



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

A Comprehensive Study on the Vulnerabilities and Mitigation Strategies on Network Switches for SMEs

by

Rohan Ravindra Chavan

2212517

Supervisor: Kapilan Radhakrishnan

Second Marker: Munyaradzi Nicholas Murira

Project submitted as part of the requirements for the award of MSc Computer Networks and
Cyber security

July 2024

Declaration

I, Rohan Ravindra Chavan declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :

Date : 05/07/2024

Form of Consent

I Rohan Ravindra Chavan hereby consent that my Project, submitted in candidature for the M.Sc. Computer networks and cyber security, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed  _____

Date 05/07/2024

Abstract:

This dissertation investigates critical vulnerabilities in network switches that pose significant security risks for Small and Medium-sized Enterprises (SMEs). The primary focus is on identifying and mitigating threats such as DHCP starvation, rogue DHCP servers, STP root takeover attacks, VLAN hopping, and ARP poisoning. These vulnerabilities, if left unaddressed, can lead to severe disruptions and unauthorized access within SME networks, highlighting the importance of robust and cost-effective security measures. To conduct this research, a comprehensive literature review was undertaken to identify common switch vulnerabilities and their potential impacts. This was followed by practical experiments and simulations to observe these vulnerabilities in real-world scenarios. The methodology included setting up a controlled network environment to test various attack vectors and implementing corresponding security measures to evaluate their effectiveness. The key findings of this research reveal that SMEs are particularly susceptible to the aforementioned attacks due to often limited resources and expertise in network security. However, the study also identifies several effective and cost-efficient mitigation strategies. These include port security, DHCP snooping, ARP spoofing prevention, BPDU guard, root guard, BPDU filter, and disabling the Dynamic Trunking Protocol (DTP). Each of these measures was tested and shown to significantly reduce the risk of network compromise while being affordable for SMEs. The implications of these findings are profound for SMEs. By adopting the recommended security measures, SMEs can enhance their network resilience against common attacks, thereby protecting sensitive data and ensuring business continuity. This research provides a practical guide for network administrators in SMEs to implement these security measures effectively and economically. In conclusion, this dissertation not only highlights the critical vulnerabilities in network switches but also offers actionable and cost-effective solutions to mitigate these risks. The subsequent sections of this report delve deeper into the technical details of each vulnerability, the methodology of the research, and the step-by-step implementation of the proposed security measures, providing a comprehensive resource for enhancing network security in SMEs.

Contents

1. CHAPTER 1: Introduction	7
1.1 Background and Context.....	7
1.2 Problem Statement	8
1.3 Research Aim and Objectives	9
1.4 Significance of the Study	10
1.5 Scope and Limitations.....	10
1.6 Structure of the Dissertation.....	11
1.7 Practical Application	11
2. CHAPTER 2: Literature Review.....	13
2.1 Introduction	13
2.2 Background and Context.....	13
2.2.1 Definition of SME	13
2.2.2 Challenges faced by SMEs	14
2.2.3 What are switches?	15
2.2.4 Benefits of Network Switches	16
2.2.5 Why Network Switches are Important for SMEs?	17
2.2.6 What protocols run on switches?	18
2.2.7 What are vulnerabilities on switches?.....	19
2.3 Network Protocols on Switches and their Vulnerabilities.....	19
2.3.1 Overview:.....	19
2.3.2 DHCP	20
2.3.3 Address Resolution Protocol (ARP).....	25
2.3.4 STP	30
2.3.5 Virtual Local Area Networks (VLAN).....	33
2.4 Conclusion.....	35
3. CHAPTER 3: Methodology	36
3.1 Introduction	36
3.2 Research Philosophy: Pragmatism	36
3.3 Research Approach: Deductive	37
3.4 Research Strategy: Experimental	37
3.5 Research Choice: Qualitative	37
3.6 Data Collection Methods.....	37
3.7 Conclusion.....	38
4. CHAPTER 4: Design, Implementation, Results and Analysis	39

4.1 Introduction	39
4.1.1 Main Device Specification:.....	41
4.1.2 Resource allocation:.....	41
4.1.3 Attack 1: DHCP Starvation attack and Rouge DHCP attack:	42
4.1.4 Attack 4: ARP Poisoning:	53
4.1.5 Attack 3: STP:.....	60
4.1.6 Attack 5: VLAN hopping:.....	64
4.1.7 Conclusion:	69
5. CHAPTER 5: Overall Discussion and Recommendations	70
5.1.1 Interpretation of Results	70
5.1.2 Recommendations	71
5.1.3 Broader Implications.....	72
6. CHAPTER 6: Conclusions.....	73
6.1.1 Introduction	73
6.1.2 How Aims and Objectives Were Achieved?	73
6.1.3 Limitations of the Study	74
6.1.4 Recommendations for Future Research	74
6.1.5 Reflection.....	74
6.1.6 Gannt Chart	76
7. References.....	77

1. CHAPTER 1: Introduction

1.1 Background and Context

Project Origin

The suggestion for this project on the security of network switches for small and medium-sized enterprises (SMEs) emerged from a combination of industry needs, academic gaps, and specific incidents that have underscored the critical importance of securing network infrastructure. Network switches, as central components of network architecture, are crucial for ensuring seamless communication and data transfer within a local area network (LAN). [1] The increasing frequency and sophistication of cyber-attacks, coupled with the growing reliance on digital infrastructure by SMEs, have highlighted significant vulnerabilities in network switches. [2] [3].

Previous Research

Several key studies and findings have laid the groundwork for this research project. A systematic review of SME cybersecurity literature from 2017 to 2023 identified common cyber threats and the controls adopted by SMEs to mitigate these risks. [6] Another study explored the challenges SMEs face in implementing effective information security management and proposed a holistic approach to address these issues. [7] delves into the vulnerabilities inherent in Layer 2 protocols and proposes various security measures to protect against common attacks [8] [9] [10] [11] [12]. These studies collectively underscore the necessity for focused research on the security of network switches in SMEs to bridge existing gaps and enhance protective measures.

However, there is a significant gap in the literature regarding the detailed mechanics of how attacks on network switches are executed. While many studies discuss the types of attacks and general mitigation strategies, few delve into the specific methods attackers use to compromise network switches. For instance, attacks such as MAC address flooding, DHCP spoofing, and VLAN hopping are often mentioned, but the detailed processes and techniques used by attackers to exploit these vulnerabilities are not thoroughly covered. Understanding these attack mechanics is crucial for SMEs, as it enables them to test their networks after applying mitigations, ensuring that the implemented security measures are effective. This gap underscores the necessity for focused research on the security of network switches in SMEs to bridge existing gaps and enhance protective measures. This revised section now

emphasizes the need for detailed research on the mechanics of attacks on network switches, highlighting the gap in existing literature and the importance of understanding these attacks for effective testing and mitigation by SMEs [13] [14].

Importance of the Problem

The security of network switches in SMEs is a critical issue with far-reaching implications for business operations, data protection, and the overall cybersecurity landscape. SMEs are often viewed as easier targets by cybercriminals due to their typically less robust security measures compared to larger corporations. [3] The financial and reputational damage resulting from cyber-attacks can be devastating for SMEs, potentially leading to significant financial losses, legal repercussions, and loss of customer trust. [4] [5] Moreover, regulatory requirements such as the General Data Protection Regulation (GDPR) impose strict data protection obligations on SMEs, making robust network security essential for compliance and avoiding substantial fines. [3] [4]

The impact of inadequate network security extends beyond individual businesses, as SMEs play a crucial role in the broader economy. They represent 99% of all businesses in the EU and employ around 100 million people, contributing significantly to the GDP. [5] Therefore, enhancing SME network security is not only vital for the survival and growth of these enterprises but also for maintaining the stability and security of the economic ecosystem they support.

In conclusion, the importance of SME network security cannot be overstated. It is essential for protecting sensitive data, ensuring business continuity, and maintaining customer trust. Addressing this issue through targeted research and practical solutions will help SMEs mitigate cyber risks and contribute to a more secure digital landscape.

1.2 Problem Statement

Broad Overview

Small and medium-sized enterprises (SMEs) face significant challenges in securing their networks against cyber threats. These challenges are exacerbated by limited resources, lack of expertise, and the increasing complexity of cyber-attacks.

Specific Issues

- **Resource Constraints:** SMEs often lack the financial and human resources to implement comprehensive network security measures. [15]
- **Lack of Expertise:** Many SMEs do not have dedicated IT staff or cybersecurity experts, making it difficult to identify and mitigate network vulnerabilities. [15]
- **Complexity of Threats:** The evolving nature of cyber threats, including ransomware, phishing, and advanced persistent threats, poses a significant challenge to SMEs. [15] [16]

Unsolved Aspects

The problem persists due to several gaps and limitations in current solutions:

- **Cost-Prohibitive Solutions:** Many advanced security solutions are too expensive for SMEs to implement and maintain. [15]
- **Lack of Awareness:** There is a general lack of awareness among SMEs about the specific network security threats they face and the potential impact of these threats. [15] [17]

1.3 Research Aim and Objectives

Overall Aim

The overall aim of this research is to improve network security for SMEs by analysing vulnerabilities in switch protocols, simulating network attacks, and developing cost-effective mitigation strategies.

Specific Objectives

- **Identify Vulnerabilities in Switch Protocols:** To identify and analyse the vulnerabilities in protocols run on network switches commonly used by SMEs.
- **Simulate Network Attacks:** (test)To simulate various network attacks that exploit these vulnerabilities to understand their mechanics and impact.
- **Develop Mitigation Strategies:** To develop and demonstrate cost-effective mitigation strategies that SMEs can implement without additional expenses.
- **Evaluate Mitigation Effectiveness:** To evaluate the effectiveness of these mitigation strategies in protecting against the identified network attacks.

Research Questions

Primary Research Question

What are the most effective cost-free strategies for mitigating network security vulnerabilities in switch protocols can be used by small and medium-sized enterprises?

Secondary Questions

- What are the common protocol vulnerabilities in network switches used by SMEs?
- How can network attacks exploiting these vulnerabilities be simulated to understand their mechanics and impact?
- What are the cost-effective mitigation strategies for SMEs to address these vulnerabilities?
- How effective are these mitigation strategies in protecting against network attacks without incurring additional costs?

1.4 Significance of the Study

This study aims to bridge the gap in securing network infrastructure for small and medium-sized enterprises (SMEs). It will achieve this by providing a focused analysis of vulnerabilities in network switch protocols, how these vulnerabilities are exploited in network attacks, and, crucially, how to mitigate these risks without requiring additional equipment. This will empower SMEs by offering a practical solution for implementing cost-effective network switch security, directly addressing their unique needs and resource constraints.

Practical Implications

For SMEs, the study will offer practical recommendations and a comprehensive security framework that can be implemented to enhance their network switches security. This will help SMEs protect their data, ensure business continuity, and comply with regulatory requirements.

1.5 Scope and Limitations

Scope

The research will focus on network security challenges and solutions for SMEs, including the identification of common threats, evaluation of current security measures, and development

of a tailored security framework. It will not cover other aspects of cybersecurity, such as physical security or broader information security management.

Limitations

The rapidly evolving nature of cyber threats may pose challenges in keeping the research findings up-to-date. Using of physical networking devices for experiment is not possible because of budget constraints.

1.6 Structure of the Dissertation

- **Chapter 2: Literature Review:** Summarizes existing research on SME network security and identifies gaps.
- **Chapter 3: Methodology:** Describes the research design, data collection, and analysis methods of the dissertation.
- **Chapter 4: Design, Implementation, Results and Analysis:** It covers various simulations, results and their analysis.
- **Chapter 5: Discussion:** Discusses key findings, implications, and recommendations.
- **Chapter 6: Conclusion:** Summarizes the study, its contributions, future research directions and reflection.

1.7 Practical Application

The project incorporates the practical application of security principles through the EVN-NG simulation tool. This industry-standard tool mirrors real-world network behaviour, allowing for the creation of a realistic network environment for testing and validating attack scenarios and countermeasures. Cisco equipment images will further enhance the realism of the testing environment. This hands-on approach ensures the proposed strategies not only meet theoretical best practices but also translate effectively into practical application for SMEs with limited resources. This effort extends beyond the immediate advantage of safeguarding a single SME's network. By pushing for an organized and thorough strategy, using industry best practices, and addressing vulnerabilities, the initiative serves as a useful resource for other organizations experiencing similar difficulties. The expected outcome is a well-documented and implementable network security strategy specifically tailored for SMEs. This strategy will provide clear guidelines, configurations, and

recommendations to secure network infrastructure, mitigate attacks, and protect valuable assets and data.

2. CHAPTER 2: Literature Review

2.1 Introduction

A report of government of UK from 2023 states that 5.51 million business were Small-sized and medium-sized were 36,900 Small employing 0 to 49 employees and 50 to 249 employees respectively [18]. A survey of 500 SME leaders in UK revealed that 36% small sized and 41% Medium-sized business are still using on-premises equipment [19]. University of Salford Manchester says “ 43% of cyber-attacks target SME businesses, and 60% of these SMEs that fall victims of a cyber-attack go out of business within six months” [20]. This vulnerability stems from the limited resources, expertise, and awareness that often plague SMEs. According to the "2024 Insider Threat Report" commissioned by Securonix, 76% of organizations reported experiencing insider attacks in 2024, which marks an increase from 66% in 2019. This data is based on a survey of 467 cybersecurity professionals, highlighting the growing concern and prevalence of insider threats over the past five years [21].

Due to the substantial increase in insider threats, it is imperative for small and medium-sized enterprises (SMEs) to prioritise strong cybersecurity measures, specifically at the Layer 2 (L2) level of their network infrastructure. L2 security is a critical aspect of local area network (LAN) security, as it pertains to the data link layer that facilitates node-to-node data transfer. This layer can be susceptible to different types of attacks, including those initiated by insider threats [22] [23].

2.2 Background and Context

2.2.1 Definition of SME

A popular definition of small and medium-sized enterprises (SMEs) is based on the number of workers and financial measures such as turnover or assets. However, the definition of SMEs may vary depending on the context and place in which it is being used. The term "small and medium-sized enterprises" (SMEs) is often understood to refer to businesses that have a turnover of less than fifty million euros and fewer than two hundred and fifty workers [24]. This definition has gained widespread acceptance inside the European Union and is in accordance with the criteria established by the European Commission [25].

According to the United States Small Business Administration, small and medium-sized enterprises (SMEs) are often classified as companies that have less than 500 workers in the

context of the United States [25]. This disagreement exemplifies the fact that definitions may vary greatly depending on the criteria used by different institutions and regions.

The European Commission's (2021) definition categorizes SMEs into three groups [25]:

- **Micro-firms:** Fewer than 10 employees
- **Small firms:** 10-49 employees
- **Medium-sized firms:** 50-249 employees

The establishment of these standards is essential for the formulation of policies and the provision of targeted assistance to these businesses, which are substantial contributors to economic development, the creation of new jobs, and innovation [26].

2.2.2 Challenges faced by SMEs

Several factors contribute to the challenges SMEs face in implementing L2 security measures:

- **Resource Constraints:** The high expenses that are associated with modern cybersecurity solutions are expensive, and small and medium-sized enterprises (SMEs) often operate with restricted budgets. The fact that they are limited financially makes it difficult for them to make investments in the essential security infrastructure and staff with the requisite skills [27] [28] [29].
- **Lack of Expertise:** There are a lot of small and medium-sized enterprises (SMEs) that do not have cybersecurity professionals on staff and instead depend on outside consultants or basic IT assistance, which may not be enough to deal with sophisticated cyber-attacks. The absence of this knowledge may result in insufficient security measures, which in turn can lead to an increase in susceptibility [27] [29].
- **Awareness and Training:** Security awareness among workers of small and medium-sized enterprises (SMEs) is often poor, and training programmes are either non-existent or inadequate. It is possible for human mistakes to jeopardise security, such as falling prey to phishing attempts or improperly managing sensitive information, as a consequence of this knowledge and preparation gap [29] [30].

- **Complexity of Security Solutions:** For small and medium-sized enterprises (SMEs), the complexity of installing and monitoring cybersecurity solutions may be intimidating. The majority of security frameworks and technologies are developed with huge corporations in mind, which makes it challenging for smaller organisations to adopt and maintain them [27] [28].
- **Insider Threat:**

Insider threats are cybersecurity risks that originate from within an organization, typically involving employees, contractors, or business partners who misuse their legitimate access to the organization's systems, data, or networks. These threats can be either intentional, such as malicious insiders seeking to harm the organization for personal gain or revenge, or unintentional, resulting from negligence or human error [31]. Insider threat agents can leverage switch vulnerabilities to exploit SMEs by taking advantage of their authorized access to introduce malicious code, escalate privileges, or exfiltrate sensitive data [1]. For instance, vulnerabilities like improper checks for exceptional conditions in network switches can be exploited by insiders to alter configurations, disrupt operations, or create backdoors for further attacks. [1] This exploitation is particularly damaging for SMEs, which often lack the robust cybersecurity infrastructure of larger organizations, making them more susceptible to such internal threats [32]. Survey of 467 cybersecurity professionals highlights 76% of organisations have reported an increase in the number of insider threats over the course of the previous five years; yet, fewer than 30% of those organisations think they are equipped with the appropriate tools to deal with these threats [21].

2.2.3 What are switches?

A network switch is a hardware device that connects devices on a computer network by using packet switching to receive and forward data to the destination device. It operates primarily at the data link layer (Layer 2) of the OSI model, but some advanced switches can also operate at the network layer (Layer 3), incorporating routing functionalities. A Content Addressable Memory (CAM) table is a memory architecture used by Ethernet switches. This architecture allows for the storage of a dynamic table that is used to associate the Media Access Control (MAC) addresses of devices with the ports they are connected to, as seen in the below figure.

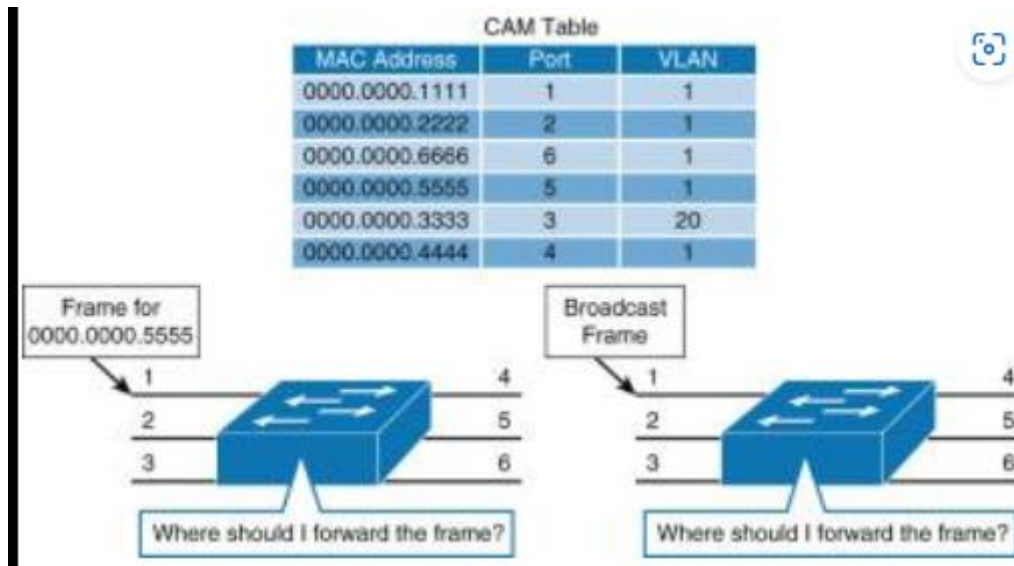


Figure 1Cam Table [33]

By avoiding the need to broadcast frames to all ports on the switch, this allows the switch to selectively transfer data directly to any connected device. The switch reads the frame header to get the destination MAC address of the target device. The switch thereafter matches the address with its CAM database and subsequently transmits the frame to the suitable device [11]. Network switches are essential components in local area networks (LANs), enabling multiple devices such as computers, printers, and servers to communicate efficiently and securely [34] [35].

