164–173.

Mehran, U. E. T. (2022). Detection of server-side DHCP DoS and spoofing attack using machine learning techniques. 3rd International Conference on Computer Science and Technology.

Miftah, Z. (2018). Simulasi keamanan jaringan dengan metode DHCP snooping dan VLAN. Faktor Exacta, 11(2), 167.

Pradana, D. A., & Budiman, A. S. (2021). The DHCP snooping and DHCP alert method in securing DHCP server from DHCP rogue attack. International Journal of Informatics Development (IJID), 10(1), 38–46.

Purnomo, A. (2024). Implementation of DHCP snooping method to improve security on computer networks. bit-Tech, 6(3).

Roshani, M., & Nobakht, M. (2022). Hybriddad: Detecting DDoS flooding attack using machine learning with programmable switches. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–11.

Sandhya, M. (2023). Empirical investigations on the security and threat mitigation of campus switches. 2023 International Conference on Computer Communication and Informatics (ICCCI), 1–8.

Shrestha, P., & Sherpa, T. D. (2023). Dynamic host configuration protocol attacks and its detection using Python scripts. 2023 International Conference on Artificial Intelligence, Knowledge Discovery and Concurrent Engineering (ICECONF), 1–5.

Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. Journal of Information and Telecommunication, 4(4), 482–503.

Syed, S., Khuhawar, F., Talpur, S., Memon, A. A., Luque-Nieto, M. A., & Narejo, S. (2022). Analysis of dynamic host control protocol implementation to assess DoS attacks. 2022 Global Conference on Wireless and Optical Technologies (GCWOT), 1–7.

Tok, M. S., & Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. Computers & Security, 109, 102394.

Tripathi, N., & Hubballi, N. (2018). Detecting stealth DHCP starvation attack using machine learning approach. Journal of Computer Virology and Hacking Techniques, 14, 233–244.

Yan, A., Jing, S., Qi, Q., & Xiao, B. (2016). A study on campus network access and export management. Proceedings of the 2nd Workshop on Advanced Research Technology in Industry Applications (WARTIA-16), 1812–1816.