University of New Haven

# Comprehensive Analysis of Wireless Network Vulnerabilities and Mitigation Strategies with a Simulation-Based Evaluation Using Cisco Packet Tracer

Kyle Mather, Braeden Allen, Anthony Ciavarella

CSCI 4482: Wireless Networks

Dr. Moin Bhuiyan

3 May 2025

# Contents

# Abstract

Over the past decade, wireless network technologies have revolutionized connectivity with unprecedented scalability and flexibility. The open-air transmission medium, however, exposes these networks to sophisticated threats such as rogue access points (APs), denial-of-service attacks, session hijacking, and eavesdropping. Rogue APs exploit user assumptions about legitimate SSIDs to intercept credentials and inject malicious traffic, a vulnerability highlighted through theoretical analysis and Cisco Packet Tracer simulations. The simulation shows how unintentional users could associate with nefarious networks and how malicious elements can take charge or steal data in organizational setups. Pre-authentication based only on pre-shared keys is inadequate in shared contexts, and as such more evolved defenses such as Daldoul's Robust Certificate Management System (RCMS) have come into focus. RCMS extends 802.1X authentication through server and client certificate validation codes, repelling evil twin attacks without necessitating a modification of existing IEEE 802.11 protocols. Besides authentication improvement, physical-layer detection techniques like Channel State Information (CSI) analysis use unique signal propagation characteristics to identify rogue transmissions. CSI-based solutions offer non-intrusive and precise rogue AP localization even under high traffic conditions with overlapping signal spaces. The project suggests a multi-layered security approach that imposes secure authentication, certificate validation, traffic inspection, anomaly detection, and physical-layer protection to counter a broad spectrum of wireless attacks. By integrating these multi-disciplinary methods, organizations can strengthen their defenses and dynamically adapt to evolving wireless security threats.

# Introduction

With the world progressing to a digital era, the channels of communication have kept pace with technological advancements. Among the most groundbreaking developments is the adaptation of wireless networks, which have become a cornerstone of digital communication in today's era. A wireless network is a collection of computers that transfer data between devices using radio frequency signals as opposed to traditional physical connectors such as Ethernet ("What Is a Wireless Network?"). This way, devices can remain connected within the network without having to be connected into physical network ports, hence offering greater mobility, flexibility, and ease of installation. For this reason, wireless networking is now ubiquitous for both consumer and business use. From home wireless installs to complex enterprise implementations, wireless technologies continue to reshape how information is communicated in almost every aspect.

Wireless networking is not just nicety, it is a strategic necessity in present-day organizations. Corporations globally employ wireless infrastructure for providing seamless connectivity across their buildings. This infrastructure is typically superimposed over existing wired networks to allow employees to access anywhere within the organization, enhance productivity, and facilitate real-time communication (Nazir et al.). Employees are no longer bound to specific workstations; instead, they can roam between rooms, floors, or even buildings, but remain securely connected to the company's virtual world. This convergence of wireless and wireline infrastructures allows businesses the adaptability to support modern workflows, remote work, and rapid data access, which are crucial in staying competitive in a highly connected world.

But as greater reliance on wireless networks comes to pass, so too does the matched expansion in threats and vulnerabilities associated with them. Unlike wired networks, whose physical presence is an intrusion condition, wireless networks exist outside the physical realm, and thus, are more susceptible to unauthorized access, signal tapping, and all types of cyber attacks. As Laghari et al. observe in their wireless security survey, "Wireless networks inherently possess a greater attack surface due to their broadcast nature, which permits malicious parties to eavesdrop, intercept, or spoof signals from beyond the physical limits of a secure environment." The identical traits that render wireless networking so attractive—mobility, open nature, and simplicity of setup—also render it susceptible to exploits such as man-in-the-middle (MitM), denial-of-service (DoS), spoofing, and most critically, rogue access point (AP) installations.

A rogue access point is any unauthorized wireless AP that is installed on a secure network without permission. This can occur when an employee accidentally installs an insecure router, or worse, when an attacker installs a fake AP, also widely known as an evil twin, to impersonate a legitimate network and trick users into joining. The moment a device gets associated with the rogue AP, attackers can steal confidential data, capture login credentials, and even disseminate

malware. Such attacks are not limited to public networks; corporate networks are particularly appealing since the data transferred in them is high-value.

To show the actual impact of such attacks, our research exemplifies an instance in which a malicious AP was installed and utilized inside an emulated corporate network with Cisco Packet Tracer. Cisco Packet Tracer offers a training ground to mimic real-world networking scenarios, and hence it is the most suitable tool to simulate wireless vulnerabilities and try out countermeasures in a risk-free, virtual laboratory. In our case study, we demonstrate how an intruder AP can be configured to mimic a trusted network, how devices will automatically associate with it because of signal strength and known SSIDs, and how attackers can use this setup to steal data. The simulation emphasizes the necessity of robust authentication and network monitoring procedures to guard against such attacks.

Knowing the shortcomings of traditional password-based security, particularly in settings where network credentials are being shared among numerous users, our research also explores advanced methods of combating wireless vulnerabilities. These include certificate-based authentication systems such as IEEE 802.1X and other defense layers such as the Robust Certificate Management System (RCMS) proposed by Daldoul. RCMS enhances traditional 802.1X implementations by incorporating an authentication code to allow users to verify the validity of the certificate of the network, hence avoiding evil twin attacks without changing the 802.11 standard (Daldoul). The process provides an effective and secure mechanism for small as well as large wireless environments using elimination of reliance on user decision-making and certificate verification simplicity.