2.2.4 Benefits of Network Switches

Network switches offer various benefits such as:

- **Increased Bandwidth and Performance:**

Switches increase the available bandwidth of the network by creating separate collision domains for each connected device. This reduces the likelihood of data collisions and improves overall network performance [34].

- **Enhanced Security:**

By using VLANs, switches can isolate sensitive data and restrict access to authorized users only. Managed switches also offer advanced security features such as port security, access control lists (ACLs), and intrusion detection systems (IDS) [34].

- **Efficient Data Transmission:**

Switches use MAC addresses to forward data only to the intended recipient, reducing unnecessary traffic and improving network efficiency. This targeted data transmission minimizes broadcast traffic and enhances the speed of data transfers [34].

- **Scalability and Flexibility:**

Modern switches support features like stacking and modular configurations, allowing networks to scale easily as the number of devices grows. This flexibility ensures that network infrastructure can adapt to changing business needs without significant overhauls [35].

- **Simplified Network Management:**

Managed switches provide tools for monitoring and managing network performance, such as SNMP and network analytics. These tools help administrators troubleshoot issues, optimize traffic flow, and maintain network health [35].

- **Redundancy and Reliability:**

Features like STP and link aggregation provide redundancy, ensuring that network services remain available even if a link fails. This redundancy is crucial for maintaining high availability in mission-critical environments [35].

Network switches are foundational to modern networking, offering robust performance, security, and manageability. They are indispensable in both small and large network environments, from home offices to enterprise data centres.

2.2.5 Why Network Switches are Important for SMEs?

A network switch is an essential component for SMEs (small and medium-sized enterprises) while establishing a business network. SMEs can leverage this technology to facilitate communication and information sharing inside a local area network (LAN), linking people and devices within a certain geographic location, such as an office, department, or building. This promotes collaboration and provides access to crucial company information [36].

The importance of investment networks has increased for most small and medium-sized businesses after the COVID-19 epidemic. To effectively distinguish your company and improve staff efficiency while promoting greater cooperation both internally and with

business partners, it is essential to carefully evaluate and invest in a network switch that aligns with present requirements and accommodates future expansion [36].

2.2.6 What protocols run on switches?

Small and Medium-sized Enterprises (SMEs) often rely on a variety of networking protocols to ensure efficient, secure, and scalable network operations. Here are some of the most commonly used protocols:

- **VLAN (Virtual Local Area Network):**

VLANs allow network administrators to segment a physical network into multiple logical networks. This segmentation improves security and performance by isolating traffic within each VLAN. VLANs are configured using protocols like IEEE 802.1Q, which tags Ethernet frames with VLAN identifiers [37].

- **STP (Spanning Tree Protocol):**

STP is used to prevent network loops in Ethernet networks. It ensures a loop-free topology by selectively setting links to standby mode. Variants like Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) offer enhanced performance and scalability [38].

- **DHCP (Dynamic Host Configuration Protocol):**

DHCP automates the assignment of IP addresses, subnet masks, gateways, and other IP parameters. This protocol simplifies network management by dynamically assigning IP addresses to devices on the network, reducing the need for manual configuration [37].

- **QoS (Quality of Service)**

QoS protocols prioritize certain types of network traffic to ensure that critical applications receive the necessary bandwidth. This is crucial for SMEs that rely on VoIP, video conferencing, or other latency-sensitive applications [37].

These protocols collectively ensure that SMEs can maintain efficient, secure, and scalable network operations, catering to their specific needs and resource constraints.

2.2.7 What are vulnerabilities on switches?

As many as features come along with network switches, multiple manufacturers of network switches, cybersecurity professionals, and government agencies have highlighted that network switches are vulnerable to various types of cyberattacks. These attacks exploit the fundamental operations of switches to disrupt network functionality and compromise data integrity. For instance, DHCP spoofing involves an attacker responding to DHCP requests with fake responses, potentially redirecting network traffic through malicious devices. STP attacks can manipulate the spanning tree protocol to create network loops or designate rogue devices as root bridges, leading to network instability. VLAN hopping allows attackers to access multiple VLANs by exploiting trunk port configurations, thereby bypassing network segmentation and gaining unauthorized access to sensitive data. These vulnerabilities underscore the critical need for robust security measures to protect network infrastructure from sophisticated cyber threats [39] [40] [41] [42].

2.3 Network Protocols on Switches and their Vulnerabilities

2.3.1 Overview:

Several networking manufacturing companies and research studies have brought to light the fact that Layer 2 (L2) attacks may be carried out against a variety of network protocols [39] [40] [41].

In this part, we will investigate these protocols in further detail. We are going to investigate the following different elements of each protocol:

Overview of the Protocols: A concise introduction to the protocol, providing an overview of its fundamental purpose as well as its relevance in the functioning of the network.

Operational mechanism: A detailed description of how the protocol operates, including the communication mechanisms and important components that are involved.

Vulnerabilities: In this section, we will conduct an examination of the specific vulnerabilities that are intrinsic to the protocol, with a particular emphasis on the ways in which these flaws might be exploited by attackers.

Mitigation Strategies: A description of the different methods and best practices that can be

used to mitigate the vulnerabilities that have been found and to improve the security of the protocols.

By investigating these components, we want to get a full knowledge of the dangers that are connected to these protocols as well as the precautions that may be taken to safeguard the network infrastructures of small and medium-sized enterprises (SMEs) against the possibility of L2 attacks.

2.3.2 DHCP

The Dynamic Host Control Protocol is a client-server protocol that assists hosts connected to a network in obtaining the appropriate network configurations. These parameters contain the IP address, default gateway, DNS address, and other settings. These setups are essential for network connectivity of internal and external hosts. The client component of this protocol is supposed to be implemented by any network host that wants network settings without human input. One or more specialised DHCP servers in the system will then give clients with specific network configurations after receiving the requests. The lease time is the duration for which these configurations are effective. However, the configurations must be renewed upon the expiration of the lease time [43].

Small and Medium Enterprises (SMEs) face IT challenges such as limited resources, cybersecurity risks, and the need for scalable solutions. Dynamic Host Configuration Protocol (DHCP) addresses these issues by automating IP address assignment, centralizing network management, and enhancing security. This reduces IT overhead, lowers costs, and supports network scalability, making DHCP a valuable tool for SMEs [44].

The growth of the Internet of Things (IoT) and smart personal gadgets has increased the requirement to provide them with network parameters and IP addresses [45]. Although vital, the Dynamic Host Configuration Protocol (DHCP) was not originally created with security in mind. Several vulnerabilities were revealed, and the attackers utilised them to launch several attacks [10].

However, DHCP protocol has inherent issues. DHCP's biggest drawback is that the server and client can't verify each other's identities and can't ensure the other node's authenticity. UDP packets used by DHCP are likewise preserved in plaintext. Attackers may launch several attacks against DHCP due to its weaknesses [46], [47]. These weaknesses let

attackers bypass security. Numerous studies [48]- [49] have investigated the security of the DHCP protocol.

2.3.2.1 – How Does DHCP operate?

There are two versions of DHCP, DHCPv4 and DHCPv6 are used for IPv4 and IPv6, respectively [50]. This article will focus on DHCPv4. DHCP operation is shown in below figure.

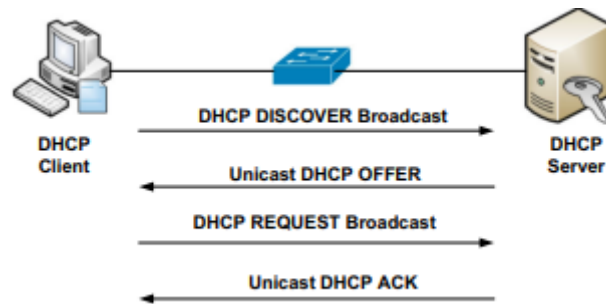


Figure 2 DHCP Operations [47]

DHCP uses well known UDP port 67 and 68, where The DHCP server listens on UDP port 67 for incoming requests from clients and the DHCP client sends requests to the DHCP server on UDP port 67, with the source port being 68 [51].

2.3.2.2 DHCP Communication Process [51]:

- **DHCPDISCOVER**: The client broadcasts a DHCPDISCOVER message on network from UDP port 68 to UDP port 67.
- **DHCPOFFER**: The server responds with a DHCPOFFER message in which it offers an IP address and other configurations from UDP port 67 to UDP port 68.
- **DHCPREQUEST**: The client selects one of the offers and broadcasts a DHCPREQUEST message from UDP port 68 to UDP port 67, requesting the offered IP address
- **DHCPACK**: The selected DHCP server acknowledges the request by sending a DHCPACK message from UDP port 67 to the client's UDP port 68, confirming the IP address assignment.

2.3.2.3 DHCP Vulnerabilities

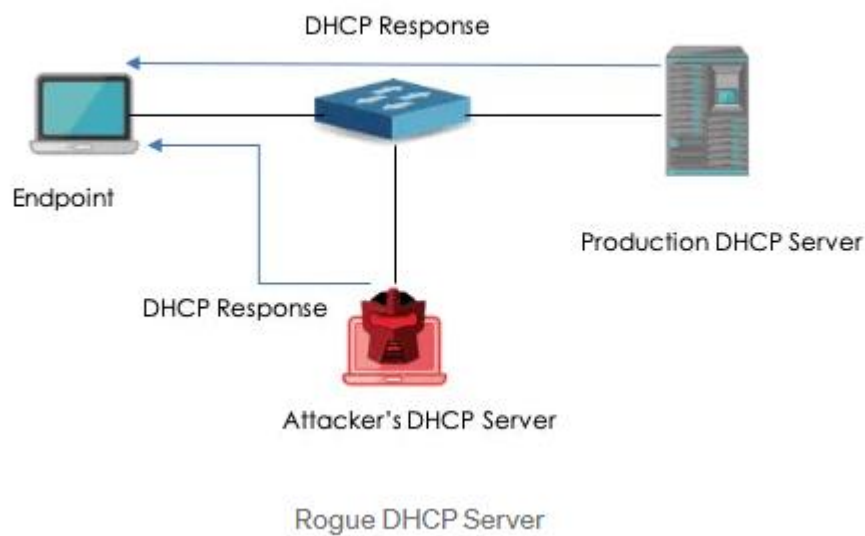
The DHCP protocol suffers from several critical vulnerabilities due to the lack of authentication, confidentiality, and integrity mechanisms [52]. Without authentication, malicious nodes can inject DHCP packets, posing as legitimate servers or clients to control the network state, leading to attacks like DHCP starvation and spoofing [47]. The absence of confidentiality means that DHCP packets are broadcasted in cleartext, making them susceptible to being read and altered by unauthorized nodes, which can result in MITM attacks and rogue DHCP server attacks [46]. Additionally, the lack of integrity checks allows attackers to capture and modify DHCP packets, perform replay attacks, and spoof MAC addresses to launch further attacks, such as DHCP starvation. These vulnerabilities collectively place network administrators in challenging situations to mitigate these threats effectively. [53]

2.3.2.4 Different attack mechanisms on DHCP

DHCP starvation

An attacker will flood a DHCP server with a large number of fake DHCP DISCOVER packets in order to carry out a DHCP starvation attack onto the service. This puts the service open to the possibility of being attacked. Because each one of these packets makes use of a fabricated source MAC address, the DHCP server is led to believe that there are a significant number of new clients who are looking for more IP addresses based on this assumption. As the server works to respond to these requests, it quickly exhausts all of the IP addresses that are available to it. Genuine clients are unable to get IP addresses after all of the available IP addresses in the pool have been used and this also results in mac-flooding attack on the switch, which leads to a situation known as a denial of service(DOS) [54].

DHCP Rouge server



Once depleting all the ip addresses from the DHCP pool by doing the DHCP starvation attack, the attacker can introduce DHCP Rouge server [55]. This will provide the consumers with a fake IP address, Subnet mask, Gateway, and Domain name without the clients being aware of the fact that they are receiving these things. This server continues to listen to each and every DHCP discovery packet that is sent to it. As soon as it is able to receive the DHCP discover, it instantly sends the DHCP Offer to the machine that is being victimised and provides it the IP address that is linked with the network that the attacker has selected [56]. Which means that victims will under Man in the middle(MITM) attack as well as the traffic will be transversing via the rouge DHCP server [52].

2.3.2.5 Existing solution for mitigating DHCP starvation and rouge server

A digital certificate-based approach involves using the DHCP server's private key to sign messages, which clients can verify using the public key. However, this method requires manually installing certificates on each client, posing a problem if the certificates are compromised [57].

In another paper proposed a measurement inconsistent discrete event system (MIDES) framework with an Intrusion Detection System (IDS) to detect rogue DHCP servers using a dummy client. Their evaluation, however, was limited to a small-scale simulation analysis and lacked a detailed evaluation of the mechanism for DHCP attacks [58].

A Kerberos-based solution was proposed long ago but never became an RFC due to the complexity of requiring additional components like an authentication server and ticket-granting server [59].

DHCP snooping is a security feature that can be implemented on network switches to prevent DHCP attacks [60]. It works by monitoring DHCP messages and ensuring that only trusted DHCP servers can respond to DHCP requests. This technique helps mitigate both DHCP starvation and rogue DHCP server attacks by filtering out malicious DHCP traffic and ensuring that only legitimate DHCP servers can allocate IP addresses [61]. A study published in the "ACM International Conference Proceeding Series" discusses the implementation of DHCP snooping to mitigate DHCP starvation attacks, demonstrating its effectiveness in securing network environments [62]. Cisco's white paper on DHCP snooping explains how it acts as a firewall between untrusted hosts and trusted DHCP servers, validating DHCP messages and maintaining a binding database to prevent unauthorized IP address assignments. [61]

Port security is another method used to prevent DHCP starvation attacks. By configuring port security on network switches, administrators can limit the number of MAC addresses that can be learned on a single port. This prevents attackers from flooding the network with DHCP requests using spoofed MAC addresses, thereby mitigating DHCP starvation attacks [63] [64]. Cisco's documentation outlines the benefits of port security, including preventing unauthorized devices from accessing the network, mitigating MAC address flooding attacks, and ensuring network reliability and availability [65].

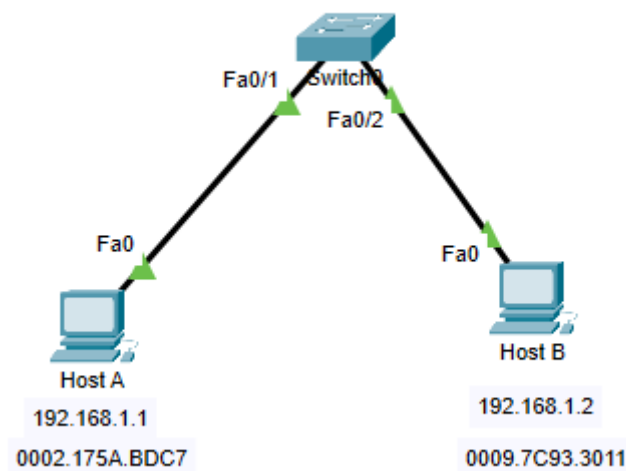
From various research papers and industry white papers, it is evident that DHCP snooping, and switch port security are widely adopted and effective solutions for enhancing network security [60] [61]. Combining DHCP snooping with port security provides a robust defence against DHCP-related attacks. DHCP snooping ensures that only trusted DHCP servers can operate, while port security limits the potential for MAC address spoofing and excessive DHCP requests, effectively preventing both DHCP starvation and rogue server attacks [63].

These solutions are standard features in enterprise-grade switches from major vendors like Cisco and Juniper, indicating their widespread adoption in the industry for corporate networks, educational institutions, and data centres [60] [61] [66].

2.3.3 Address Resolution Protocol (ARP)

The Address Resolution Protocol, more frequently referred to as ARP, is a network protocol that is used in a local area network (LAN) to map an Internet Protocol (IP) address to a physical machine address. This address is also sometimes referred to as a Media Access Control (MAC) address. It is necessary for a device to be aware of the MAC address that is linked with the IP address of the target device in order for it to be able to interact with another device that is connected to the same network [67].

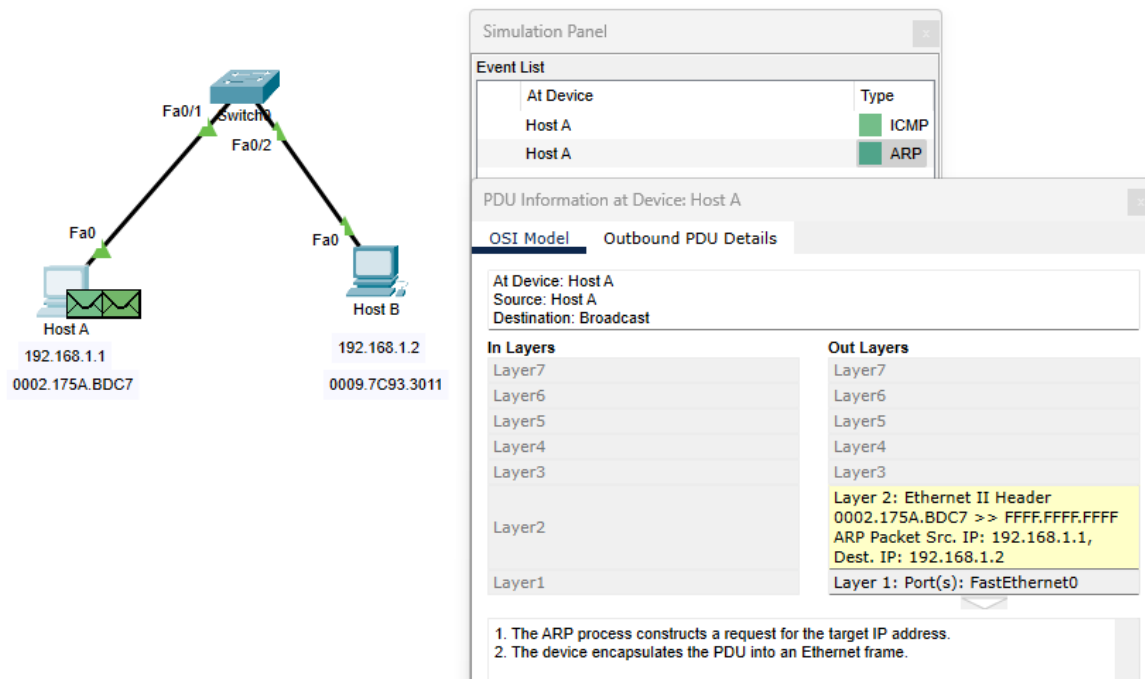
2.3.3.1 ARP Process [68]



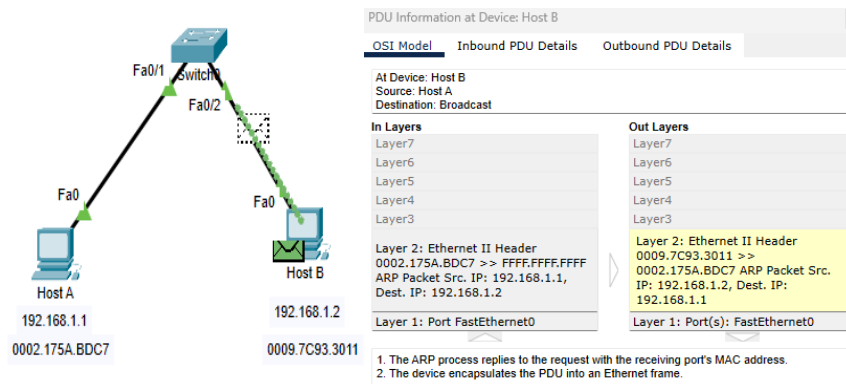
As shown in the figure above, I have taken two PCs, Host A (MAC address: 0002.175A.BDC7) and Host B (MAC address: 0009.7C93.3011), on Cisco Packet Tracer with their IP addresses 192.168.1.1 and 192.168.1.2, respectively. Both hosts are connected via a switch. When I initiate a ping command from Host A to Host B, Host A is initially unaware of Host B's MAC address, as shown in the figure below.

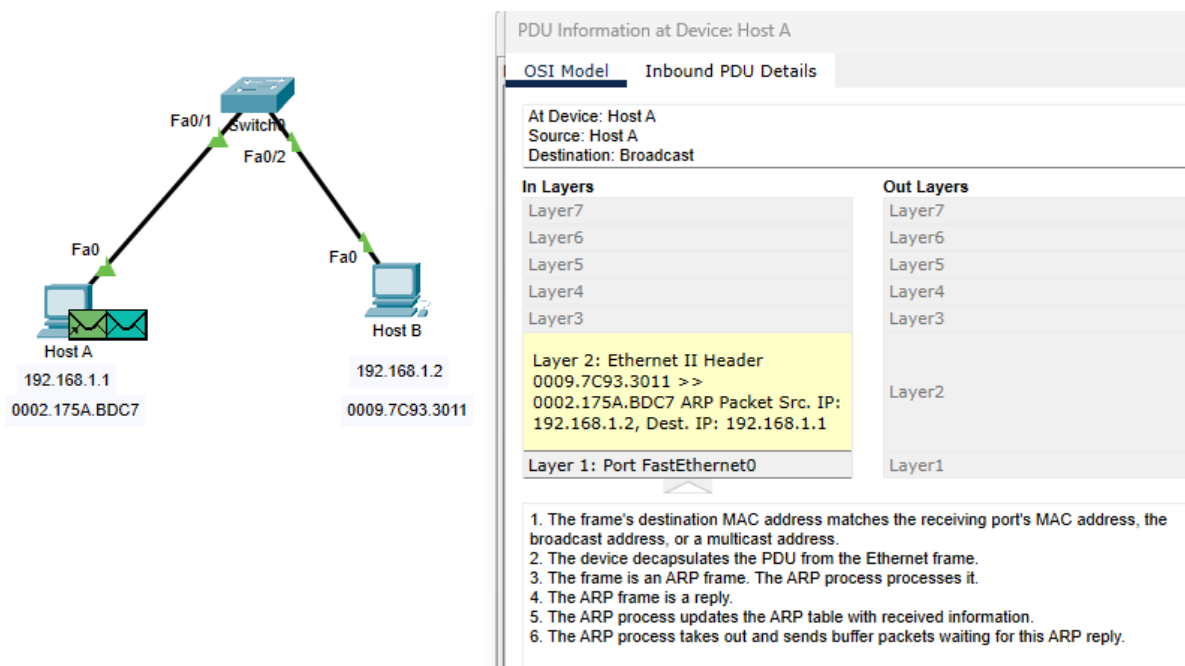
```
C:\>arp -a
No ARP Entries Found
```

Host A broadcasts an ARP request to the address FFFF.FFFF.FFFF, as you can see in the figure below.



In the following figure, you can see that Host B replies to the ARP request from Host A.





Once Host A receives the reply to the ARP request, it adds the MAC address and its associated IP address to the ARP table, as shown in the figure below.

```
C:\>
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.2          0009.7c93.3011       dynamic
```

2.3.3.2 ARP Spoofing

When an attacker sends faked ARP packets over a local network from their own computer, they are engaging in a kind of cyber-attack known as ARP spoofing, which is also sometimes referred to as ARP poisoning. The result of this is that the (MAC) address of the attacker is associated with the (IP) address of a real computer or server that is connected to the network. The attacker can intercept, alter, or block data that is meant for a victim's IP address once the attacker's MAC address has been connected with victim's IP address [67] [68]. This can lead to several types of attacks, including:

Session Hijacking: The attacker can take over an active session between two devices by intercepting and manipulating the data packets [67].

Man-in-the-Middle (MITM) Attacks: The attacker can intercept and potentially alter the data being transmitted between two devices. Which is also highlighted in CVEs (Common Vulnerabilities and Exposures) **CVE-1999-0667** [69].

Denial of Service (DoS): As shown in **CVE-2023-31190**, the attacker can disrupt the communication between devices by associating non-existent MAC addresses with IP addresses, causing the network traffic to be misrouted or dropped [70].

There have been instances of ARP poisoning being used to break into internal networks in business settings. Using ARP spoofing, for example, an attacker inside a corporate network was able to divert traffic via their computer, which gave them the ability to steal sensitive company conversations and data. When it comes to securing sensitive company information, this kind of assault highlights how important it is to have comprehensive network security procedures [71].

2.3.3.3 Mitigation Techniques for ARP poisoning

Static ARP Entries: When static ARP entries are manually configured in the ARP cache, it is possible to prevent unauthorised modifications from occurring. On the other hand, this approach cannot be scaled up to accommodate enormous networks [9] [72].

Cryptographic Techniques: It is possible to avoid spoofing by authenticating ARP communications via the use of cryptographic technologies. Secure ARP, often known as S-ARP, is a method that verifies the validity of ARP messages by using public and private key pairs but this is also not scalable as this should be available across all devices running on the network [73] [74].

ARP Spoofing Detection Tools: Monitoring ARP traffic and alerting administrators to potentially malicious behaviour may be accomplished with the use of tools such as ARPwatch and XARP, amongst others [75] [74] [76].

Routing Trace: The key disadvantages of DS-ARP include its complexity and the ongoing maintenance required, which can add significant overhead to network management. Continuous monitoring introduces performance overhead, potentially slowing down network operations, especially in larger environments. There is also a risk of false positives and negatives, leading to unnecessary alerts or undetected attacks. Compatibility issues can arise when integrating DS-ARP into diverse network environments, and scalability concerns become prominent in large networks due to increased ARP traffic. Additionally, the resource consumption associated with continuous monitoring and analysis can impact overall network performance. These factors must be carefully considered to ensure that the benefits of implementing DS-ARP outweigh its drawbacks. [75] [77].

DHCP Snooping is a security feature that monitors and controls DHCP traffic on a network. It classifies switch ports into trusted and untrusted categories [78]:

- **Trusted Ports:** These are typically connected to legitimate DHCP servers and are allowed to send DHCP server messages [78].
- **Untrusted Ports:** These are connected to clients and are restricted from sending DHCP server messages [78].

When DHCP snooping is enabled, the switch:

- **Validates DHCP Messages:** It inspects DHCP messages from untrusted sources and filters out invalid ones [78].
- **Maintains a DHCP Snooping Binding Table:** This table records the MAC address, IP address, lease time, VLAN, and interface information for each DHCP lease. This database is crucial for subsequent validation [78].

Dynamic ARP Inspection (DAI) is a security feature that protects against ARP spoofing attacks by validating ARP packets on the network. DAI uses the DHCP snooping binding table to verify the integrity of ARP packets [79]:

- **Intercepts ARP Packets:** DAI intercepts ARP requests and responses on the network [79].
- **Validates ARP Packets:** It compares the MAC and IP address information in ARP packets against the entries in the DHCP snooping binding table. If an ARP packet's information does not match a valid entry, the packet is dropped [79].

Integration of DHCP Snooping and DAI [80]

The integration of DHCP Snooping and DAI provides a robust defence mechanism against network attacks:

- **DHCP Snooping** ensures that only legitimate DHCP traffic is allowed, preventing rogue DHCP servers from assigning IP addresses.
- **DAI** uses the DHCP snooping binding table to validate ARP packets, preventing ARP spoofing attacks.

Together, these features create a layered security approach:

- **First Layer - DHCP Snooping:** Ensures that IP addresses are correctly assigned by legitimate DHCP servers and maintains a binding table of valid IP-to-MAC address mappings.
- **Second Layer - DAI:** Uses the binding table to validate ARP packets, ensuring that ARP requests and responses are legitimate and consistent with the DHCP snooping database.

A popular vendor in networking industry, recommends using a combination of DHCP Snooping, Dynamic ARP Inspection (DAI), and Port Security to collectively prevent ARP poisoning attacks. DHCP Snooping builds a database of IP-to-MAC bindings by monitoring DHCP traffic, which DAI then uses to validate ARP packets, ensuring that only legitimate ARP requests and responses are processed. Port Security further enhances protection by limiting the number of MAC addresses that can connect to a port, preventing unauthorized devices from accessing the network. These features are built into most business-grade switches, providing a cost-effective solution for small and medium-sized enterprises (SMEs) without additional costs. This integrated approach not only mitigates ARP spoofing but also enhances overall network security [81].

2.3.4 STP

Loops in Ethernet networks, and more specifically in Local Area Networks (LANs), are avoided with the use of a network protocol known as the Spanning Tree Protocol (STP). This protocol is turned on by default all network switches by vendors. STP was intended to solve problems that might arise in a network when redundant routes are present. These problems include broadcast storms, MAC table instability, and multiple frame transmission. STP was developed to overcome these problems in which a switch is elected as central point reference for all switches, also known as root bridge [82].

2.3.4.1 How STP works?

- **Root Bridge Election:**

The selection of a root bridge is the first stage in the functioning of the STP protocols. All of the switches in the network first believe themselves to be the root bridge, and they begin broadcasting Bridge Protocol Data Units (BPDUs) that include their Bridge ID. This Bridge ID is a mix of their priority and their MAC address. The root bridge is determined to be the switch that has the lowest Bridge ID total [82].

- **Path Cost Calculation:**

The route cost, which is determined by the bandwidth of the connections, is used by all of the other switches to determine the shortest way to the root bridge after the root bridge has been chosen [45].

- **Port Roles Assignment:**

Each switch assigns roles to its ports:

1. **Root Port:** The port with the lowest path cost to the root bridge.
2. **Designated Port:** The port on each network segment that has the lowest path cost to the root bridge.
3. **Blocked Port:** Ports that are neither root nor designated ports are put into a blocking state to prevent loops.

- **BPDU Exchange:**

Switches exchange BPDUs every 2 seconds by default to maintain the network topology. BPDUs contain information about the root bridge, path costs, and port roles. This helps in detecting any changes in the network and recalculating the spanning tree if necessary.

- **Port States:**

STP ports transition through several states to prevent loops during topology changes:

1. **Blocking:** The port does not forward frames and only listens to BPDUs.
2. **Listening:** The port prepares to forward frames but does not yet learn MAC addresses.
3. **Learning:** The port learns MAC addresses but does not forward frames.
4. **Forwarding:** The port forwards frames and continues to learn MAC addresses.
5. **Disabled:** The port is administratively shut down and does not participate in STP.

2.3.4.2 STP vulnerabilities

STP has several vulnerabilities that can be exploited by attackers. Here are some key points on STP vulnerabilities:

- **Lack of Authentication:**

As a result of the fact that the Spanning-tree Protocol (STP) does not natively incorporate authentication procedures, it is susceptible to attacks in which malicious users may attempt to alter the topology of the network. An example of this would be a threat transmitting Bridge Protocol Data Units (BPDUs) with a lower bridge ID in order to establish themselves as the

root bridge. The topology of the network would be changed as a consequence of this, which might potentially result in disruptions that damage the network [83] [84].

- **BPDU Manipulation:**

By sending bogus BPDUs, attackers may take advantage of the fact that there is no authentication for BPDUs. This can result in the root bridge being selected from among the switches that have been hacked. Consequently, this may lead to loops in the network, a decrease in performance, or even total network failures [83] [84].

- **Denial of Service (DoS) Attacks**

An attacker may utilise STP to carry out a denial-of-service attack by sending a large number of BPDUs. This would be feasible for the attacker to do. Because of this, the network is forced to undergo configuration changes on frequently, which in turn leads the network to become unstable and suffer outages [83] [84].

2.3.4.3 Mitigation Strategies

BPDU Guard:

When BPDU Guard has been configured on edge ports , it is possible to prevent unauthorised devices from sending BPDUs into the network. When a BPDU is received on a port that has BPDU Guard active, the port will be immediately shut down [83] [84].

Root Guard:

In order to prevent ports from ever becoming the root port, Root Guard may be activated on such ports. When a superior BPDU is received on a port that has Root Guard enabled, the port is put into a root-inconsistent state. This prevents the port from becoming the root port [83] [84].

BPDU Filtering: It eliminates the potential of STP manipulation by preventing BPDUs from being transmitted or received on certain ports. This eliminates the possibility of STP manipulation [85].

Various industry standards emphasize the importance of implementing security measures such as BPDU Guard, Root Guard, and BPDU Filtering to protect against Spanning Tree Protocol (STP) attacks. For instance, cisco's Enhance Spanning Tree Protocol (STP) with Root Guard, includes the use of BPDU Guard to prevent unauthorized devices from sending

BPDUs into the network, thereby shutting down compromised ports immediately [86]. Similarly, the Hewlett Packard Enterprise underscores the importance of BPDU filtering on per-port basis [87]. These strategies are widely endorsed to safeguard network infrastructures from malicious STP attacks, and these should be enabled on all ports where end devices are connected.

2.3.5 Virtual Local Area Networks (VLAN)

VLANs partition a physical network into distinct logical networks. This enables devices to establish communication as if they were connected to the same network, regardless of their physical location. VLANs enhance network performance, increase security, and management [88].

VLANs partition networks into separate segments, organise devices across different locations, and confine broadcast traffic. This leads to a decrease in traffic congestion and enhances overall security. VLANs provide the advantageous qualities of flexibility and scalability, making them highly suitable for dynamic contexts.

Small and medium-sized enterprises (SMEs) get several advantages from using virtual local area networks (VLANs). VLANs save expenses by using pre-existing hardware for the purpose of logical segmentation. They enhance network performance by mitigating congestion. VLANs improve security by segregating departments and operation [89].

On a network switch, a trunk port is a specialised type of port that is designed to handle data traffic for several Virtual Local Area Networks (VLANs) by encapsulating the traffic with unique VLAN tags. This allows the trunk port to fulfil its purpose of managing data traffic. The simultaneous transmission of numerous virtual local area networks (VLANs) across a single physical connection between switches or other network devices is made possible on account of this [90].

2.3.5.1 VLAN Vulnerabilities

VLAN Hopping: Also known as switch spoofing, is an attack that involves taking advantage of a vulnerability in physical Cisco switches that make use of the proprietary Dynamic Trunking Protocol (DTP) in order to automatically negotiate trunk connections between

switches. This vulnerability gives the attacker the opportunity to exploit the vulnerability and take advantage of it. With the great majority of older Cisco switches, DTP is activated by default on all ports straight out of the box. This is a standard feature that is included in Cisco switches [91]. SMEs can go for older equipment due to budget constraints [92]. This allows trunk links to be formed automatically and with convenience. In the event that the switch's physical ports are left in the dynamic preferred mode, an attacker has the ability to connect a machine to a Cisco switch by using any of the available ports on the switch. Using this method, the attacker is able to deceive the switch into thinking that the hacked system is another switch that is seeking to negotiate a trunk connection. If the attack is successful and a trunk connection is created, the attacker will have access to all the virtual local area networks (VLANs) that are linked with the trunk. Under these circumstances, the system of the attacker will be able to get access to any system that is located on any virtual local area network (VLAN). Extensive evidence of this attack, which was successfully carried out against physical networks, has been presented by past study that was carried out by Cisco and the SANS Institute [93].

2.3.5.2 Mitigating VLAN hooping [94]

Cisco recommends disabling DTP on interfaces where trunking is not needed. This can be done by setting the interface to access mode and using the “switchport nonegotiate” command to prevent DTP frames from being sent. This ensures that the interface does not attempt to negotiate trunking.

Second, for interfaces that require trunking, configure them statically. Set the interface to trunk mode and disable DTP negotiation by using the “switchport nonegotiate” command. This prevents the interface from participating in DTP negotiations while still allowing trunking.

Third, always set interfaces to access mode if trunking is not necessary. This prevents the interface from becoming a trunk port even if it receives DTP frames, enhancing security by ensuring that the interface remains in access mode.

Lastly, regularly monitor and audit switch configurations to ensure that DTP settings are correctly applied, and that no unauthorized trunk links are formed.

By implementing these strategies, network administrators can reduce the risk of unauthorized trunk formation and enhance network security.

2.4 Conclusion

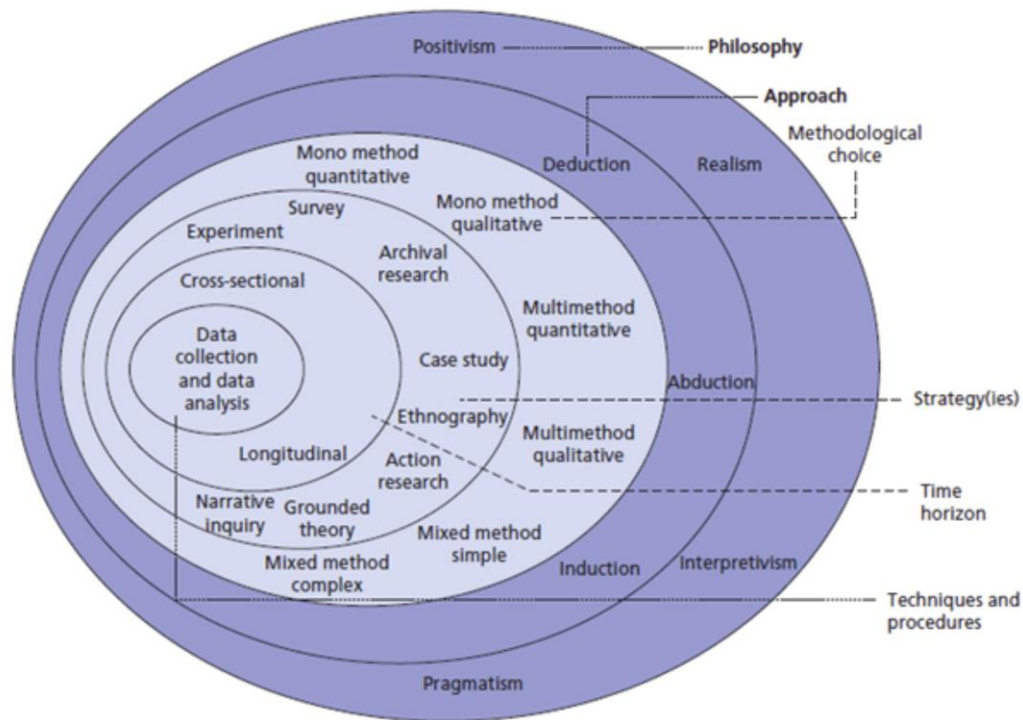
In this chapter, we have explored the critical role of Small and Medium-sized Enterprises (SMEs) in the global economy, the benefits that network switches bring to these enterprises, the inherent vulnerabilities associated with network switches, and the strategies to mitigate these vulnerabilities.

Based on the literature review, the chapter 4 will focus on conducting simulations to validate the findings and recommendations discussed. These simulations will provide practical insights into the effectiveness of various mitigation strategies and help in developing a comprehensive security framework for SMEs. By understanding the benefits and vulnerabilities of network switches and implementing appropriate security measures, SMEs can leverage technology to drive growth while safeguarding their digital assets.

3. CHAPTER 3: Methodology

3.1 Introduction

This chapter outlines the research methodology employed in this study on switch security, focusing on SMEs. The research design is structured using research Onion framework, which provides a comprehensive approach to research methodology.