Other rival security solutions focus on physical-layer detection. Methods such as channel state information (CSI) analysis have been used to accurately localize rogue access points using the detection of subtle differences in signal propagation patterns. Because CSI is effectively unspoofable, it is an even better mechanism for verifying AP authenticity, especially in densely populated city or campus environments where many networks may utilize the same SSIDs (Zheng et al.).

In short, while wireless networks are integral to the freedom and usability of modern digital infrastructure, they also present certain and distinct security threats. Organizations will be required to put in place a multilayered defense strategy that goes beyond existing password-based protection methods and adds advanced detection, authentication, and access control features. This essay discusses these measures using literature review, technical simulation, and analytical evaluation and gives insights on how wireless networks can both be a vulnerability and an advantage in the wired world of today.

# Rogue Access Point (AP) Attacks

In the modern interconnected digital world, wireless networks are ubiquitous, providing unprecedented convenience and mobility. But with this omnipresence comes the huge security problem. Rogue access points (RAPs), unauthorized wireless appliances, are some of the most devious threats as they can breach the integrity of the network and that of the user's data (Alotaibi and Elleithy). Familiarity with the mechanisms, implications, and mitigation of RAPs is necessary to ensure strong network security.

## Types and Deployments of RAPs

Rogue access points can be broadly categorized based on their origin and intention. Unauthorized RAPs are typically created by innocent employees attempting to obtain better connectivity, inadvertently creating vulnerabilities. Compromised RAPs result from legitimate devices being taken over by attackers. Improperly configured RAPs are the result of misconfigurations that compromise networks. Evil twin RAPs, on the other hand, are purposely deployed to masquerade as legitimate access points, enticing users to connect and then pilfering their data (Alotaibi and Elleithy).

The deployment of RAPs is alarmingly simple. Hackers can use readily available software and hardware to deploy these rogue access points. For instance, tools like Aircrack-ng and Kismet allow for the setup and management of rogue APs with minimal technical expertise (McGinniss). Moreover, the availability and portability of hardware like Raspberry Pi make it simple for hackers to deploy RAPs in most environments discreetly.

## Attack Vectors and Techniques

RAPs employ several techniques to compromise network security. Among the usual techniques employed is the deauthentication attack, where attackers send spoofed deauthentication frames to valid clients, which then disconnect. Afterwards, those clients will automatically reconnect to a rogue AP that is broadcasting the same SSID and, in the process, unwittingly compromise their data (McGinniss).

Another sophisticated technique is the KARMA attack, in which attackers exploit the preferred network list (PNL) of devices. Devices broadcast their PNLs to discover known networks, and attackers can respond by spoofing these networks, thereby inducing devices to

connect automatically (Wright). This is an efficient approach as it leverages the implicit trust devices place in networks they have connected to before.

Furthermore, captive portals are used by attackers to hijack user credentials. Once a device is associated with a rogue AP, the user may be redirected by the attacker to a spoofed login page that resembles one from a legitimate service. Oblivious users will then enter their credentials, which are captured by the attacker for malicious use (Wolfe).

## Detection and Mitigation Strategies

Detection of RAPs becomes rather difficult based on their ability to mimic legitimate access points very convincingly. Traditional detection methods appear in the form of tracing intruder devices through the use of network management software. Those detection methods could, however, not work against stealthy RAPs that imitate the behavior and pattern of normal APs (Alotaibi and Elleithy).

Advanced detection techniques employ data from the physical layer, i.e., Channel State Information (CSI), to identify anomalies in signal propagation. It is possible to distinguish between legitimate and rogue APs on the basis of the unique characteristics of wireless signals, even if they share the same SSID (McGinniss). This method improves accuracy but can be achieved only with specialized hardware and expertise.

Another potential solution is the implementation of Robust Certificate Management Systems (RCMS) that enhance the security of 802.1X authentication. RCMS inserts a verification code based on client credentials and the server's certificate, through which clients can authenticate the network before establishing a connection (Daldoul). RCMS essentially defeats evil twin attacks because it compels clients to establish connections on authenticated networks.

Additionally, location-based detection methods utilize the determined locations of authentic APs for the sake of detecting anomalies. Comparison of measured signal strength and location with expected signal strengths and locations as derived from real-time measurement facilitates the detection of rogue APs deviating from established patterns (Liu and Papadimitratos). The method is most applicable to infrastructure-fixture environments like corporate campuses and centers.

## Bringing it all Together

Malicious access points pose a significant security risk to wireless networks, exploiting the built-in trust and convenience of wireless connections. Attackers are able to steal confidential information and disrupt network activities through a range of techniques, including deauthentication attacks, KARMA attacks, and credential theft via captive portals. Detection and mitigation need to be multi-pronged, with conventional monitoring supplemented by advanced techniques like CSI analysis, certificate-based authentication, and position-based detection. With wireless networks growing rapidly, paying special attention to the design and deployment of robust security against RAPs is the requirement of the time to secure digital infrastructure.