Research Onion [95]

3.2 Research Philosophy: Pragmatism

Pragmatism is a philosophical tradition that emphasizes the practical application of ideas and the use of empirical evidence to inform decision-making. In the context of this research, pragmatism underpins the approach by focusing on the practical implications and outcomes of the study. Pragmatism asserts that truth and knowledge are best understood through their practical effects and usefulness in addressing real-world problems [95]. This philosophy aligns with the study's aim to explore and mitigate L2 attacks through practical experimentation and qualitative analysis.

3.3 Research Approach: Deductive

The deductive research approach involves starting with a general theory or hypothesis and then designing a research strategy to test this hypothesis [96]. This study begins with existing theories on network switch attacks and their mitigation strategies. Hypotheses are formulated based on these theories, and the experimental research strategy is designed to test these hypotheses. The deductive approach ensures that the research is grounded in established knowledge and systematically tests the validity of the hypotheses through empirical observation and analysis.

3.4 Research Strategy: Experimental

Experimental research is chosen as the strategy as the goal of the study is to examine cause-effect relationships [97]. This simulation-based approach to analyse various network switch attacks. The simulations leveraged tools like Ettercap for simulating man-in-the-middle attacks, Yersinia for DHCP starvation, Rogue DHCP and STP, and Wireshark for network traffic capture and analysis. These simulations demonstrate the impact of these attacks and evaluate the effectiveness of potential mitigation strategies. This approach allows for a detailed examination of the attack vectors and the potential effectiveness of mitigation strategies in a controlled setting.

3.5 Research Choice: Qualitative

Despite the experimental strategy typically being associated with quantitative methods, this study employs a qualitative research choice. Qualitative research is concerned with understanding phenomena from the perspective of the participants and the context in which they occur [98]. In this study, qualitative data is collected to gain deeper insights into the nature of network switch attacks, the effectiveness of mitigation strategies. This approach allows for a richer, more nuanced understanding of the research problem.

3.6 Data Collection Methods

Data for this study is collected from a variety of sources, including peer-reviewed articles, journals, industry documents, and government documents. These sources provide a comprehensive foundation for understanding switch attacks and mitigation strategies. The data collection process involves:

- **Literature Review:** Conducting a thorough review of existing literature on switch attacks and mitigation strategies to inform the experimental setup and provide context for the study.
- **Document Analysis:** Analysing industry reports and government documents to gather relevant information and data on current practices and policies related to switch attacks.
- **Peer-Reviewed Articles and Journals:** Reviewing academic articles and journals to identify key theories, findings, and gaps in the existing research.

3.7 Conclusion

The methodology chapter outlines a comprehensive approach to studying L2 attacks and mitigation strategies through a pragmatic, deductive, experimental, and qualitative framework. By combining these elements, the research aims to provide practical, evidence-based insights that can inform and improve strategies for mitigating L2 attacks.

4. CHAPTER 4: Design, Implementation, Results and Analysis

4.1 Introduction

In this chapter, we delve into the comprehensive process of designing, implementing, and evaluating security measures at Layer 2 (L2) within a simulated network environment tailored for Small and Medium-sized Enterprises (SMEs). The chapter begins by outlining the design requirements and processes that underpin the network topology and security architecture. It provides a comprehensive overview of the hardware and software employed to create the controlled virtual lab environment, mimicking a real-world network.

Leveraging insights from the literature review, we systematically conduct a series of L2 attacks on network switches, which include MAC Flooding, DHCP Starvation, Rouge DHCP server, VLAN Hopping, ARP Spoofing and STP Manipulation. Step-by-step procedures guide you through the configuration process and the implementation of various attack simulations. Detailed explanations of commands and tutorials are included to ensure a clear understanding of the attack mechanisms. Each attack is meticulously executed to assess the vulnerabilities inherent in typical network switches. Following the attack simulations, we present and analyse the results, highlighting the impact of each attack on the network's performance and security posture.

Subsequently, we implement various mitigation techniques aimed at countering these attacks, followed by an evaluation of their effectiveness. To wrap things up, the chapter discusses what we learned from the simulations. It compares these findings to what others have discovered and explains how these mitigation benefits small and medium-sized businesses (SMEs). This integrated approach provides a holistic view of L2 security challenges and solutions, contributing valuable insights to the field of network security for SMEs.

Design Requirements:

Initial Requirements: This project focuses on simulating network attacks in a virtual lab environment. The key requirements include:

- **Network Emulation Tool:** A robust platform to create complex network topologies for attack simulations.

- **Virtualization Software:** Software capable of efficiently managing network simulation machine to isolate from outside world.
- **Operating system:** Security tools pre-loaded with functionalities to execute various network attacks.
- **Network Devices:** To mimic a realistic small and medium enterprise network environment.

Design Decisions:

Considering the requirements, the following design decisions were made:

EVE-NG: Selected for its user-friendly interface and extensive library of network devices. EVE-NG facilitates the creation of intricate network configurations, enabling the simulation of diverse network attack scenarios [99].

VMware Workstation Pro: Chosen for its compatibility with EVE-NG and its ability to efficiently manage multiple virtual machines with allocated resources. VMware Workstation Pro ensures smooth operation of the virtual network environment during attack simulations [100].

Operating Systems: Parrot OS and Kali Linux were selected due to their wide range of pre-installed security tools for network attack simulations. These operating systems provide the necessary functionalities to execute various network attacks within the simulated environment [99] [100].

Cisco Devices: Cisco switch and router were chosen to simulate a realistic enterprise network environment commonly encountered in practice. Utilizing industry-standard equipment enhances the applicability of the simulations and the generalizability of the findings to real-world network deployments.

Attack Tools: Yersinia, Wireshark, and Ettercap are essential tools for conducting various network attacks, including MAC flooding, DHCP, STP, and VLAN attacks. Yersinia is a versatile framework designed to exploit weaknesses in network protocols, making it effective for launching attacks on STP, DHCP, and VLAN configurations. Wireshark serves as a powerful network protocol analyser, capable of capturing and inspecting data packets in real-time, which is crucial for identifying vulnerabilities and monitoring network traffic during

attacks like MAC flooding. Ettercap is specialized for man-in-the-middle attacks, allowing for the interception and manipulation of live network connections. It can perform MAC flooding by overwhelming a switch's MAC address table, DHCP spoofing by responding to DHCP requests with malicious configurations, and VLAN hopping to send traffic across different VLANs. Together, these tools provide a comprehensive suite for testing and exploiting network vulnerabilities, making them indispensable for penetration testers and cybersecurity professionals. [103] [103] [104].

Design Processes:

The design process involved setting up EVE-NG on a Lenovo c390 laptop running Windows 11 Pro. The network topology included a Cisco router acting as the DHCP server, a Cisco switch, and multiple virtual machines running.

4.1.1 Main Device Specification:

Laptop Model	Lenovo Yoga C930
Operating System	Windows 11 Pro
Processor	Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz 1.99 GHz
Ram	16 GB
Storage	521 GB

While the above specifications serve as a valuable reference point for mimicking the simulation, strict adherence is not essential. However, following these guidelines will help ensure smooth operation of the virtual environment.

4.1.2 Resource allocation:

For EVE-NG on VMware

Memory	8.6 GB
Processors	4
Hard Disk	60 GB
Network Adapter 1	NAT
Network Adapter 1	Host-only
Network Adapter 1	Bridged (Automatic)

USB Controller	Present
Display	Auto detect

Virtual Devices on EVE-NG

In the simulation, Cisco routers and switches were utilized alongside Parrot OS, Kali Linux, and Virtual PC to create a comprehensive testing environment. Parrot OS, known for its extensive suite of tools for penetration testing, computer forensics, and cryptography, provided a robust platform for security assessments [99]. Similarly, Kali Linux, a Debian-based distribution renowned for its penetration testing and security auditing capabilities, was employed to conduct various security tests and audits [100]. The Virtual PC Simulator (VPCS) was used to simulate lightweight PCs, supporting essential network functions such as DHCP and ping, thereby enhancing the realism and functionality of the simulation [101]. This setup allowed for thorough testing and troubleshooting of network configurations, ensuring a secure and efficient network environment.

4.1.3 Attack 1: DHCP Starvation attack and Rouge DHCP attack:

4.1.3.1 Literature Review Findings of **Error! Reference source not found.**:

The Dynamic Host Configuration Protocol (DHCP) is an essential network protocol that automates the allocation of IP addresses and other network settings to devices on a network, guaranteeing uninterrupted connection and effective network administration. Although DHCP is widely used and offers advantages, it also has risks. Existing literature clearly indicates that DHCP was not originally developed with security as a priority, resulting in inherent vulnerabilities such as the absence of authentication, secrecy, and integrity methods. These flaws make DHCP susceptible to attacks such as DHCP starvation and DHCP rogue server attack.

In a DHCP starvation attack, an attacker floods the DHCP server with numerous fake DHCPDISCOVER packets, exhausting the available IP addresses and causing a denial of service (DoS) for legitimate clients. Following this, a DHCP rogue server attack can be launched, where the attacker sets up a malicious DHCP server to provide fraudulent network configurations to clients, leading to potential man-in-the-middle (MITM) attacks and unauthorized data interception. These attacks exploit the fundamental weaknesses of DHCP,

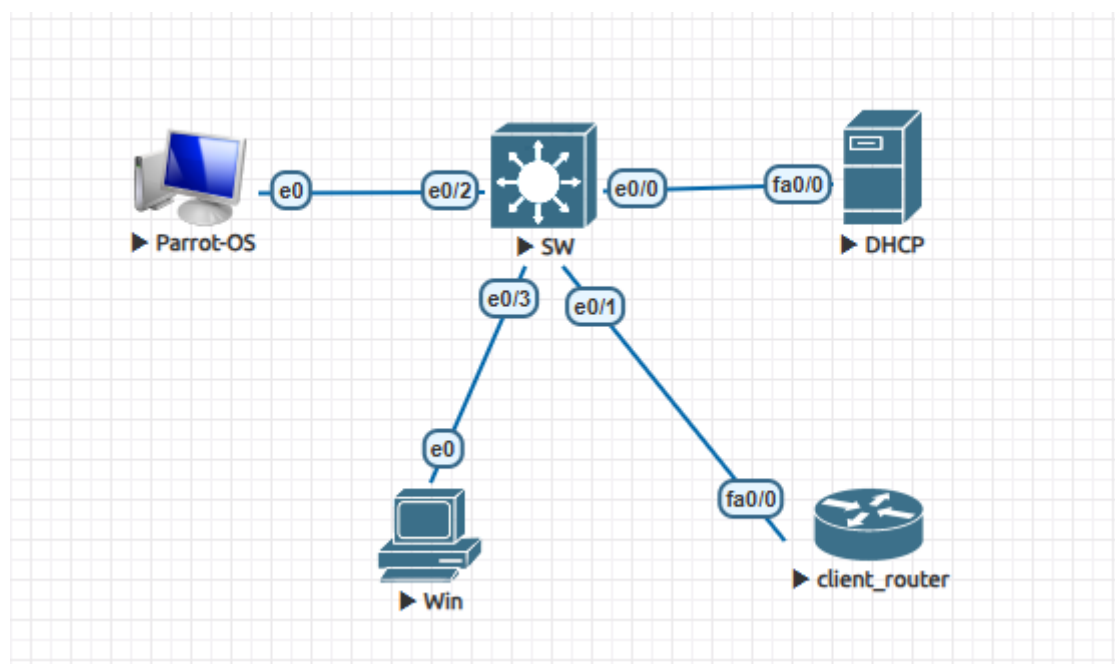
such as the inability of the server and client to authenticate each other and the use of plaintext UDP packets, making them susceptible to interception and manipulation by malicious actors.

Given the critical nature of these vulnerabilities and their potential impact on network security, it is imperative to conduct simulations of DHCP starvation and rogue server attacks. These simulations will provide a deeper understanding of the attack mechanisms, their effects on network performance and security, and the effectiveness of various countermeasures. By doing so, we can develop more robust security strategies to protect DHCP implementations and ensure the reliability and integrity of network services.

4.1.3.2 Methodology for DHCP Starvation:

- We will utilize the Yersinia tool to launch a DHCP starvation attack against a router running DHCP services.
- The attack will flood the network with spoofed DHCP Discover packets, each containing a unique MAC address.
- This will exhaust the DHCP server's IP address pool, preventing legitimate clients from acquiring IP addresses.

4.1.3.3 Network Topology and Device Configurations.



The provided network topology above is ideal for demonstrating DHCP starvation and rogue DHCP server attacks due to its simplicity and inclusion of essential components. The topology consists of a DHCP server, a switch, and multiple client devices (Parrot-OS, Win, and client_router), all interconnected to simulate a typical network environment.

DHCP Starvation Attack:

In this attack, the attacker (parrot-OS) floods the DHCP server with numerous DHCP DISCOVER packets, exhausting the available IP address pool of the DHCP server using the Yersinia tool. This prevents legitimate clients from obtaining IP addresses, leading to a denial of service (DoS).

Rogue DHCP Server Attack:

After DHCP Starvation attack, the attacker sets up an unauthorized DHCP server that responds to DHCP requests with malicious configurations and setting its own IP as default gateway for client. This will lead to man-in-the-middle attacks, data interception, and network disruption.

By using this topology, one can effectively demonstrate the mechanics of DHCP starvation and rogue DHCP server attacks, as well as the corresponding mitigation techniques, providing a comprehensive understanding of these network security threats.

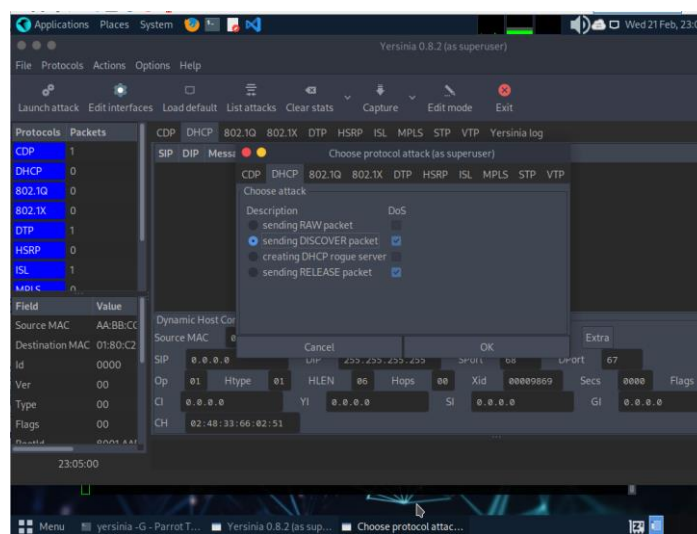
Configure the cisco router for DHCP

For this topology DHCP is a cisco router distributing IP addresses to all the clients and there is are no other services or security measures in place. Below are configuration commands to host the DHCP server:

config t	Enter global configuration mode.
interface f0/0	Select the FastEthernet 0/0 interface.
ip address 192.168.1.1 255.255.255.0	Assign IP address 192.168.1.1 with a subnet mask of 255.255.255.0 to the interface.
no shutdown	Enable the interface.
exit	Exit the interface configuration mode.
ip DHCP pool MAIN-POOL	Create a DHCP pool named MAIN-POOL.
network 192.168.1.100 255.255.255.0	Define the network and subnet mask for the

	DHCP pool.
default-router 192.168.1.1	Set the default gateway for DHCP clients.
dns-server 8.8.8.8	Set the DNS server for DHCP clients.
domain-name cisco.com	Set the domain name for DHCP clients.
lease 7	Set the lease duration to 7 days.
ip DHCP excluded-address 192.168.1.1	Exclude the router's IP address from the DHCP pool.

Launch DHCP Starvation Attack:



- **Select the DHCP Protocol:**

In the Yersinia GUI, navigate to the DHCP tab.

- **Choose the Attack Type:**

Select the sending DISCOVER packet option. This will flood the DHCP server with DHCP DISCOVER packets, consuming all available IP addresses.

- **Launch the Attack:**

Click on Launch Attack to start the DHCP Starvation Attack. This will consume all the IP addresses from DHCP server as shown in below figure, preventing legitimate clients from obtaining an IP address.

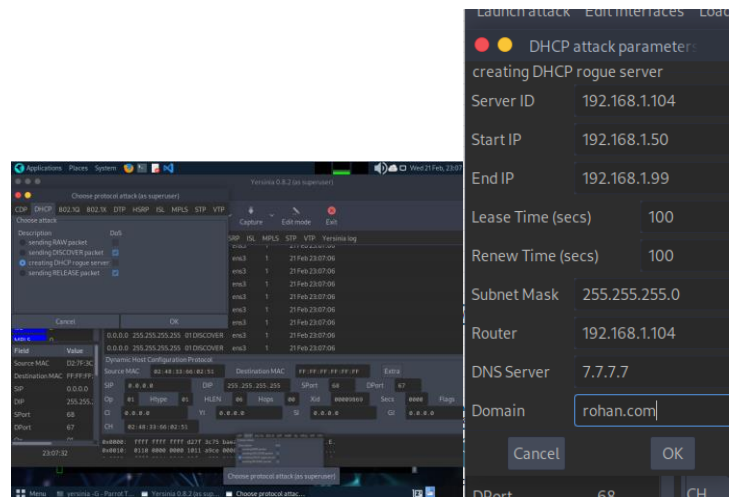
4.1.3.4 Methodology for Creating a Rogue DHCP Server

- **Setup:** The attacker connects a device running a rogue DHCP server to the target network.
- **DHCP Offer:** When a client sends a DHCP Discover message, both the legitimate and rogue DHCP servers respond with a DHCP Offer.
- **DHCP Acknowledgment:** The client may accept the offer from the rogue server, leading to incorrect network configuration.
- **Network Disruption:** The client may be assigned an incorrect IP address, DNS server, or default gateway, causing network issues or redirecting traffic through the attacker's device.

Steps For Creating a Rogue DHCP Server

Once the DHCP Starvation Attack is successful and all IP addresses are consumed, proceed to create a Rogue DHCP server as shown in below figures:

- **Select the DHCP Protocol Again:**
In the Yersinia GUI, navigate back to the DHCP tab.
- **Choose the Rogue DHCP Server Attack:**
Select the creating DHCP rogue server option.
- **Configure the Rogue DHCP Server:**
 - **IP Address Pool:** Define the range of IP addresses the rogue server will assign.
 - **Default Gateway:** Set the default gateway (Router field in Yersinia) to the attacker's IP address. This is crucial for conducting a successful Man-in-the-Middle (MITM) attack.
- **Launch the Rogue DHCP Server:**
Click on Launch Attack to start the rogue DHCP server. When a client tries to obtain an IP address, it will receive one from the rogue DHCP server, along with the attacker's IP address as the default gateway.



After launching the rogue DHCP server, verify that clients are receiving IP addresses from the rogue server. When a client_router tries to get IP address, it gets IP address from the rogue DHCP server which is evident from the pool given by it as shown in the below figure:

```

client_router(config)#int f0/0
client_router(config-if)#ip add dhcp
client_router(config-if)#do sh ip int b

```

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	unassigned	YES	DHCP	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down

```

client_router(config-if)#
*Feb 21 23:18:17.751: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.1.50, mask 255.255.255.0, hostname client_router
do sh ip int b

```

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	192.168.1.50	YES	DHCP	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down

Mitigation based on literature review on pg.23: Based on the literature review, implementing DHCP snooping and port security is a well-supported and effective strategy for enhancing network security. DHCP snooping acts as a firewall between untrusted hosts and trusted DHCP servers, validating DHCP messages and maintaining a binding database to prevent unauthorized IP address assignments. This mitigates DHCP spoofing and starvation attacks by ensuring only legitimate DHCP servers can respond to requests. Port security complements this by limiting the number of MAC addresses on a port, preventing attackers from flooding the network with spoofed DHCP requests, effectively mitigating DHCP starvation attacks. Together, these features provide a robust defence against DHCP-related attacks, ensuring a secure and reliable network infrastructure.