# Cisco Packet Tracer Analysis

The following section outlines a simulated Rogue Access Point attack in Cisco Packet Tracer version 8.2.2. This network layout shows a common rogue access point (RAP) attack environment within a segmented wireless network. On the left, we have a legitimate wireless network with a server (Server1) that is hooked up to a 2960-24TT switch, then to a 1941 router and a legitimate access point (Access Point0). This is a secure corporate LAN with centralized resources and access control.

On the topology's right, we observe that a rogue access point (RogueAP) has been added. A client wireless device (PC0) connects directly to this unauthorized AP, bypassing the organization's authorized infrastructure. The rogue AP is bridged to a sniffer node (Sniffer0), which has been configured for intercepting or monitoring traffic. Sniffer0 is connected to PC2, which is an attacker's monitor station or external victim's endpoint. This setup explicitly illustrates how attackers would use rogue APs to trick unaware users into associating, enabling them to sniff data packets, steal credentials, or perform man-in-the-middle (MitM) attacks.

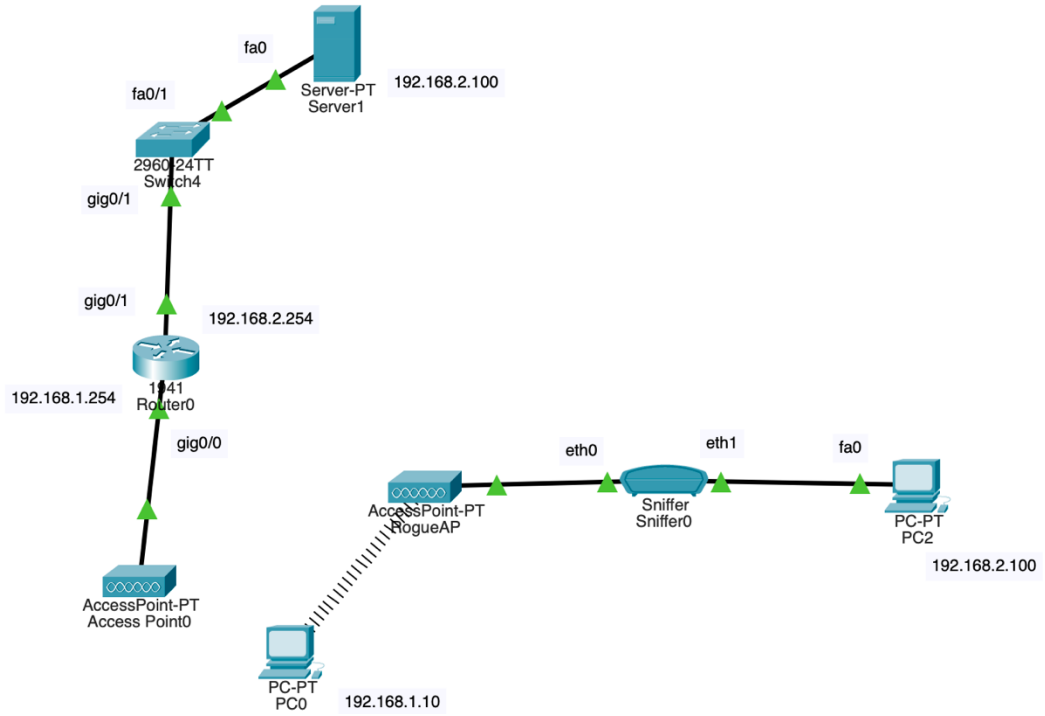


Figure 1. Simulated RAP Attack Network Topology

## Attack Vector

In this simulation, the attacker deploys a rogue access point (RogueAP) configured to broadcast the same SSID as the legitimate corporate Wi-Fi network managed by Access Point0. The victim device (PC0) is within the wireless range of both access points. Due to factors such as stronger signal strength or lack of proper certificate verification, PC0 connects to the rogue AP, believing it is the legitimate network.

Once the victim connects, all of its traffic is funneled through RogueAP, which is wired to a sniffer device (Sniffer0). This traffic can include a simple web request (Figure 2), which is the most likely action here as the user believes there is a legitimate server at the other end of their connection. Sniffer0 acts as the adversary's interception node, capable of capturing unencrypted traffic, session cookies, and authentication credentials or even performing real-time data manipulation (Figure 3). From Sniffer0, the attacker can relay traffic to PC2, simulating further data exfiltration or control.