DHCP Snooping Commands:

Command	Description
ip DHCP snooping	Enables DHCP snooping globally on the switch.
ip DHCP snooping VLAN <VLAN-id>	Enables DHCP snooping on a specific VLAN.
interface <interface-id>	Enters interface configuration mode for the specified interface.
ip DHCP snooping trust	Configures the specified interface as a trusted port for DHCP snooping.
ip DHCP snooping limit rate <rate>	Sets a rate limit for DHCP requests on the interface.
show ip DHCP snooping	Displays the current DHCP snooping configuration on the switch.
show ip DHCP snooping binding	Shows the DHCP snooping binding table, which contains information about the IP addresses assigned to clients and their corresponding MAC addresses.

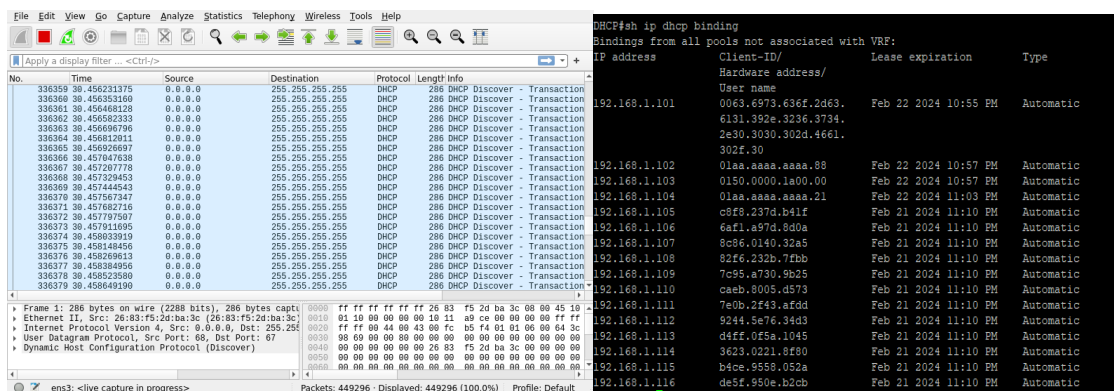
Port Security Commands [96]:

Command	Description
interface <interface-id>	Enters interface configuration mode for the specified interface.
switchport mode access	Configures the interface as an access port.
switchport port-security	Enables port security on the specified interface.
switchport port-security maximum <number>	Sets the maximum number of secure MAC addresses allowed on the interface.
switchport port-security mac-address <mac-	Specifies a static secure MAC address that is

address>	allowed to access the interface.
switchport port-security mac-address sticky	Enables sticky MAC address learning, which dynamically learns and retains MAC addresses on the interface.
switchport port-security violation Shutdown	The port is taken out of service and placed in an error-disabled state. The port remains in this state until manually removed and generates Log messages.

4.1.3.5 Analysis -*Impact of DHCP Starvation and DHCP Rogue Server Attacks on Network and Topology*

1. Network Availability:



No.	Time	Source	Destination	Protocol	Length	Info
336359	38.456231375	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336360	38.456231380	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336361	38.456468128	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336362	38.456562333	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336363	38.456696796	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336364	38.456812811	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336365	38.456926697	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336366	38.457047638	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336367	38.457207778	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336368	38.457329453	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336369	38.457444543	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336370	38.457567347	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336371	38.457682716	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336372	38.457797507	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336373	38.457911695	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336374	38.458033919	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336375	38.458148456	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336376	38.458269613	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336377	38.458384956	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336378	38.458523580	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction
336379	38.458648190	0.0.0.0	255.255.255.255	DHCP	288	DHCP Discover - Transaction

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
192.168.1.101	0063.6973.636f.2d63. 6131.392e.3236.3734. 2e30.3030.302d.4661. 302f.30	Feb 22 2024 10:55 PM	Automatic
192.168.1.102	01aa.aaaa.aaaa.88	Feb 22 2024 10:57 PM	Automatic
192.168.1.103	0150.0000.1a00.00	Feb 22 2024 10:57 PM	Automatic
192.168.1.104	01aa.aaaa.aaaa.21	Feb 22 2024 11:03 PM	Automatic
192.168.1.105	c9f8.237d.b41f	Feb 21 2024 11:10 PM	Automatic
192.168.1.106	cafl.a97d.8d0a	Feb 21 2024 11:10 PM	Automatic
192.168.1.107	8cd6.0140.32a5	Feb 21 2024 11:10 PM	Automatic
192.168.1.108	02f6.232b.7fbb	Feb 21 2024 11:10 PM	Automatic
192.168.1.109	7c55.a730.9b25	Feb 21 2024 11:10 PM	Automatic
192.168.1.110	caeb.8006.d573	Feb 21 2024 11:10 PM	Automatic
192.168.1.111	7e0b.2f43.afdd	Feb 21 2024 11:10 PM	Automatic
192.168.1.112	9244.5e76.34d3	Feb 21 2024 11:10 PM	Automatic
192.168.1.113	d4ff.0f5a.1045	Feb 21 2024 11:10 PM	Automatic
192.168.1.114	3623.0221.8f80	Feb 21 2024 11:10 PM	Automatic
192.168.1.115	b4ce.9558.052a	Feb 21 2024 11:10 PM	Automatic
192.168.1.116	de5f.950e.b2cb	Feb 21 2024 11:10 PM	Automatic

Denial of Service (DoS): From the above two figures, you can see the , the attacker generated more than 330000+ discover packets within 30 seconds, the attacker didn't just exhaust all the IP addresses from the DHCP server but also did a MAC flooding attack on the switch causing it have fake entries in the mac-address and you can see traffic was generated

from port E0/2 where the attacker is connected on the switch as show in below figure.

Plan	Mac Address	Type	Ports
1	0000.b54e.7c76	DYNAMIC	Eto/2
1	0000.fc24.3346	DYNAMIC	Eto/2
1	0001.3a34.3379	DYNAMIC	Eto/2
1	0001.6365.9630	DYNAMIC	Eto/2
1	0002.e152.3445	DYNAMIC	Eto/2
1	0003.b478.9630	DYNAMIC	Eto/2
1	0004.033b.b5a2	DYNAMIC	Eto/2
1	0004.bae2.3e48	DYNAMIC	Eto/2
1	0005.f12c.724c	DYNAMIC	Eto/2
1	0006.3844.b5a2	DYNAMIC	Eto/2
1	0007.2a7a.f2e4	DYNAMIC	Eto/2
1	0007.2a74.5469	DYNAMIC	Eto/2
1	0008.5d53.6927	DYNAMIC	Eto/2
1	0008.74fb.b6e5	DYNAMIC	Eto/2
1	0008.835d.2382	DYNAMIC	Eto/2
1	0009.ac70.f420	DYNAMIC	Eto/2
1	000a.653f.34f2	DYNAMIC	Eto/2
1	000a.5480.1753	DYNAMIC	Eto/2
1	000c.ae41.37db	DYNAMIC	Eto/2
1	000d.115c.77d4	DYNAMIC	Eto/2
1	000e.417a.66a5	DYNAMIC	Eto/2
1	000e.984a.b497	DYNAMIC	Eto/2
1	000f.3343.8530	DYNAMIC	Eto/2
1	000e.ea3c.6e37	DYNAMIC	Eto/2
1	0011.c043.1b7b	DYNAMIC	Eto/2
1	0013.2a38.4b4f	DYNAMIC	Eto/2
1	0013.4178.8e34	DYNAMIC	Eto/2
1	0013.4a1a.803d	DYNAMIC	Eto/2
1	0013.5f4b.4ff6	DYNAMIC	Eto/2
1	0017.806d.c088	DYNAMIC	Eto/2
1	0017.e152.4250	DYNAMIC	Eto/2
1	0018.397f.cfd9	DYNAMIC	Eto/2
1	0019.e85d.44a8	DYNAMIC	Eto/2
1	001c.9c25.84a6	DYNAMIC	Eto/2
1	001c.e45d.1bf7	DYNAMIC	Eto/2
1	001d.106e.3968	DYNAMIC	Eto/2
1	001d.2779.f2ba	DYNAMIC	Eto/2
1	001d.4046.6852	DYNAMIC	Eto/2
1	001e.1541.ac98	DYNAMIC	Eto/2
1	001e.9212.4b45	DYNAMIC	Eto/2
1	001f.5a74.923c	DYNAMIC	Eto/2
1	0020.055a.de28	DYNAMIC	Eto/2
1	0020.2126.68d0	DYNAMIC	Eto/2
1	0020.7210.50a8	DYNAMIC	Eto/2
1	0020.a16d.c20d	DYNAMIC	Eto/2
1	0020.d703.100e	DYNAMIC	Eto/2
1	0021.3a15.7f40	DYNAMIC	Eto/2
1	0021.6634.c8a8	DYNAMIC	Eto/2
1	0023.290a.9957	DYNAMIC	Eto/2
1	0023.6094.c1a8	DYNAMIC	Eto/2
1	0023.842c.584f	DYNAMIC	Eto/2
1	0024.bdl9.35bf	DYNAMIC	Eto/2
1	0024.f60e.7db7	DYNAMIC	Eto/2

Increased Traffic: The flooding of DHCP requests generates a significant amount of network traffic. This led to network congestion, slowing down the overall performance of the network and causing legitimate traffic to be dropped as shown in below figure.

```
client_router>
client_router>en
client_router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
client_router#
```

Server and Switch Overload: Both the DHCP server and network switches experience increased CPU usage due to the high volume of DHCP traffic. The DHCP server becomes overwhelmed by the flood of requests, leading to higher CPU and memory usage, which degrades its performance and impacts its ability to manage other network services effectively. Simultaneously, the network switches also suffer from increased CPU usage, affecting their ability to handle other network traffic efficiently and leading to overall network performance degradation.

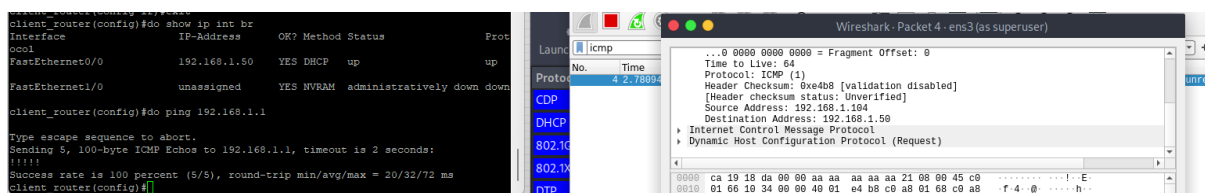
Administrative Overhead:

Troubleshooting: In complex networks, administrators could need to spend significant time identifying and mitigating the attack, which can divert resources from other critical tasks. The process of clearing the IP address pool and restoring normal operations can be complex and time-consuming.

4.1.3.6 Impact of DHCP Rogue Server Attack on Network and Topology

Network Security:

Traffic Redirection: A rogue DHCP server provided incorrect gateway and DNS server addresses to clients, redirecting their traffic through attacker's machine as you can see from below figure the new IP address on the client_router is from pool of rouge DHCP server. Despite a ping being generated from 192.165.1.50 to 192.168.1.1, the attacker's machine's Wireshark captures ICMP traffic from the victim which shows in the below figure that attacker could see 192.168.1.104 pinged 102.168.1.50. This led to MITM attack and eavesdropping and interception, of data, compromising the confidentiality and further the attack can manipulate the data and compromise the integrity of network communications.



Network Reliability:

Connectivity Issues: Clients that receive incorrect network configurations experienced connectivity issues, such as being unable to reach certain network resources. This can disrupt normal business operations and cause frustration for users.

Network Topology Changes:

Unauthorized Devices: The introduction of a rogue DHCP server represents an unauthorized change to the network topology. This can complicate network management and monitoring, making it harder to maintain a clear understanding of the network's structure and status.

Administrative Challenges:

Detection and Mitigation: Identifying the presence of a rogue DHCP server can be challenging, especially for SMEs with limited IT staff and resources. Implementing and

maintaining security measures like DHCP snooping and network segmentation requires expertise and ongoing management, which may be beyond the capabilities of many SMEs.

4.1.3.7 Analysis after mitigating Mac flooding, DHCP starvation and rouge DHCP server:

Network Availability:

By limiting the number of MAC addresses per port, port security effectively counters attacks involving fake DHCPDISCOVER packets with bogus MAC addresses. When the attacker attempted to generate these packets, the port connected to the attacker's machine was shut down and a log entry was generated, as shown in the figure below. The port was placed in error-disabled mode, which successfully prevented DHCP starvation on the DHCP server and mitigated MAC flooding on the switch.

```
Switch#sh
*Jun 30 22:53:19.697: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh int e0/2
Ethernet0/2 is down, line protocol is down (err-disabled)
  Hardware is Ethernet, address is aabb.cc01.7020 (bia aabb.cc01.7020)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
```

Network Reliability:

```
ip
client_router(config-if)#do sh ip int br
Interface                IP-Address      OK? Method Status        Protocol
FastEthernet0/0          192.168.1.146   YES DHCP    up            up
FastEthernet1/0          unassigned      YES NVRAM   administrativ down down
client_router(config-if)#
*Jun 30 23:14:43.527: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP a
ddress 192.168.1.146, mask 255.255.255.0, hostname client_router
```

As DHCP snooping was used, the attempted attack for MITM attack using rogue DHCP server was prevented. As shown in the above figure, the client_router didn't receive IP address from the rouge DHCP server's pool which was from 192.168.1.50 to 192.168.1.99 as show in above figure.

Infrastructure strain:

Because of port security, we observed that there was neither any unusual traffic spike nor abnormal load on CPU and memory.

Administrative Overhead:

Implementing DHCP snooping and port security significantly reduces the administrative overhead associated with identifying and mitigating DHCP starvation and rogue server attacks. DHCP snooping creates a binding database that logs legitimate DHCP transactions,

making it easier for network administrators to detect and block malicious DHCP traffic. This database acts as a reference point for troubleshooting, allowing administrators to quickly identify unauthorized DHCP servers and mitigate their impact. Port security further simplifies management by limiting the number of MAC addresses per port, preventing MAC flooding attacks and reducing the complexity of clearing IP address pools. These measures streamline the process of restoring normal operations, enabling administrators to focus on other critical tasks without being diverted by extensive troubleshooting efforts.

4.1.3.8 Summary:

For SMEs, DHCP starvation and rogue server attacks can have severe implications for network availability, performance, security, and manageability. These attacks can lead to significant disruptions in service, compromise sensitive data, and increase the administrative burden on limited IT resources. Effective mitigation strategies, including port security, DHCP snooping, and network segmentation, are essential to protect against these types of attacks and maintain the integrity and reliability of the network. However, SMEs must balance these needs against their often limited resources, making proactive planning and investment in network security crucial.

4.1.4 Attack 4: ARP Poisoning:

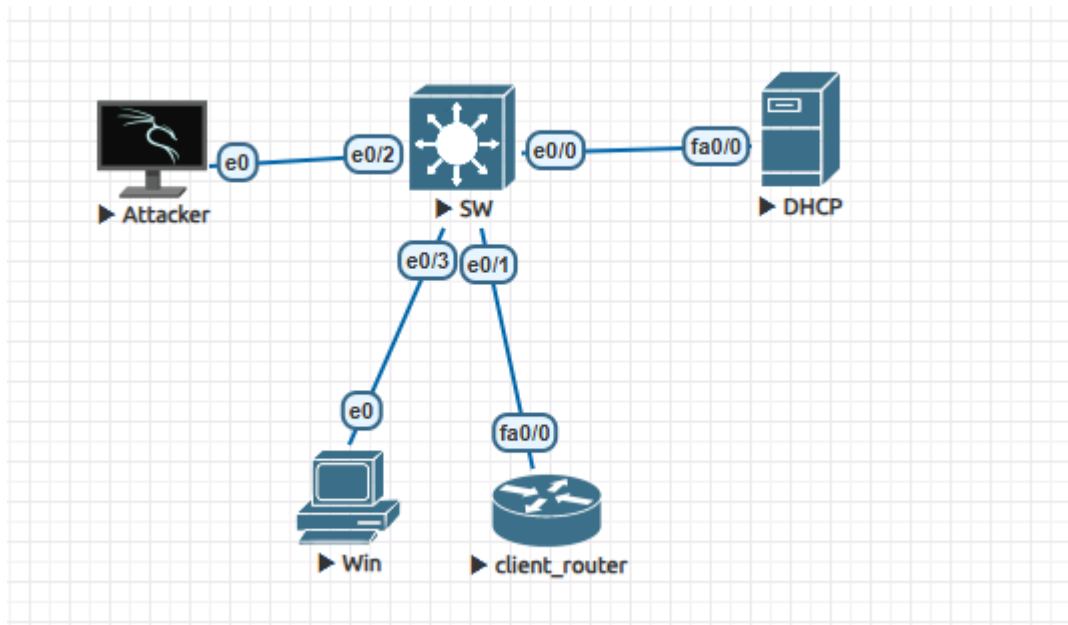
Literature review findings on pg.25: The literature review highlights a critical vulnerability within the core functionality of Local Area Networks (LANs). The Address Resolution Protocol (ARP), responsible for mapping IP addresses to physical device addresses (MAC addresses), lacks inherent security features. This vulnerability is actively exploited through a cyber-attack known as ARP spoofing, or ARP poisoning. In this attack, malicious actors manipulate ARP messages, tricking the network into associating their device's MAC address with a legitimate device's IP address. This deception allows attackers to intercept, alter, or block data intended for the targeted device, potentially leading to a range of threats including session hijacking, man-in-the-middle attacks, and denial-of-service attacks. Understanding the mechanics of this attack is crucial for implementing robust network security measures and safeguarding sensitive information within the network.

Methodology

- **Preparation:** The attacker must have access to the target LAN.
- **Spoofing:** The attacker sends fake ARP replies to the target devices, associating the attacker's MAC address with the IP address of the legitimate device.

- **Interception:** The target devices update their ARP tables with the attacker's MAC address, redirecting traffic to the attacker.
- **Manipulation:** The attacker can now intercept, modify, or drop the intercepted traffic.

Network topology and device config



This meticulously designed network topology serves as an ideal simulation for comprehending ARP poisoning attacks. Its simplicity and inclusion of essential components (DHCP server, switch, and diverse client devices) accurately reflect real-world network environments. By simulating an attack where a Kali Linux machine targets the router to intercept traffic between a client router and the DHCP server (potentially stealing Telnet credentials), this setup effectively reveals the mechanics of ARP poisoning. The ability to showcase not only the attack itself, but also corresponding mitigation strategies, elevates this topology to a powerful tool for gaining a thorough understanding of these network security threats and how to combat them.

Step-by-Step Guide to Using Ettercap

Launch Ettercap

In CLI: `sudo ettercap -G`

This command will launch Ettercap with root privileges and opens the GUI.

Select Network Interface

In the Ettercap GUI, Select primary interface and click on accept button which will start unified sniffing as show in below:



Scan for Hosts:

Click on magnifying glass to scan for hosts on the network.