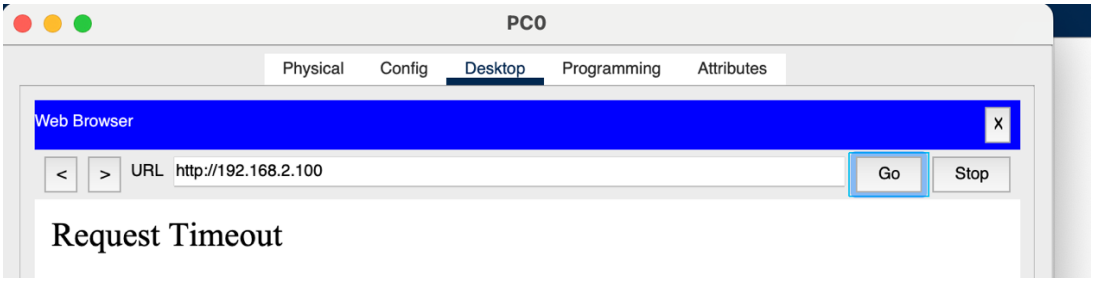


Figure 2. Spoofed Web Request

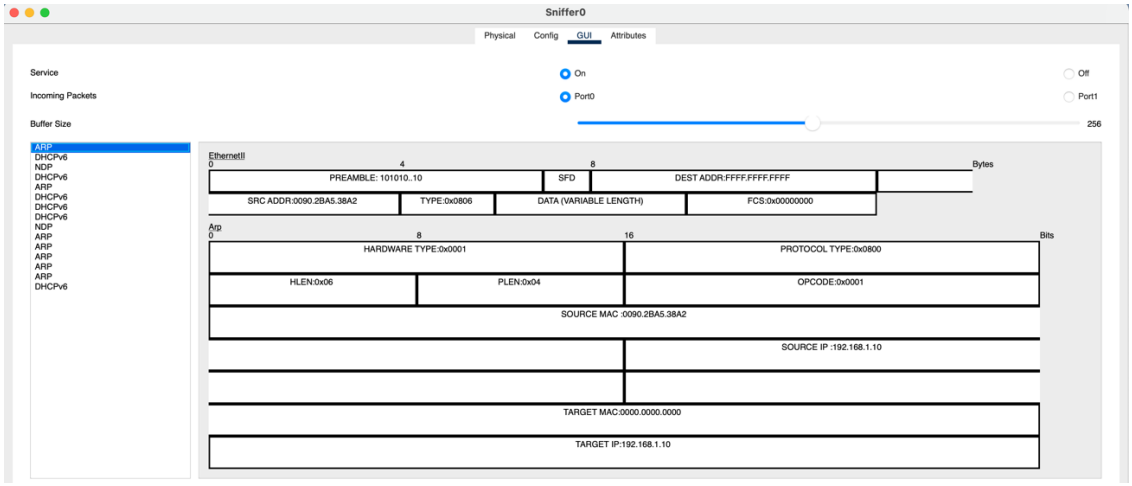


Figure 3. Packets captured by Sniffer0

This attack exploits the lack of mutual authentication and insecure SSID trust behavior by client devices. It is highly effective in environments where pre-shared key (PSK) security is used without additional validation mechanisms, such as certificate-based 802.1X authentication. By positioning themselves between the victim and the legitimate network, the attacker can intercept sensitive communications, launch phishing portals, or inject malicious payloads.

## Defense Mechanisms

To prevent the rogue access point attack observed in the previous network structure, WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key) authentication was implemented on the legitimate access point and associated client devices. This configuration change serves as a basic layer of wireless security since it requires all devices to authenticate using a shared secret passphrase before receiving encrypted data. Access Point0 and PC0 have both been configured to use WPA2-PSK with AES encryption and the passphrase being P@ssw0rd (Figures 4 and 5).