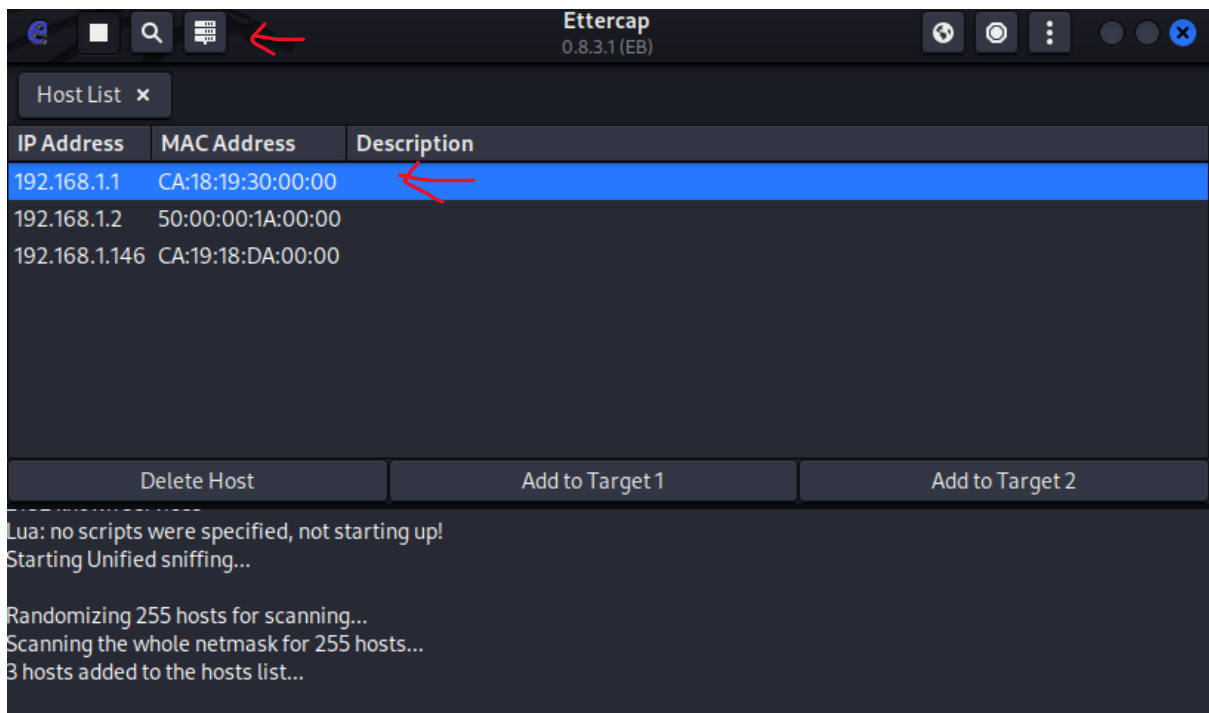


Ettercap will scan the network and list all detected hosts. This step is crucial for identifying potential targets on the network.

Add Targets

After scanning, you need to specify the hosts you want to target

Click on Hosts List: Select the target IP and add it to “Add to Target 1”



Start ARP Poisoning

To initiate ARP poisoning, navigate to:

MITM > ARP poisoning

A dialog will appear. Check the option "Sniff remote connections" and click "OK". This action will start the ARP poisoning attack, making Ettercap intercept traffic between the two targets.

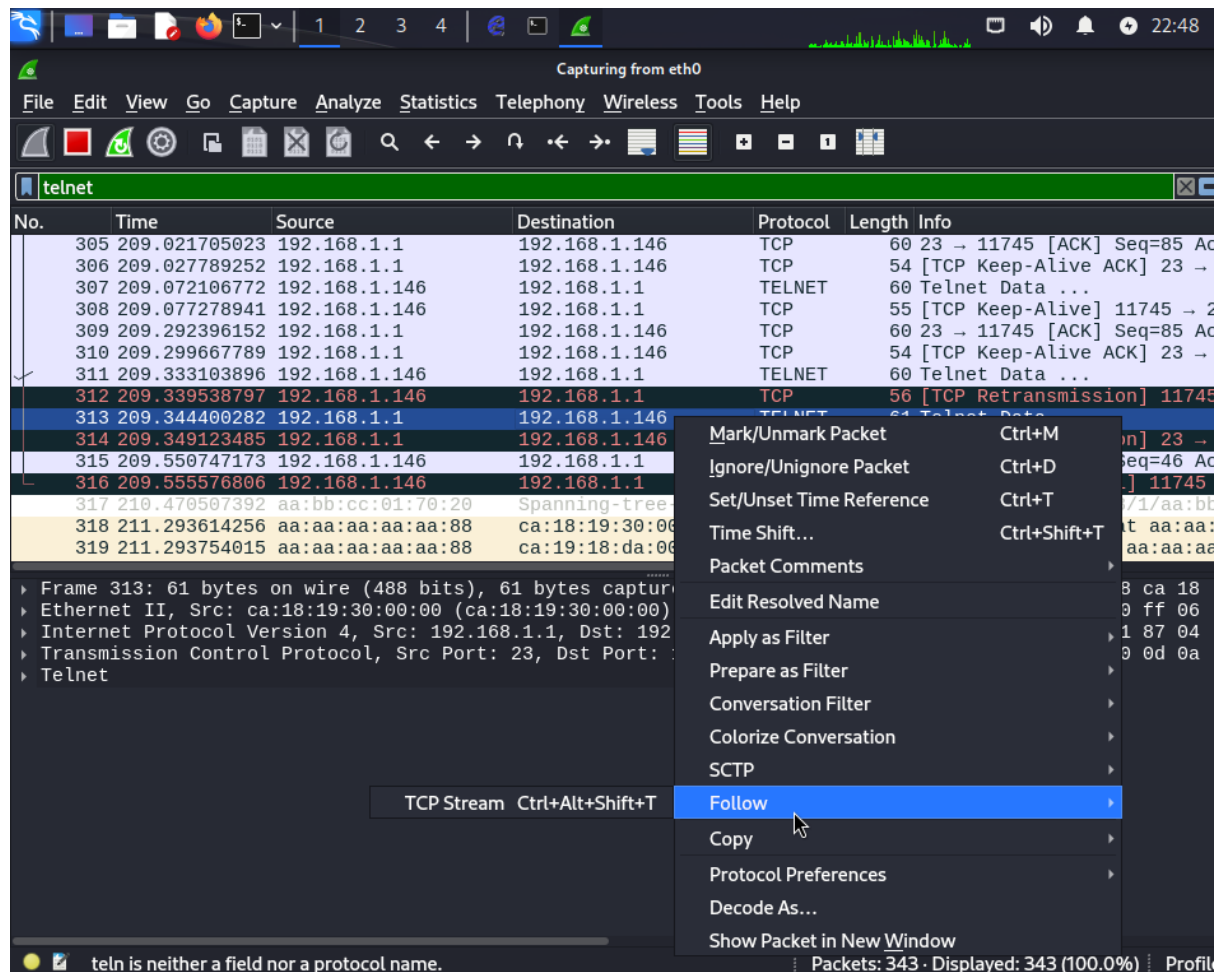
Start Sniffing

Finally, to begin sniffing the network traffic, go to Wireshark:

Select the interface and start scan, now whenever targeted machines will communicate, everything would be visible to the attacker.

Look for telnet packets:

Try to find telnet traffic for 192.168.1.1, you can do this by applying telnet filter.



Once you find telnet traffic, click on it and go to Follow> TCP stream.

As you can see you could see the username and password user for telnet from 192.168.1.146 to 192.168.1.1.

Mitigation based on literature review on pg.28: To defend the simulation against ARP poisoning attacks, DHCP Snooping, DAI, and Port Security were included. This conclusion was reached after reviewing the relevant literature. This combination works because DHCP Snooping monitors DHCP traffic to create a database of IP-to-MAC links. After then, DAI checks ARP packets using this database to guarantee only real requests and answers are sent. Port security limits MAC addresses that may connect to a port. This function prevents unauthorised devices from entering the network, increasing safety. Because most business-grade switches contain these features, SMEs may benefit from a cost-effective and free solution. This integrated strategy reduces ARP spoofing and improves network security.

Mitigation Commands on Switch and Description

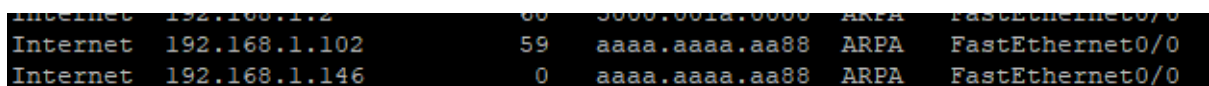
Command	Description
ip DHCP snooping VLAN 1	Enables DHCP snooping on VLAN 1. DHCP snooping is a security feature that filters untrusted DHCP messages and builds a DHCP binding table.
int e0/0 (DHCP)	Enters interface configuration mode for interface Ethernet 0/0, typically used to apply DHCP-related configurations.
ip DHCP snooping trust	Configures the interface as trusted for DHCP snooping. Trusted interfaces can forward DHCP server messages.
no ip DHCP snooping information option	Disables the insertion of DHCP Option 82 information into DHCP packets. This option is used to provide additional information about the DHCP relay agent.
ip ARP inspection VLAN 1	Enables Dynamic ARP Inspection (DAI) on VLAN 1. DAI validates ARP packets to prevent ARP spoofing attacks.
int e0/0 (DHCP)	Re-enters interface configuration mode for interface Ethernet 0/0, typically used to apply ARP inspection-related configurations.
ip ARP inspection VLAN trust	Configures the interface as trusted for ARP inspection. Trusted interfaces can forward ARP packets without inspection.
switchport port- security	Enables port security on the interface. Port security restricts input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port.
switchport port- security sticky	Enables sticky MAC address learning on the interface. Sticky MAC addresses are dynamically learned and saved in the running configuration.

Command	Description
switchport port-security shutdown	Configures the port to shut down if a security violation occurs. A security violation happens when the maximum number of secure MAC addresses is exceeded.
switchport port-security maximum	Sets the maximum number of secure MAC addresses allowed on the interface. If the number of MAC addresses exceeds this limit, a security violation occurs.

Network Security Analysis: ARP Poisoning

Traffic Redirection and MITM Attack

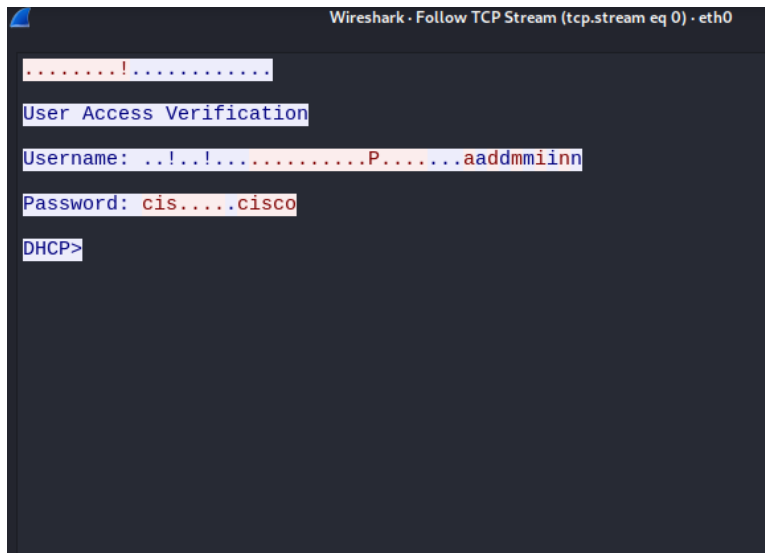
The attacker successfully clones the MAC address of the victim's device, allowing them to intercept and manipulate network traffic directed towards the victim. IP address 192.168.1.102 and 192.168.1.146 have the same mac-address which is evident in the below figure.



Internet	192.168.1.2	59	aaaa.aaaa.aa88	ARPA	FastEthernet0/0
Internet	192.168.1.102	59	aaaa.aaaa.aa88	ARPA	FastEthernet0/0
Internet	192.168.1.146	0	aaaa.aaaa.aa88	ARPA	FastEthernet0/0

Network Reliability

During the ARP poisoning attack, clients may experience connectivity issues, such as being unable to reach certain network resources or experiencing unusual network latency. This disruption can affect normal business operations and frustrate users. However, in this specific scenario, there was no noticeable downtime or performance drop, although the attacker was able to intercept messages from the victim in which attacker could see credentials via Wireshark as show in below figure.



Network Topology Changes

The introduction of a rogue device performing ARP poisoning represents an unauthorized change to the network topology. This complicates network management and monitoring, making it harder to maintain a clear understanding of the network's structure and status. The attacker's machine, now acting as a man-in-the-middle (MITM), did intercept and potentially could alter communications between network devices.

Analysis After Mitigating ARP Poisoning

Network Reliability

The network devices did not accept the falsified ARP messages, ensuring that legitimate IP-to-MAC mappings were maintained. This prevented the attacker from intercepting or manipulating network traffic, thereby maintaining the reliability of network communications.

Infrastructure Strain: did not result in any unusual traffic spikes or abnormal load on CPU and memory. These measures are designed to enhance network security without significantly impacting network performance or infrastructure resources.

4.1.5 Attack 3: STP:

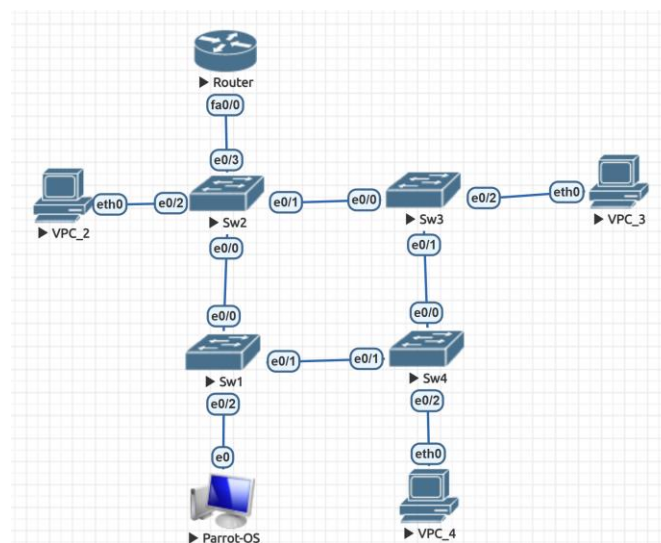
Based on literature Review Findings on pg.30: The Spanning Tree Protocol (STP) is essential for preventing network loops in Ethernet LANs by electing a root bridge, calculating path costs, assigning port roles, and exchanging BPDUs. However, STP's lack of authentication makes it vulnerable to attacks. Malicious users can manipulate BPDUs to alter the network topology, causing loops, broadcast storms, and network failures. Denial-of-

Service (DoS) attacks can also be executed by flooding the network with BPDUs, leading to instability and outages. By simulating different scenarios, network administrators can identify potential weaknesses, test their configurations, and ensure their networks are resilient against these threats.

Methodology

1. **Preparation:** Identify the current root bridge in the network.
2. **Attack Execution:** Use a tool like Yersinia to send out Bridge Protocol Data Units (BPDUs) with a lower bridge ID than the current root bridge.
3. **Result:** The network reconfigures itself, making the attacker's device the new root bridge.

Network Topology and device configuration:



This carefully structured network topology, featuring a router as gateway for the network and four switches and a PC connected to each switch, is perfectly suited for demonstrating Spanning Tree Protocol (STP) attacks. By incorporating an attacker's machine running Parrot OS, which is equipped with penetration testing tools like Yersinia, this setup accurately simulates real-world network environments. The attacker can manipulate STP by sending malicious Bridge Protocol Data Units (BPDUs) to become the root bridge, causing network disruptions such as loops and congestion. This topology not only highlights the mechanics of

STP attacks but also emphasizes the importance of implementing security measures like BPDU Guard and Root Guard to mitigate such threats.

Configuration to Perform the Attack with Yersinia

- **Launch Yersinia:**
Open Yersinia on the attacker's machine running Parrot OS.
- **Initiate the Attack:**
Navigate to the STP (Spanning Tree Protocol) tab within Yersinia. Select the option to launch an attack.
- **Claim root role:**
Choose the option claim root role. In this attack, the malicious device sends BPDUs with a lower Bridge ID (lower priority or MAC address) than the current Root Bridge. This tricks other switches into believing that the attacker should be the new Root Bridge as.

Mitigation based on literature review 2.3.4.3 above: As discussed in the literature, we are going to use BPDU Guard and root guard, for this simulation to mitigate STP attacks. BPDU Guard prevents unauthorized devices from sending BPDUs by shutting down compromised ports, this should be configured on all ports of switch where end devices are connected as they shouldn't be sending BPDUs. Root Guard ensures certain ports never become the root port by placing them in a root-inconsistent state upon receiving superior BPDUs.

Mitigation Commands on Switch and Description

Mitigation Technique	Command	Description
Select End device interface	Interface E0/2	
Root Guard	spanning-tree guard root	Prevents a port from becoming a root port.

Mitigation Technique	Command	Description
BPDU Guard	spanning-tree bpduguard enable	Disables a port if it receives a BPDU.

Analysis of STP Attack

Connectivity Issues: The attack caused frequent topology changes, leading to intermittent connectivity issues and increased packet loss. This disrupted normal business operations and degraded user experience.

Unauthorized Role Changes: The attacker's machine becoming the Root Bridge represented an unauthorized change to the network topology. This complicated network management and monitoring, making it harder to maintain a clear understanding of the network's structure and status.

Detection and Mitigation: Identifying and mitigating the STP attack required expertise in network protocols. Implementing security measures like Root Guard and BPDU Guard was essential to prevent unauthorized devices from influencing the STP topology.

Efficient Resource Usage: Claiming root bridge sent caused unusual traffic spikes and abnormal load on CPU and memory because constant spamming of BPDU from the attacker's machine.

Analysis After Mitigating the STP Attack

Stable Topology: By enabling Root Guard on all ports where end devices are connected, any port receiving superior BPDUs was placed in a root-inconsistent state, preventing unauthorized devices from becoming the Root Bridge. This maintained a stable and predictable network topology.

Consistent Connectivity: With BPDU Guard enabled globally on all PortFast-enabled ports, any port receiving a BPDU was immediately shut down. This prevented unauthorized devices from sending BPDUs, ensuring consistent connectivity and reducing the risk of network loops.

Efficient Resource Usage: The implementation of Root Guard and BPDU Guard did not introduce any unusual traffic spikes or abnormal load on CPU and memory. The network operated efficiently without additional strain on infrastructure resources.

Simplified Management: Root Guard and BPDU Guard significantly reduced the administrative overhead associated with detecting and mitigating STP attacks. These measures streamlined network management by preventing unauthorized topology changes and ensuring a loop-free environment, allowing administrators to focus on other critical tasks.

4.1.6 Attack 5: VLAN hopping:

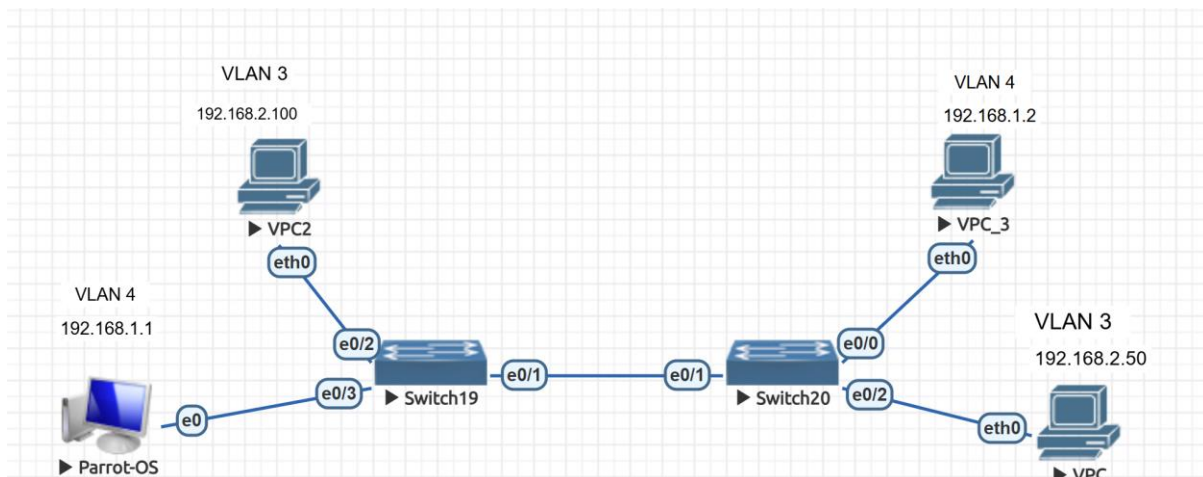
Literature review findings on page 33: VLANs partition a physical network into distinct logical networks. VLANs enable network administrators to segment a single physical network into multiple, isolated logical networks. This enhances network performance, increases security, and simplifies management by reducing traffic congestion and confining broadcast traffic. VLANs offer flexibility and scalability, making them suitable for dynamic environments. They are particularly beneficial for small and medium-sized enterprises (SMEs) by saving costs using existing hardware for logical segmentation, improving network performance by mitigating congestion, and enhancing security by segregating departments and operations.

As discussed in VLAN hopping 33on page 33, this attack exploits a vulnerability in Cisco switches using the Dynamic Trunking Protocol (DTP), which is enabled by default. Attackers can connect a device to a switch port in dynamic preferred mode, tricking the switch into forming a trunk link. This allows the attacker access to all VLANs associated with the trunk, compromising network security.

Methodology

- 1. Send DTP Packets:** The attacker sends Dynamic Trunking Protocol (DTP) packets to negotiate a trunk link with the switch.
- 2. Establish Trunk Link:** If the switch is configured to negotiate trunks automatically (dynamic auto or dynamic desirable mode), it establishes a trunk link with the attacker's device.
- 3. Access Multiple VLANs:** The attacker now has access to traffic from all VLANs allowed on the trunk link.

Network topology



The above topology reflects a common network design where VLANs are used to separate traffic for different departments or functions. VLAN 3 and VLAN 4 represent distinct segments of the network, ensuring that traffic from one VLAN does not interfere with the other under normal circumstances.

By using this topology, the demonstration of VLAN hopping attacks and their mitigation becomes straightforward and educational, providing a clear understanding of the vulnerabilities and the necessary security measures to protect against such exploits

Device configuration

Command	Description
interface Ethernet0/0	Selects interface Ethernet0/0 for configuration.
switchport access VLAN 4	Assigns the interface to VLAN 4, making it an access port for VLAN 4.
switchport mode access	Configures the interface to operate in access mode, ensuring it handles traffic for a single VLAN only (VLAN 4 in this case).
interface Ethernet0/1	Selects interface Ethernet0/1 for configuration.

Command	Description
switchport trunk encapsulation dot1q	Specifies that the interface should use IEEE 802.1Q encapsulation for VLAN tagging.
switchport mode trunk	Configures the interface to operate in trunk mode, allowing it to carry traffic for multiple VLANs.
interface Ethernet0/2	Selects interface Ethernet0/2 for configuration.
switchport access VLAN 3	Assigns the interface to VLAN 3, making it an access port for VLAN 3.
switchport mode access	Configures the interface to operate in access mode, ensuring it handles traffic for a single VLAN only (VLAN 3 in this case).

Attack Implementation Steps

From attacker's machine create sub interfaces for each VLAN using below commands:

```
Sudo ip link add link ens3 name ens3.3 type VLAN id 3
```

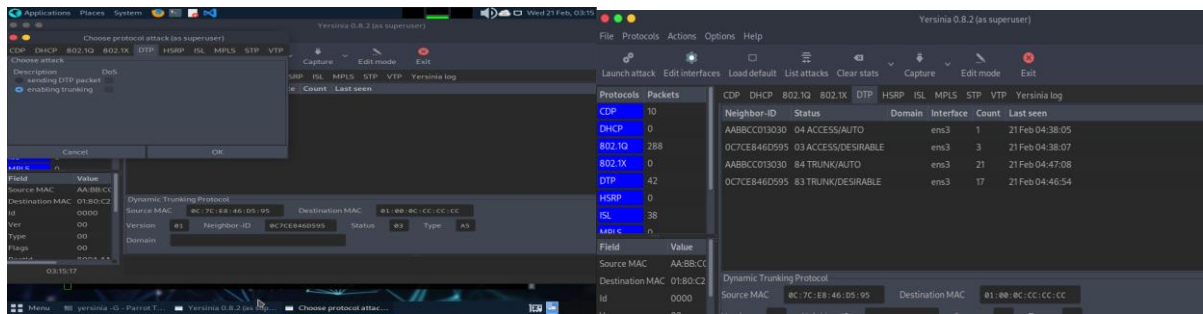
```
Sudo ip link add link ens3 name ens3.4 type VLAN id 4
```

Assign IPs to those newly created sub interfaces by below commands:

```
ifconfig ens3.3 192.168.2.5 netmask 255.255.255.0 up
```

```
ifconfig ens3.4 192.168.1.5 netmask 255.255.255.0 up
```

These commands set up the attacker's machine to interact with both VLAN 3 and VLAN 4, facilitating VLAN hopping attacks.



Use yersinia in parrot OS to initiate a DTP (Dynamic Trunking Protocol) trunking with the switch as shown in above figures. By exploiting DTP, the attack attempts to convert an access link into a trunk link, thereby gaining unauthorized access to traffic across multiple VLANs as shown in above figures.

Mitigation based on literature review findings on page 34: As discussed in the literature, we will implement strategies such as disabling Dynamic Trunking Protocol (DTP) on non-trunk ports, configuring trunk ports statically, and setting interfaces to access mode on edge devices.

Mitigation commands:

Task	Command	Description
Disable DTP on Non-Trunk Ports	<code>interface <interface-id> switchport mode access</code>	This command sets the interface to access mode, which disables DTP negotiation on the port.
Configure Trunk Ports Statically	<code>interface <interface-id> switchport mode trunk switchport nonegotiate</code>	This command configures the interface as a trunk port and disables DTP negotiation by preventing the port from sending DTP frames.
Set Interfaces to	<code>interface</code>	This command sets the interface to access mode

Task	Command	Description
Access Mode on Edge Devices	<pre> <interface-id> switchport mode access switchport access VLAN <VLAN-id> </pre>	and assigns it to a specific VLAN, making it suitable for edge devices.

Analysis of Network Security Measures for DTP Vulnerabilities in a Simulated Environment

Before Applying Security Measures

Network Availability:

Dynamic Trunking Protocol (DTP) vulnerabilities can allow unauthorized devices to form trunk links, leading to network disruptions and unauthorized access to multiple VLANs. Although the simulation did not experience downtime or performance drops, real-world networks could face severe availability issues during such attacks.

Network Reliability:

Without proper security configurations, the network's reliability is compromised. Attackers can exploit DTP to intercept and manipulate network traffic, leading to data breaches and loss of integrity.

Infrastructure Strain:

DTP vulnerabilities can flood the network with malicious traffic, overwhelming network devices and causing potential failures or degraded performance. This strain could result in hardware malfunctions and increased latency in real-world scenarios.

Administrative Overhead:

Managing a network with DTP vulnerabilities requires constant vigilance and manual intervention to detect and mitigate attacks. This leads to high administrative overhead and increased complexity for network management teams.

After Applying Security Measures (Disabling DTP, Manually Configuring Trunks, and Using VLAN Access Control)

Network Availability:

Disabling DTP and manually configuring trunk ports significantly enhances network availability by preventing unauthorized trunk links and reducing the risk of network disruptions. The network remains operational and accessible to legitimate users even during attempted attacks.

Network Reliability:

With these security measures in place, the network's reliability improves markedly. Disabling DTP ensures that only authorized devices can form trunk links, while manually configuring trunk ports and using VLAN access control mechanisms prevent unauthorized access, ensuring consistent and reliable performance.

Infrastructure Strain:

Implementing these security features reduces the strain on network infrastructure. By preventing unauthorized trunk links and filtering out malicious traffic, network devices are less likely to be overwhelmed by attack traffic, leading to more stable and efficient network operations.

Administrative Overhead:

Automating security by disabling DTP and manually configuring trunk ports reduces administrative overhead significantly. These measures simplify network management and enhance overall security posture, allowing network administrators to focus on more strategic tasks.

4.1.7 Conclusion:

In conclusion, this chapter has provided a detailed exploration of designing, implementing, and evaluating Layer 2 security measures within a simulated network environment for SMEs. By systematically conducting and analysing various L2 attacks and their mitigations, we have gained valuable insights into the vulnerabilities and defence mechanisms of network switches. The findings underscore the importance of robust security practices and offer practical guidance for enhancing network security in SMEs.

5. CHAPTER 5: Overall Discussion and Recommendations

5.1.1 Interpretation of Results

Our experimental setup demonstrated how attackers could exploit vulnerabilities in STP, DHCP, ARP and VLAN, to disrupt network operations.

During DHCP Starvation attack, switch also suffers from MAC flooding attack, attackers sent a large volume of spoofed DISCOVER packets, overwhelming the switch's MAC address table and causing significant delays in legitimate traffic, rendering the switch unable to process any commands due to spiked CPU and RAM usage and exhausting the DHCP pool of DHCP server which prevented any legitimate clients from receiving IP addresses causing DoS attack on the network. Furthermore, the attacker introduced a rogue DHCP server to perform MITM attack which comprised availability and integrity of the network.

Similarly, APR poisoning enables attacker to capture the DHCP server's MAC address and then is able to mimic the DHCP server's MAC address as his own, which caused MITM attack in which the attacker could see confidential data. However, as literature suggested that I could lead to network instability but didn't show in the simulation. The assumption is as there is no real traffic that is generating on the network because of which there wasn't instability.

In STP, the attacker advertised superior BPDUs tricking the connected switch to assume there is a superior switch connected and making it the root bridge. This caused an unauthorized topology change, and further attacker could spam more BPDUs causing DoS attack in the topology.

VLAN hopping attacks, on the other hand, leveraged weaknesses in DTP to gain unauthorized access to restricted VLAN segments, potentially compromising sensitive data.

To mitigate attacks, several security measures were employed. Port security limited the number of MAC addresses on a port to prevent unauthorized access. DHCP snooping filtered DHCP messages, ensuring only valid devices get network configurations. Root guard prevented a switch from accepting another device as the root bridge, protecting the network topology. BPDU guard disabled ports receiving Bridge Protocol Data Units to stop rogue devices from changing the topology and during configuring mitigation for stp, due to

misconfiguration it led to broadcast storm and had turn off the switch to stop the broadcast loop. Dynamic ARP Inspection validated ARP requests and replies to prevent spoofing. Disabling Dynamic Trunking Protocol prevented automatic trunking and reduces VLAN hopping risks. Together, these measures provide robust network security.

These findings align with previous research highlighting the inherent security risks associated with protocols run on network switches. The observed increase in traffic and unauthorized access during attacks underscores the critical need for robust security measures in SME networks. Our findings align with existing literature, which emphasizes the effectiveness of mitigation strategies like port security, DHCP snooping, and others. Implementing these strategies significantly reduce risk of attack and empowers SMEs to safeguard their network infrastructure against the identified attacks.

5.1.2 Recommendations

In the digital age, small and medium-sized enterprises (SMEs) must prioritize network security to protect sensitive data, maintain customer trust, and comply with regulatory standards. Modern network switches that incorporate robust defensive mechanisms are essential for SMEs. A structured framework for selecting and deploying switches is recommended, considering their specific security and performance needs.

SMEs should focus on switches that support advanced security features such as Access Control Lists (ACLs), port security, DHCP snooping, DAI, loop guard, BPDU guard, BPDU filter and network segmentation. ACLs filter traffic based on various criteria, while port security restricts access by limiting the number of MAC addresses that can be learned on a port. Network segmentation, achieved through VLANs, isolates different network segments, not to use native VLAN, shutting down ports which are not in use, these steps reduce potential attack surface and containing breaches.

Switch firmware updates are crucial for protecting against vulnerabilities and ensuring device functionality. Vendors like Cisco, HP Aruba, and Juniper Networks regularly release updates for their switches, making them suitable options for SMEs. Managed switches provide greater control and flexibility, allowing administrators to configure, manage, and monitor the network more granularly.

The Cisco Catalyst 9200 series, HP Aruba 2930F series, and Juniper EX2300 series are recommended for SMEs due to their comprehensive security features, ease of management,

and regular firmware updates. Network infrastructure design with security in mind includes proper network segmentation, firewalls, and intrusion detection and prevention systems (IPS/IDS).

A network security policy outlines procedures for maintaining and updating network security, and regular training for IT staff on the latest security practices and threats can enhance overall security posture. By adopting a comprehensive approach to network security, SMEs can significantly reduce cyber threats and ensure data integrity and confidentiality.

5.1.3 Broader Implications

This research addresses a critical gap in network security for SMEs, which are often targeted by cybercriminals due to their perceived lack of robust security infrastructure. The findings can influence policy by encouraging regulatory bodies and network equipment vendors to adopt standardized security practices for SME network devices. In the long term, implementing the recommended mitigation strategies (port security, dynamic ARP inspection, and proper VLAN configuration) can empower SMEs to protect their valuable data, maintain business continuity, and build trust with their clients. Additionally, the cost-effectiveness of these strategies makes them an attractive option for resource-constrained SMEs.

Furthermore, the research paves the way for advocating for mandatory security standards for SME network equipment. This could involve collaborating with industry stakeholders to develop and implement baseline security requirements for network switches and other network infrastructure components commonly used by SMEs. By raising awareness and advocating for improved security practices, this research can contribute significantly to a more secure digital environment for SMEs.

6. CHAPTER 6: Conclusions

6.1.1 Introduction

This research aimed to enhance network infrastructure security for Small and Medium-sized Enterprises (SMEs) by identifying and mitigating vulnerabilities in network switches. To achieve this, we set out the following objectives:

- **Evaluate Security in Network Switch Protocols:** We analysed existing research to identify security mechanisms, vulnerabilities, and mitigation strategies for common switch protocols.
- **Assess Impact of Attacks:** Based on the literature review, we designed and tested various attacks on network switches in a controlled environment to understand their real-world impact.
- **Validate Mitigation Strategies:** We evaluated the effectiveness of existing mitigation strategies against identified attacks.
- **Propose Defence Mechanisms:** We aimed to propose cost-effective best practices for configuring Ethernet switches to prevent Layer 2 attacks, tailored for easy implementation by SMEs.

6.1.2 How Aims and Objectives Were Achieved?

Chapter 2: Literature review

We conducted a comprehensive review of network switch protocols, focusing on their security mechanisms and vulnerabilities. This provided a foundation for understanding current switch security.

Chapter 4: Design, Implementation, Results, and Analysis

In this chapter, we detailed the design and implementation of our experiments, followed by the results and analysis. We designed a series of tests to simulate Layer 2 attacks in a controlled environment, implemented the necessary configurations on network switches, and monitored their performance. The results highlighted the vulnerabilities and the effectiveness of various mitigation strategies. We analysed these findings to draw conclusions about the real-world applicability and efficiency of each strategy.

Chapter 5: Overall Discussion and Recommendations

Combining insights from previous chapters, we discussed and proposed best practices for configuring Ethernet switches to prevent Layer 2 attacks. Key recommendations included enabling security features such as DHCP snooping, port security, etc and regularly updating switch firmware.

By following these best practices, SMEs can enhance their network security and protect against common Layer 2 attacks. These defence mechanisms are designed to be cost-effective and straightforward to implement, ensuring even organizations with limited IT resources can safeguard their network infrastructure.

In conclusion, the research successfully achieved its aims and objectives by evaluating switch security, assessing attack impacts, validating mitigation strategies, and proposing practical defence mechanisms. The findings provide valuable guidance for SMEs to strengthen their network security and protect critical assets from cyber threats.

6.1.3 Limitations of the Study

The main limitations of this research include the controlled environment of the experiments, which may not fully replicate real-world conditions. Additionally, the study focused on a limited set of protocols and attacks, which may not cover all potential vulnerabilities. These limitations might have influenced the results, but steps were taken to ensure the validity of the findings, such as using diverse literature and attack scenarios.

6.1.4 Recommendations for Future Research

Future research should expand the scope by investigating a broader range of network switch protocols and attack vectors. This would provide a more comprehensive understanding of the evolving threat landscape for SMEs. Conducting research in real-world network deployments would further validate the effectiveness of mitigation strategies in practical settings. Additionally, exploring the integration of advanced security technologies, such as machine learning-based intrusion detection systems (IDS), could offer promising insights into proactive threat detection and prevention for SMEs.

6.1.5 Reflection

The project I worked on was a highly enriching and educational journey, requiring dedication, technical skill, and self-discipline. It presented both challenges and opportunities, testing my abilities and resilience. The project involved comprehensive research, data

analysis, and a detailed project plan with clear milestones and deadlines. The technical work involved designing, implementing, testing, and analysing various network attacks and their mitigations to meet quality standards.

The project allowed me to take full ownership of the initiative and see tangible results from my efforts. I documented the process, maintained records of progress, and adjusted the plan as needed based on findings and challenges encountered. My supervisor provided valuable insights and feedback, which greatly contributed to refining my approach and improving the overall quality of the project.

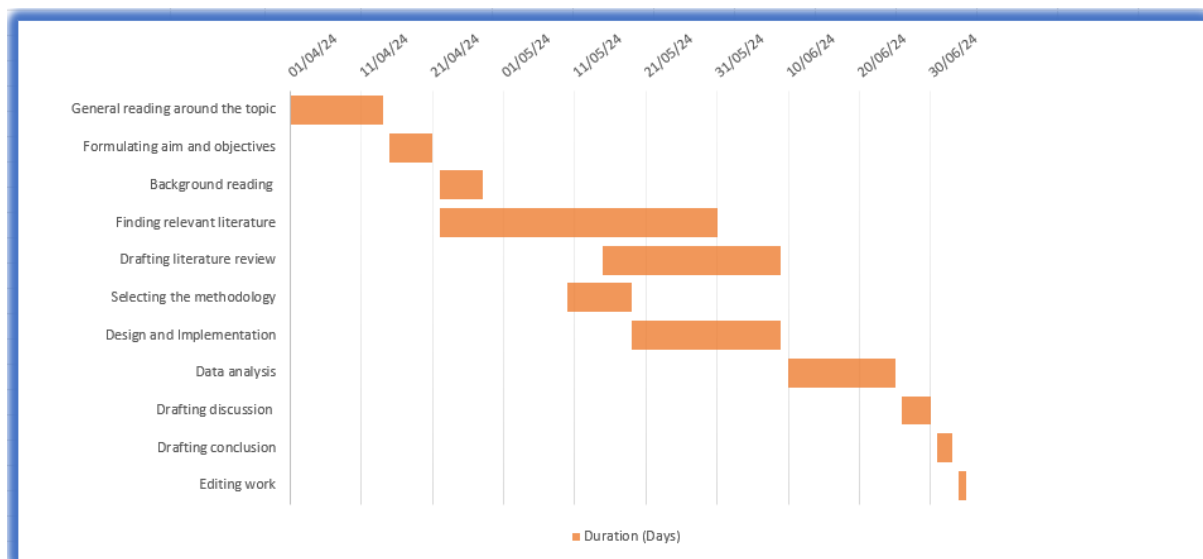
Throughout the project, I learned the importance of self-motivation and independent problem-solving, trusting my judgment and making decisions confidently. I also gained a deeper understanding of project management principles, particularly in planning, risk management, and resource allocation. Technically, I enhanced my skills in network security, particularly in configuring and managing switch security features.

Managing the project required a strategic approach to balance multiple responsibilities, prioritizing tasks based on urgency and impact, time management, regular self-assessments, and deadlines. My supervisor's guidance was instrumental in maintaining focus and providing direction throughout the process.

On a personal level, this project taught me the significance of resilience and adaptability, learning to stay focused and persevere during moments of uncertainty and setbacks. The experience reinforced the importance of self-discipline and commitment, as managing a project largely on my own required sustained effort and dedication.