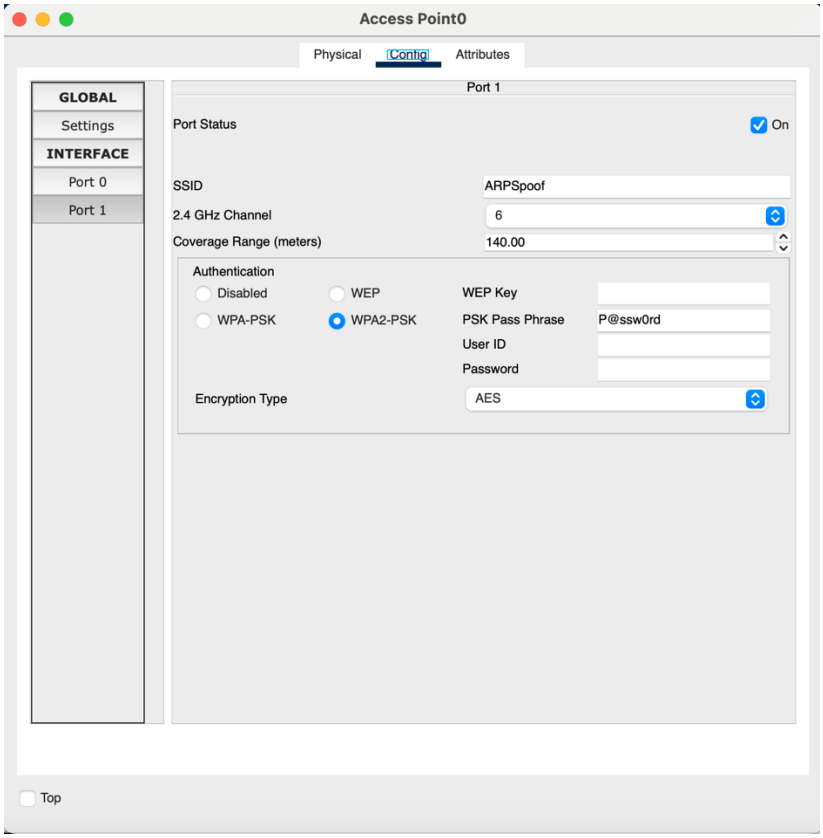


Figure 4. WPA2-PSK implemented in legitimate AP

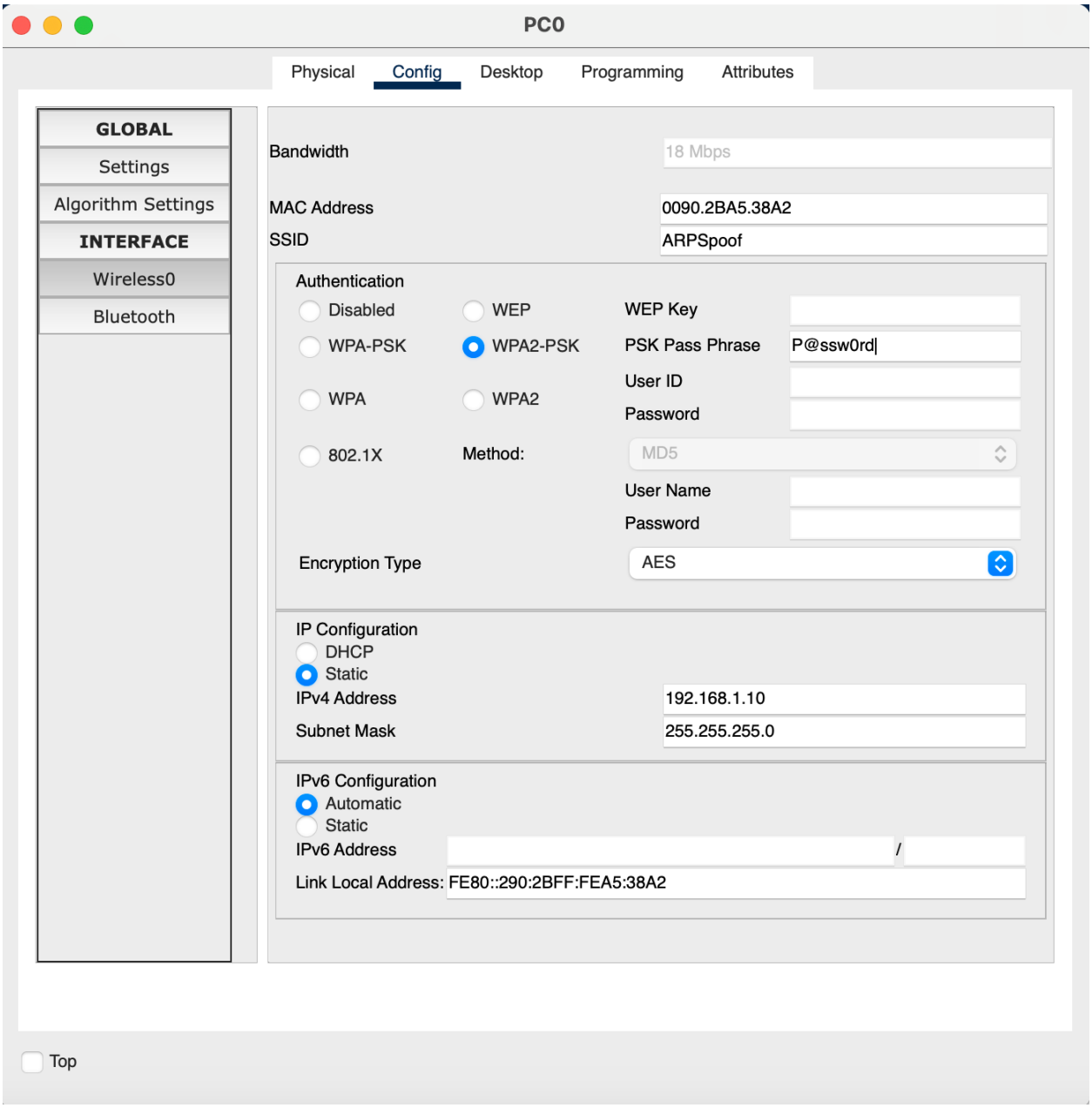


Figure 5. PC0 with WPA2-PSK credentials

This produced a successful PC0 connection to the correct access point (Figure 6).

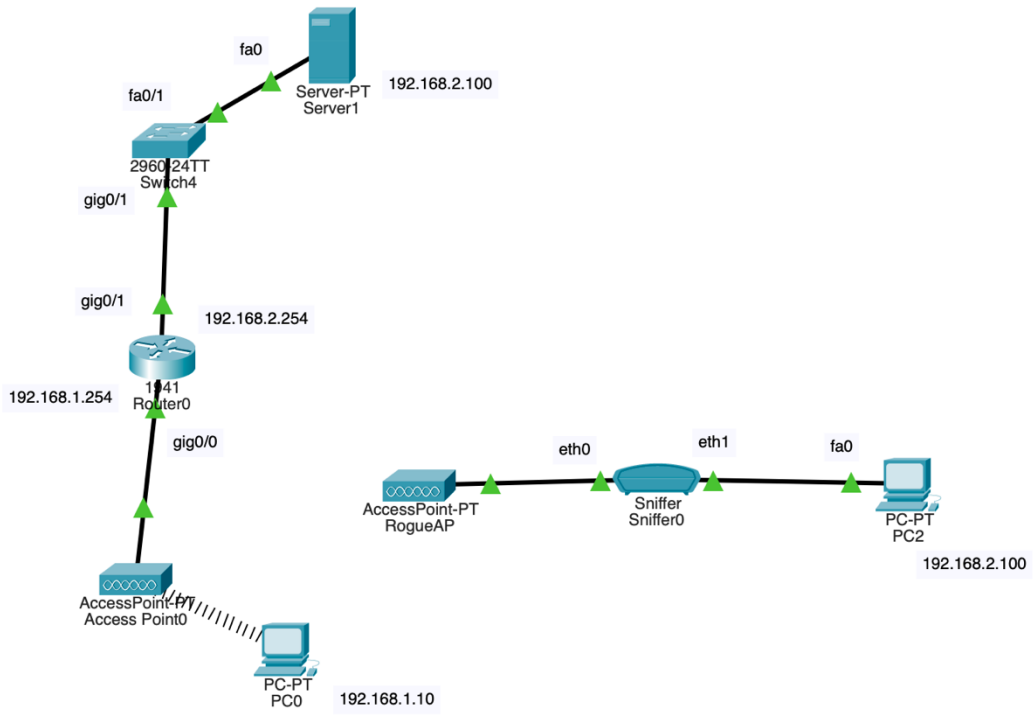


Figure 6. Remediated network topology

WPA2-PSK significantly surpasses outdated security mechanisms like WEP and open authentication by implementing dynamic key generation along with improved encryption. The Advanced Encryption Standard (AES), employed in WPA2, encrypts link-layer data, making it much more difficult for an attacker to decrypt and intercept wireless communications even if they gain access to the network traffic. In this case, AES maintains sensitive information exchanged between the client (PC0) and the legitimate AP secret and secure.

The SSID on the rogue and authentic APs, "ARPSpoof," was intentionally copied by the attacker in order to exploit client trust in familiar networks. However, as WPA2-PSK employs the correct passphrase for association, any device broadcasting the same SSID without using the correct PSK will be rejected by clients with the valid credentials. As illustrated by the browser screen shot, PC0 is able to access resources (e.g., server 192.168.2.100) safely after successful authentication with Access Point0, proving successful deployment of defense (Figure 7).

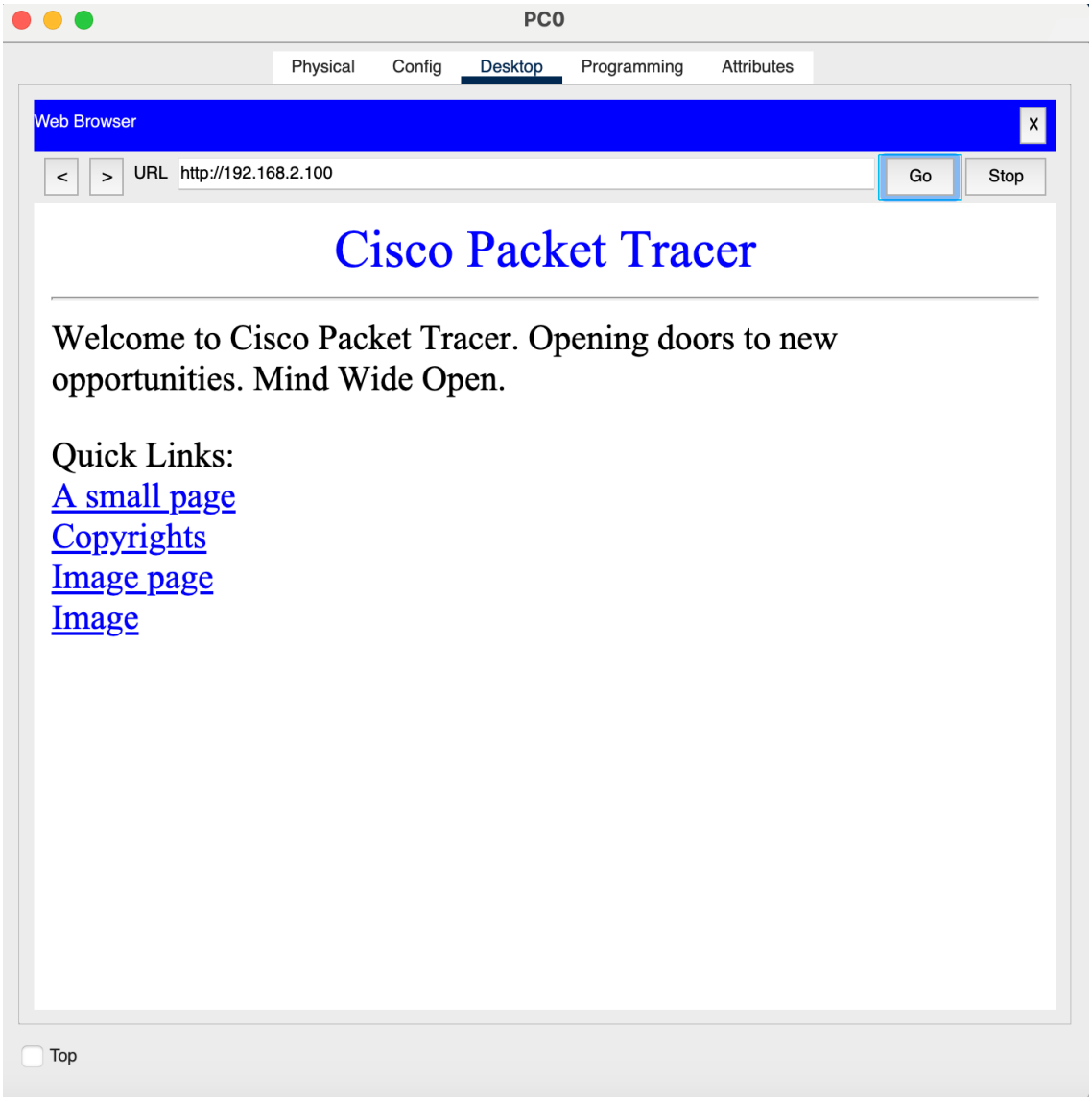


Figure 7. Successful connection to web server

While WPA2-PSK is appropriate for small to medium-sized deployments, keep in mind that in the larger enterprise environment, other security measures such as WPA3 or certificate-based 802.1X authentication would be preferable. Yet the WPA2-PSK security implemented here does prevent unauthorized access and ward off most rogue AP threats in managed networks.