In conclusion, this project was a profound learning experience that not only enhanced my technical and managerial skills but also fostered personal growth. The challenges faced and successes achieved under the guidance of my supportive supervisor have prepared me for future endeavours, and I am grateful for the opportunity to have undertaken such a dynamic and impactful project.

6.1.6 Gannt Chart



7. References

- [1] "What is a network switch?," SOPHOS, [Online]. Available: <https://www.sophos.com/en-us/cybersecurity-explained/network-switch>. [Accessed 23 06 2024].
- [2] "www.riskmanagementstudio.com," [Online]. Available: <https://www.riskmanagementstudio.com/information-security-challenges-in-smes/>. [Accessed 27 4 2024].
- [3] "cyforsecure.co.uk," [Online]. Available: <https://cyforsecure.co.uk/the-importance-of-it-security-for-smes/>. [Accessed 25 4 2024].
- [4] I. B. S. J. Carlos Rombaldo Junior, "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity," *Journal of SME Cybersecurity*, vol. 1, no. 29/9/2023, p. 23, 2023.
- [5] S. Z. a. P. K. Alladean Chidukwani, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," *IEEE Access*, 2022.
- [6] H. Baum, "DETECTION OF VLAN HOPPING ATTACKS," *taltech digikogu*.
- [7] X. M. H. Guo Mei, "Research on Preventing ARP Attack Based on Computer Network Security," *IOP Conference Series: Materials Science and Engineering*, vol. 452, no. 4, 2018.
- [8] T. N. Hubballi Neminath, "A closer look into DHCP starvation attack in wireless networks," *Computers & Security*, vol. 65, pp. 387-404, 2017.
- [9] J. M. a. R. B. Kaitlin Trumbull, "LAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments," in *DEF CON 24*, Las Vegas, NV, 2016.
- [10] I. BAXEVANOS, "Protecting with Network Security Strategies a Medium Size Enterprise and Implementing Scenarios Attacks and Countermeasures on Cisco Equipment," 2014.
- [11] Howard, "Basic Switch Security Concepts Explained," FS, [Online]. Available: <https://community.fs.com/article/basic-switch-security-concepts-explained.html>.
- [12] S. Convery, *Hacking Layer 2 : Fun with Ethernet Switches*, Cisco, 2002.
- [13] "yourshortlist.com," [Online]. Available: <https://yourshortlist.com/why-sme-cybersecurity-is-more-important-than-ever/>. [Accessed 26 4 2024].
- [14] "www.enisa.europa.eu," [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity.

[Accessed 26 4 2024].

- [15] "www.fortinet.com," [Online]. Available: <https://www.fortinet.com/uk/solutions/small-business/network-security>. [Accessed 22 5 2024].
- [16] "www.nebrcentre.co.uk," [Online]. Available: <https://www.nebrcentre.co.uk/12-cyber-security-trends-smes-should-be-aware-of-in-2024-and-beyond/>. [Accessed 22 5 2024].
- [17] "www.sharp.co.uk," [Online]. Available: <https://www.sharp.co.uk/sme-cybersecurity-exploring-the-confidence-gap>. [Accessed 22 5 2024].
- [18] "Business population estimates for the UK and regions 2023: statistical release," [Online]. Available: <https://www.gov.uk/government/statistics/business-population-estimates-2023/business-population-estimates-for-the-uk-and-regions-2023-statistical-release>. [Accessed 2024 06 18].
- [19] "Cloud vs. On-Premise: UK SMEs at a Crossroads," Techerati, 2023.
- [20] "CYBERSECURITY ISN'T A PRIORITY FOR SMES, RIGHT? CHANGE YOUR STRATEGY!," University of salford manchester .
- [21] A. Fitzgerald, "130+ Cybersecurity Statistics to Inspire Action This Year [2024 Update]," secureframe, 2024.
- [22] "Solution Guide: Solutions for LAN and WAN Protection | Allied Telesis," allied telesis, [Online]. Available: <https://www.alliedtelesis.com/gb/en/solution-guide/solutions-lan-wan-protection>. [Accessed 20 06 2024].
- [23] R. L. Brian Cusack, "Innovating additional Layer 2 security requirements fro a protected stack," *Australian Information Security Management Conference*, 2015.
- [24] W. P. Mohamed Muhidin, "Trends of digitalization and adoption of big data & analytics among UK SMEs: Analysis and lessons drawn from a case study of 53 SMEs," *Proceedings - 2020 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2020*, 2020.
- [25] K. S. M. A. Garcia-Martinez Luis Javier, "Untangling the relationship between small and medium-sized enterprises and growth: a review of extant literature," *International Entrepreneurship and Management Journal*, vol. 19, no. 2, pp. 455-479, 2023.
- [26] B. M. A. A. L. N. Gherghina Stefan Cristian, "Small and Medium-Sized Enterprises (SMEs): The Engine of Economic Growth through Investments and Innovation," *Sustainability 2020*, vol. 12, no. 1, p. 347, 2020.
- [27] J. B. E. Lacey David, "Review of Availability of Advice on Security for Small/Medium Sized Organisations," 2010.
- [28] O. J. Renaud Karen, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organizational*

Cybersecurity Journal: Practice, Process and People, vol. 1, no. 1, pp. 24-46, 2021.

- [29] C. S. T. i. S. t. M.-s. E. (. E. O. C. a. E. T. Needs, *Omolola Fagbule*, Bournemouth University, 2021.
- [30] L. O. P. T. C. Ilca Lucian Florin, "Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response," *Sensors (Basel, Switzerland)*, vol. 23, no. 15, 2023.
- [31] "Insider Threat Definition," fortinet, [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/insider-threats>. [Accessed 23 06 2024].
- [32] "7 Popular Layer 2 Attacks," pearsonitcertification, 25 02 2016. [Online]. Available: <https://www.pearsonitcertification.com/articles/article.aspx?p=2491767>. [Accessed 2024 06 23].
- [33] Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Network Design Fundamentals, Cisco Press., 2015.
- [34] "What Is Network Switching?," Cisco, [Online]. Available: <https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html#~capabilities>. [Accessed 20 06 2024].
- [35] Chiradeep BasuMallick, "What Is a Network Switch? Meaning, Working, Types, and Uses," spicework, [Online]. Available: <https://www.spiceworks.com/tech/networking/articles/what-is-network-switch/>. [Accessed 20 06 2024].
- [36] Howard, "How to Choose a Suitable Small Business Switch? | FS Community," 26 1 2022. [Online]. Available: <https://community.fs.com/article/how-to-choose-a-suitable-small-business-switch.html>. [Accessed 20 6 2024].
- [37] N. Inc, GS748T Smart Switch Soft ware Administration Manual, Netgear Inc, 2012.
- [38] Aruba Instant On 1930 Switch Series Management and Configuration Guide 2 Aruba Instant On 1930 Switch Series Management and Configuration Guide Aruba Instant On 1930 Switch Series Management and Configuration Guide, aruba instant, 2022.
- [39] "Security Standard – Network Security Design," 2018. [Online]. Available: <https://assets.publishing.service.gov.uk/media/65a66b4d640602000d3cb725/dwp-ss018-security-standard-network-security-design-v2.pdf>.
- [40] Howard, "Network Attacks Unveiled: Understanding the Threats to Your Switches," FS, [Online]. Available: <https://community.fs.com/article/network-attacks-unveiled-understanding-the-threats-to-your-switches.html>. [Accessed 20 06 2024].
- [41] Eric Vyncke, "Cisco - Layer 2 security," [Online]. Available: https://www.cisco.com/c/dam/global/da_dk/assets/docs/security2006/Security2006_Eri

c_Vyncke_2.pdf. [Accessed 20 06 2024].

- [42] "Ethernet Switching User Guide," [Online]. Available: <https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/layer-2-understanding.html>. [Accessed 20 06 2024].
- [43] S. K. a. S. H. S. Duangphasuk, "Design and implementation of improved security protocols for DHCP using digital," *ICON 2011 - 17th IEEE International Conference on Networks*, pp. 287-292, 2011.
- [44] "Global DHCP Services Market By Type (On-Premise, Cloud-Based), By Application (Small and Medium Enterprises, Large Enterprises), By Geographic Scope And Forecast," *Verified market reports*, 2023.
- [45] A. A. S. M. A. T. E. M. AbdulGhaffar, "Internet of Things based multiple disease monitoring and health improvement system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1021-1029, 2020.
- [46] C. L. Zhang Fuqiang, "OTP-SAM: DHCP security authentication model based on OTP," *Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2016*, pp. 346-350, 2016.
- [47] O. S. Younes, "Securing ARP and DHCP for mitigating link layer attacks," *Sādhanā*, vol. 42, 2016.
- [48] D. A.-A. ., A. A. M. ., F. K. Manar Aldaoud, "DHCP attacking tools: an analysis," *Journal of Computer Virology and Hacking Techniques*, vol. 17, no. 2, pp. 119-129, 2021.
- [49] J. N. Prabadevi B., "A review on various sniffing attacks and its mitigation techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, pp. 1117-1125, 2018.
- [50] V. Damjanovski, "Networking in CCTV," *CCTV*, pp. 410-477, 2024.
- [51] R. & L. T. Droms, *The DHCP Handbook* (2nd ed.), Sams Publishing, 2003.
- [52] A. a. C. An Analysis of DHCP Vulnerabilities, "AbdulGhaffar AbdulAziz,Kumar Paul Sumit,Matrawy, Ashraf".
- [53] W. K. R. S. H. O. C. N.-R. a. D. B. S. Jero, "Identifier binding attacks and defenses in software-defined networks," *26th USENIX Security Symposium*, pp. 415-432, 2017.
- [54] L. A. T. R. Shete Aishwarya, "DHCP Protocol Using OTP Based Two-Factor Authentication," *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, pp. 136-141, 2018.
- [55] S. K. Y. Mukhtar Husameldin, "Mitigation of DHCP starvation attack," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1115-1128, 2012.

- [56] S. T. D. Shresth Pratik, "Dynamic Host Configuration Protocol Attacks and its Detection Using Python Scripts," *Proceedings of the International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering, ICECONF 2023*, 2023.
- [57] D. D. D. a. M. Togan, "DHCP server authentication using digital certificates," *2014 10th International Conference on Communications*, pp. 1-6, 2014.
- [58] S. B. a. S. N. M. Agarwal, "Discrete event system framework for fault diagnosis with measurement inconsistency: case study of rogue DHCP attack," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 3, pp. 389-806, 2017.
- [59] T. L. B. A. a. J. T. K. Hornstein, "DHCP authentication via Kerberos," *IETF DHC Working Group*, 2001.
- [60] A. A. ., Nuhu, "MITIGATING DHCP STARVATION ATTACK USING SNOOPING TECHNIQUE," *FUDMA JOURNAL OF SCIENCES*, vol. 4, no. 1, pp. 560-566, 2020.
- [61] "Configuring DHCP Snooping - Cisco," CISCO, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/security/503_u2_2/Cisco_n3k_security_cg_503_u2_2_chapter10.html. [Accessed 4 5 2024].
- [62] A. Tong Yao, "A feasible method for realizing leakage of DHCP transactions under the implementation of DHCP snooping: To what extent can DHCP snooping protect clients from the cyberattack based on DHCP spoofing," *ACM International Conference Proceeding Series*, pp. 267-272, 2019.
- [63] C. Yaibuates Mayoan, "Starvation delayed dhcp service for enabling pool recovery," *Malaysian Journal of Computer Science*, no. SpecialIssue2, pp. 15-34, 2019.
- [64] S. Ali Salim M., "DESIGNING A SECURE NETWORK SOLUTION AGAINST DHCP ATTACKS," *Iraqi Journal of Information and Communications Technology*, vol. 1, no. 1, pp. 45-57, 2021.
- [65] "Switchport Security Concepts and Configuration," cisco, [Online]. Available: <https://www.ciscopress.com/articles/article.asp?p=1722561>. [Accessed 5 5 2024].
- [66] "Cisco Catalyst 1000 Series Switches White Paper," CISCO, [Online]. Available: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/white-paper-c11-743809.html>. [Accessed 5 4 2024].
- [67] J. D. L. Y.-S. J. H.-Y. J. a. J. H. P. Min Su Song, "DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments," *The Scientific World Journal*, 2014.
- [68] X. M. H. Guo Mei, "You may also like Research on Computer Network Security Vulnerabilities and Preventive Measures Based on Multi-Platform Wenchao Xing-Computer Network Security Analysis Modeling Based on Spatio-temporal Characteristics and Deep Learning Algorithm Lihua Wu," *IOP Conference Series*:

materials Science and Engineering , 2018.

- [69] "CVEdetails," [Online]. Available: <https://www.cvedetails.com/cve/CVE-1999-0667/>. [Accessed 23 4 2024].
- [70] "Nvd.nist.gov," [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2023-31190>. [Accessed 9 4 2024].
- [71] R. Siles, ""Real World ARP Spoofing" GIAC Certified Incident Handler (GCIH) Practical (Version 2.1a-Option 1: Exploit in Action) GIAC Certification Administrivia Version 2.5b," 2003.
- [72] "ARP Attack Protection Technology White Paper-6W100," 2020.
- [73] [Online]. Available: <https://www.bartleby.com/essay/S-ARP-is-a-Permanent-Solution-to-PK8RMN4C8BRA>. [Accessed 2024 06 02].
- [74] K. D. D. L. Yang Liu, "(PDF) Research of the ARP Spoofing Principle and a Defensive Algorithm," 2008.
- [75] J. Y.-S. H.-Y. J. H. Song Min SuLee Jae Dong, "DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments," 2014.
- [76] G. R. P. Zhao Yongjian, "ARP Spoofing Analysis and Prevention," *Proceedings - 2020 5th International Conference on Smart Grid and Electrical Automation, ICSGEA 2020*, pp. 572-575, 2020.
- [77] X. E. M. C. L. A. Andre P. Ortega, "Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," *Latin American Network Operations and Management Symposium*, 2009.
- [78] haword, "What Is DHCP Snooping and How It Works?," FS, [Online]. Available: <https://community.fs.com/article/what-is-dhcp-snooping-and-how-it-works.html>. [Accessed 2024 07 01].
- [79] "Dynamic ARP Inspection," [Online]. Available: Dynamic ARP Inspection. [Accessed 2024 06 01].
- [80] "Security Features on Switches," in *Network Security Technologies and Solutions (CCIE Professional Development Series)*, cisco, 2008.
- [81] "Security Configuration, Cisco Catalyst PON Series Switches," cisco, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_pon/software/configuration_guide/sec/b-gpon-config-security/preventing_arf_spoofing_and_flood_attack.html. [Accessed 2024 06 01].
- [82] P. N. N. Jain Richa, "WORKING OF SPANNING TREE PROTOCOL," *2018 JETIR October 2018*, vol. 5, no. 10, 2018.

- [83] S. F. A. J. R. M. Rehman Aleena, "Spanning tree protocol for preventing loops and saving energy in software defined networks along with its vulnerability and threat analyses," *Advances in Intelligent Systems and Computing*, vol. 857, pp. 1166-1180, 2019.
- [84] Z. S. Al-Salloum, "Topology-Aware Vulnerability Mitigation Worms: Defensive Worms," 2011.
- [85] A. Balchunas, Cisco CCNA Study Guide v2.71, 2014.
- [86] "Enhance Spanning Tree Protocol (STP) with Root Guard," Cisco, [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html> . [Accessed 02 06 2024].
- [87] Hewlett Packard Enterprise, [Online]. Available: https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8155_ra-2620_atmg/content/ch03s05.html. [Accessed 02 07 2024].
- [88] "Intro to Networking - Introduction to Virtual LANs (VLANs) and Tagging," [Online]. Available: <https://help.ui.com/hc/en-us/articles/222183968-Intro-to-Networking-Introduction-to-Virtual-LANs-VLANs-and-Tagging>. [Accessed 19 06 2024].
- [89] "How Virtual Local Area Network (VLAN) Technology Helps Small Business and Organization Cut Costs and Improve Network Performance in the Right Environment," [Online]. Available: <https://lignuniversity.com/blog/how-virtual-local-area-network-vlan-technology-helps-small-business-and-organization-cut-costs-and-improve-network-performance-in-the-right-environment>. [Accessed 24 06 2024].
- [90] "Trunk port," [Online]. Available: <https://nordvpn.com/cybersecurity/glossary/trunk-port/>. [Accessed 21 06 2024].
- [91] "Dynamic Trunking Protocol (DTP)," geeksforgeeks.org, 05 05 2023. [Online]. Available: <https://www.geeksforgeeks.org/dynamic-trunking-protocol-dtp/>. [Accessed 2024 05 03].
- [92] D. P. D. P. P. McMahon Richard A, "Building a wireless network infrastructure under budget constraints," *International Journal of Mobile Communications*, vol. 3, no. 1, pp. 445-456, 2005.
- [93] C. Hoffmann, "VLAN Security in the Lan and Man Environment," SANS insitutie, 2003.
- [94] "Cisco Networking Academy's Introduction to VLANs," in *Routing and Switching Essentials Companion Guide*, Cisco press, 2014.
- [95] [Online]. Available: https://research-methodology.net/research-philosophy/#_ftn1. [Accessed 05 06 2024].
- [96] W. C. A. Kaushik Vibha, "Pragmatism as a Research Paradigm and Its Implications for

Social Work Research," *Social Sciences* 2019, Vol. 8, Page 255.

- [97] "Deductive Approach (Deductive Reasoning)," *Business Research Methodology*, [Online]. Available: Deductive Approach (Deductive Reasoning) - Research-Methodology. [Accessed 2024 0 05].
- [98] "Chapter 10 Experimental Research," *Research Methods for the Social Sciences*, [Online]. Available: Chapter 10 Experimental Research | Research Methods for the Social Sciences. [Accessed 2024 06 05].
- [99] K. M. L. S. Hammarberg K., "Qualitative research methods: when to use them and how to judge them," *Human Reproduction*, vol. 31, no. 3, pp. 498-501, 2016.
- [100] "Eve," Eve-ng.net, [Online]. Available: <https://www.eve-ng.net/>. [Accessed 2024 06 05].
- [101] [Online]. Available: <https://www.vmware.com/products/workstation-pro/html.html>. [Accessed 2024 06 05].
- [102] "parrotsec.org," parrotsec.org, [Online]. Available: <https://parrotsec.org/>. [Accessed 2024 07 05].
- [103] "kali.org," kali.org, [Online]. Available: <https://www.kali.org/>. [Accessed 2024 06 05].
- [104] "<https://www.wireshark.org/>," [Online]. Available: <https://www.wireshark.org/>. [Accessed 2024 06 05].
- [105] "<https://www.kali.org/tools/yersinia/>," [Online]. Available: <https://www.kali.org/tools/yersinia/>. [Accessed 2024 06 05].
- [106] [Online]. Available: <https://www.ettercap-project.org/>. [Accessed 2024 06 05].
- [107] "VPCS," [Online]. Available: <https://docs.gns3.com/docs/emulators/vpcs/>. [Accessed 2024 06 05].
- [108] "Cisco Port Security Violation Modes Configuration," [Online]. Available: <https://study-ccna.com/cisco-port-security-violation-configuration/>. [Accessed 2024 06 19].
- [109] D. M. Tok Mevlut Serkan, "Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard," *Computers & Security*, vol. 109, 2021.
- [110] A.-N. A. C. B. A.-R. H. Mangut Heman Awang, "ARP Cache Poisoning Mitigation and Forensics Investigation," *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 1392-1397, 2015.
- [111] H. Team, "www.exploit-db.com," [Online]. Available: <https://www.exploit-db.com/docs/english/45050-vlan-hopping-attack.pdf>. [Accessed 9 2 2024].