# Results

Consider a determined attacker placing two adjacent wireless access points in the busy lobby of an office building—one legitimate AP promoting SSID "ARPSpoof" with WPA2-PSK (P@ssw0rd) and AES encryption, and another malicious "evil-twin" AP mimicking the same SSID on the same channel but with no security. The laptop of a passerby, PC0, initially tries to associate with whichever AP is speedy. In a non-secure environment, the evil twin would immediately hijack PC0's DHCP request and direct all of its HTTP and DNS sessions through an undetectable sniffer, giving the attacker full visibility into user sessions and credentials.

But the instant PC0's network profile is configured to require WPA2-PSK using the secure passphrase P@ssw0rd, the attacker AP's handshakes don't work: PC0 won't complete the WPA2 four-way handshake with any network that can't show proof of ownership of the shared key. Rather, it will automatically join the real AP, restoring secure access to internal resources (for example, an intranet server at 192.168.2.100) silently. No EAPOL frames for PC0 ever reach the rogue device, and no user data is compromised.

With this hypothetical real-world attack, using a robust WPA2-PSK setup effectively neutralizes the evil-twin attack in a small-to-medium network. By applying mutual authentication and AES encryption, it renders impersonation attempts worthless—no special enterprise infrastructure is required, but the confidentiality and integrity of wireless sessions are maintained.

# Discussion and Analysis

While WPA2-PSK worked for this implementation, it is not entirely robust. This section outlines alternative methods for mitigation RAP attacks.

## Wireless Intrusion Prevention Systems (WIPS)

Wireless Intrusion Prevention Systems (WIPS) are prevention systems that are employed to scan the radio frequency for unauthorized access points. Continuously scanning for devices that are not part of the authenticated network equipment, WIPS can detect and prevent unauthorized devices from accessing. WIPS typically employ sensors deployed throughout the network environment to detect and eliminate rogue devices in real-time. The power of WIPS lies in its ability to respond automatically to threats, thus closing the window of opportunity for attackers to exploit network vulnerabilities (Wexler).

## Position-Based Detection

Position-based detection relies on the physical location of access points to identify anomalies. Through processing the received signal strength indicators (RSSIs) and comparing them with the known locations of the legitimate access points, the system can detect discrepancies that can indicate the existence of a rogue device. This method enhances detection accuracy by considering spatial information, which makes it more difficult for attackers to mimic legitimate access points without being detected (Liu and Papadimitratos).

## Channel-State Information (CSI)

Channel State Information (CSI) supplies subtle information about the peculiarities of a wireless channel. By CSI analysis, one can identify tiny fluctuations in signal peculiarities that distinguish legitimate access points from rogue access points. This is a technique that involves capturing and analyzing the unique "fingerprints" of wireless signals, which are difficult to replicate for an intruder. Incorporating CSI analysis enhances the network's capability to detect and respond to unauthorized devices in an efficient manner (McGinniss).

## Software-Defined Networking (SDN)

Software-Defined Networking (SDN) offers a centralized control framework that dynamically manages network resources and policies. For the detection of rogue access points, SDN can be employed to monitor network traffic flows and implement security policies within the network. By abstracting the control plane from the data plane, SDN enables more responsive and flexible security actions, enabling the network to dynamically respond to nascent threats and quarantine rogue devices efficiently (Ampatzi).

## Multi-Agent Detection Frameworks

Multi-agent systems employ an army of autonomous agents that cooperate to monitor and safeguard the network terrain. Each of these agents is responsible for watching specific areas of the network and reporting back to other agents to generate a comprehensive picture of the security position of the network. This collaborative approach enhances the identification of unauthorized access points through the integration of perspectives from multiple points of observation, therefore enhancing the opportunities for early detection of unauthorized devices (Sasane and Pathan).

# Conclusions

In a time when connectivity is the very nature for companies, the ubiquity of wireless networks has not only provided convenience but also introduced new security concerns. Among the most pernicious and dangerous threats to wireless infrastructure are rogue access points (RAPs). Unlicensed devices exploit the unlicensed nature of radio communications, often masquerading as valid access points to lure users into logging in. Once linked, attackers are able to intercept private data, hijack traffic, or introduce malware — breaching confidentiality, integrity, and availability.

This paper tested the nature of rogue access point attack and demonstrated its impact by designing a simulation on Cisco Packet Tracer. The attack vector of the simulation entailed establishing an evil twin AP broadcasting an imitated SSID ("ARPSpoof") and managed to lured a wireless client into a man-in-the-middle (MitM) attack. Through the use of tools like a network sniffer, the attack demonstrated the ease with which susceptible traffic can be sniffed after the victim had joined the attack AP unknowingly.

Nevertheless, the simulation also highlighted how even foundational security controls — when properly configured — can mitigate such threats. By setting up the legitimate access point and client device with WPA2-PSK authentication and AES encryption, the network was able to harden against the rogue AP. The client terminal (PC0) would not be able to connect with the rogue access point unless it possessed the correct pre-shared key, which was securely set up to match only with the correct infrastructure. As exemplified with the browser test, the user could safely access the internal server and avoid the paths controlled by the adversary. This finding verifies that even in those settings lacking enterprise-grade security hardware, judicious tuning of what tools are available can make a huge difference in raising the barrier to entry for bad actors.

The results of the simulation verify the effectiveness of WPA2-PSK for mid and small-sized networks, especially with the inclusion of proper SSID setup and user awareness. All the same, the paper also experimented with the vulnerabilities of password-based protection — particularly in public areas — and explored more advanced methods introduced through research articles. Techniques like Wireless Intrusion Prevention Systems (WIPS), Channel State Information (CSI) analysis, position-based AP detection, Software-Defined Networking (SDN), and multi-agent detection systems all are robust and scalable methods against RAP attacks. Each

of these adds a further layer of context-aware validation or anomaly detection difficult for attackers to circumvent, especially when deployed in layered defense architectures.

Moreover, innovations such as certificate-based mutual authentication and infrastructure like the Robust Certificate Management System (RCMS) also address the underlying flaw WPA2-PSK can't: authentication verification of AP authenticity. Rather than relying upon SSID matching or pre-shared keys, these methods authenticate the identity of the access point using cryptographic certificates, which renders most impersonation-based attacks useless. Such systems are especially important in enterprise environments, university campuses, and public access, where open-access policy and large coverage areas render rogue AP deployment feasible and attractive to attackers.

Finally, this report emphasizes the need for an end-to-end and proactive wireless network security strategy. Organizations must look beyond default settings and adopt best practices not only in encryption and authentication but in monitoring, detection, and response as well. Layered security approaches combined — beginning with WPA2-PSK as the starting point and progressing to more advanced detection methods — enable wireless networks to function and be secure.

As wireless technology advances and goes out into applications such as IoT, edge computing, and smart infrastructure, the attack surface will inevitably grow. Future research and development will have to continue innovating on lightweight, scalable, and adaptive security paradigms. Education and awareness are also important; end users, administrators, and developers must be trained to recognize the signs of malicious activity and understand how to properly implement security configurations. Through good planning, continuous assessment, and focused investment in security technologies, organizations can build secure wireless ecosystems that can stand up to the evolving threat environment.

# References

Ampatzi, Christina. *Detection and Isolation of a Rogue Access Point*. Mälardalen University, 2021, mdh.diva-portal.org. Accessed 15 Apr. 2025.

Alotaibi, Bandar, and Khaled Elleithy. "Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions." *Wireless Personal Communications*, vol. 90, no. 4, 2016, pp. 1683–1700. Accessed 14 Apr. 2025.

Daldoul, Yousri, and Mouhebeddine Berrima. "A Robust Certificate Management System to Prevent Evil Twin Attacks in IEEE 802.11 Networks." *International Journal of Information Technology*, vol. 16, no. 2, 2024, pp. 123–134. Springer, https://doi.org/10.1007/s41870-024-02008-4. Accessed 13 Apr. 2025.

Liu, Wenjie, and Panos Papadimitratos. "Position-Based Rogue Access Point Detection." *arXiv preprint* arXiv:2406.01927, 2024. Accessed 14 Apr. 2025.

McGinniss, Irene. "The Identification of Rogue Access Points Using Channel State Information." *Montclair State University Theses*, 2023. Accessed 14 Apr. 2025.

Nazir, Rashid, et al. "Survey on Wireless Network Security." *Archives of Computational Methods in Engineering*, vol. 29, no. 3, 2022, pp. 1591–1610. Springer, https://doi.org/10.1007/s11831-021-09631-5. Accessed 13 Apr. 2025.

Sasane, Priyanka G., and S. K. Pathan. "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN: A Multi-Agent Sourcing Methodology." *International Journal of Sciences: Basic and Applied Research*, vol. 3, no. 1, 2011, pp. 9–15. Accessed 15 Apr. 2025.

Wexler, Joanie. "Security SaaS Hits WLAN Community." *Network World*, networkworld.com. Accessed 15 Apr. 2025.

Wikipedia contributors. "Wireless Intrusion Prevention System." *Wikipedia, The Free Encyclopedia*, 2024. Accessed 14 Apr. 2025.

Wolfe, Daniel. "Security Watch." *American Banker*, vol. 172, no. 31, 14 Feb. 2007, p. 7. ProQuest, https://www.proquest.com/docview/249873579. Accessed 14 Apr. 2025.

Wright, Joshua. "Issues with SSID Cloaking." *Network World*, 2007. Accessed 14 Apr. 2025.

Zheng, Xinyu, et al. "Accurate Rogue Access Point Localization Leveraging Fine-Grained Channel Information." *IEEE Conference on Communications and Network Security*, 2014, pp. 211–219. IEEE, https://doi.org/10.1109/CNS.2014.6997502. Accessed 13 Apr. 2025.

"What Is a Wireless Network?" *ExterNetworks*, https://www.extnoc.com/learn/general/wireless-network. Accessed 13 Apr. 2025.