# American Journal of Multidisciplinary Research and Innovation (AJMRI)

ISSN: 2158-8155 (ONLINE), 2832-4854 (PRINT)

VOLUME 4 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Multidisciplinary Research and Innovation (AJMRI)

Volume 4 Issue 1, Year 2025
ISSN: 2158-8155 (Online), 2832-4854 (Print)
DOI: https://doi.org/10.54536/ajmri.v4i1.3763
https://journals.e-palli.com/home/index.php/ajmri

# Fortifying The Data Link Layer: An Analysis of Security Concerns

Md Mazedul Alam[1*]

**Article Information**

**Received:** September 08, 2024

**Accepted:** October 09, 2024

**Published:** January 17, 2025

**Keywords**

*Data Link Layer Attacks, OSI Model, Vulnerability*

## ABSTRACT

Network operations are separated into seven tiers by a conceptual model of networking known as the Open Systems Interconnect Model (OSI). This explains the way layers communicate with one another.This paradigm explains the way layers communicate with one another. I discuss common Data link layer attacks in this Research, along with possible defenses, and introduce new attacks.The data link layer is regarded as an extremely vulnerable point in a secure network Because each layer operates independently of the others; if the data is compromised at the Data link layer, it cannot be discovered at higher layers. The use of various attack tools by an attacker to exploit a network is described. My findings demonstrate how effective these attacks may be when a network administrator neglects to install suitable security at the Data link layer of the OSI model.

## INTRODUCTION

Network operations are separated into seven tiers by the Open Systems Interconnect Model (OSI), a conceptual framework for networking: Physical, Data Connection, Network, Transport, Session, Presentation, and Application layers are seven layers, respectively. This model specifies how layers converse with one another. Given how difficult it is for outside hackers to connect to a company's LAN, A network administrator normally does not concentrate on data link layer (Data link layer of OSI) security solutions. To protect Layer 3 and higher levels, several methods can be utilized, including packet filtering, access lists, intrusion detection systems (IDS), encryption techniques, and firewalls. The data link layer, on the other hand, lacks the granular controls required to withstand attacks against it. A network administrator typically gives very little thought to data link layer security and frequently disregards this region. Network damage may arise from Data link layer attacks. For instance, a CDP attack can cause a device to run out of memory and become unusable. Security Data link layer devices receive very little attention from the network administrator, which makes it very simple for attacks to be launched against the network.Social engineering is the practice of using deception and cunning techniques to acquire sensitive data. It is a non-technical sort of infiltration that primarily relies on human interaction and typically entails misleading others into breaching standard security protocols. High-level security measures in the upper layers are ineffective if the data is already hacked at Data link layer. The OSI model's layers all function without expertise. If a security breach is successfully carried out, any sensitive data on the network may be taken via a variety of methods. An attacker can carry out data link layer attacks using a variety of attack tools. A network administrator should monitor the network to identify any security holes. The most frequent attacks on LAN networks include attacks on the Cisco Discovery Protocol (CDP), ARP cache poisoning, VLAN hopping, Spanning Tree Protocol (STP), CAM table overflow, and STP manipulation.

### Problem Statement

The data link layer refers to the weakest connection in a safe network. Because they don't provide a safe connection between MAC Addresses and Internet Protocol (IP), the majority of Data link layer protocols are unsafe. A network administrator focuses more when a network is being developed. To take advantage of Data link layer flaws, an attacker needs a physical link. He or she could employ social engineering to obtain entrance to the building or pose as an engineer who has been called to the scene to resolve a technical issue. Additionally, a user has the option of plugging in an unapproved switch, which can allow other devices to connect to the network.

### Aim of the Research

The Research could aim to assess the effectiveness of various Data link layer security mechanisms, such as port security, VLANs, and MAC address filtering. The goal would be to analyze the strengths, weaknesses, and potential vulnerabilities of these mechanisms in real-world network environments.

## LITERATURE REVIEW

Because data link layer security has not yet been fully addressed, data link layer assaults are common in IP over Ethernet networks. The three most common data link layer sniffing attacks are port stealing, MAC flooding, and ARP poisoning. Using the network layer protocol ARP, an IP address is mapped to a physical machine address that is recognized by the local network, such

[1] Department of Computer Science and Engineering, University of South Asia, Bangladesh
[*] Corresponding author's e-mail: alam.isoeh@gmail.com

as an Ethernet address. When a host machine wishes to discover the physical address associated with an IP address, it broadcasts an ARP request on the network that contains the IP address. An ARP reply message containing the physical address of the host that holds the IP address is sent. ARP cache tables are maintained on each host computer in order to convert IP addresses to MAC addresses. Because ARP is a stateless protocol, a host will accept an ARP entry and update its ARP cache anytime it receives an ARP reply from another host, even if it hasn't submitted an ARP request for that reply (Phys, 2020).

The data link layer (L2) is a weak link in terms of security. Switches are key components in L2 communications and they are also used for L3 communications. They are susceptible to many of the same L3 attacks as routers, as well as many unique network attacks, which include CAM table overflow, VLAN hopping, STP manipulation, ARP Spoofing (ARP Poisoning), DHCP starvation (Nasir Siddique, 2015).

The OSI model has been established as a conceptual framework for the development of types of equipment, protocols, and other technologies of networks since 1984 Phys (2020) explains that in Ethernet, the data link layer employs physical addresses, and the ARP protocol is responsible for mapping IP addresses to MAC addresses. To achieve this, the Data link layer uses ARP tables, which are in charge of connecting each IP address to a MAC address. Made a very crucial point about how transparent the protocols are. Since the method of data transmission is public, anyone can examine the protocols used by the network. This makes it possible for anyone to set up a service or application on these and produce attacks from various places. Virtual network security: risks, solutions, and difficulties explain the unique qualities of the various protocols and their built-in weaknesses, and they also hint at a basic security setting configuration. For the in-depth analysis of network traffic, there are current recommendations for novel models of data objects.

## Theoretical Framework

### Open System Interconnection (OSI)

The physical layer is the first of the seven layers in the OSI layer model. The physical layer, layer one, controls the transmission of raw bits via communication channels and verifies that neither the sender nor the received bit number has been altered or is absent. It is also accountable for the physical connectivity of hardware. The data link layer, or layer two, provides trustworthy communication across the physical layer to other locations like LAN or Wide Area Network (WAN). It deals with physical addressing such as media access control (MAC) and logical link management. The data link layer can estimation error detection and flow estimation errors. Logical addresses and the full data routing process are dealt with at layer three of the network. The network layer also has problems with transit times and packet delays. Addresses are assigned to every packet. Packets can be sent from one destination to another destination point with the aid of assigned addresses.The transport layer, layer four handle data transit. The transport layer accepts the data before dividing it into smaller portions. Once the data has been updated, the network layer receives the data along with the assurance that all data components are correctly connected. The transport layer handles end-to-end connectivity, data delivery, and dependability as it moves data from the source to the destination. To make connections, layer five's session layer interacts with users and programs running on many machines. It is typically in charge of managing, closing, and opening sessions. The operating system is a component of the presentation layer (layer 6). It modifies the format of both incoming and departing data. Sixth-layer protocol controls the syntax and semantics of sent data. Communication between computers with different internal data representations is made feasible when the data structures are conveyed and distinguished by encoding and data formatting. The application layer contains the protocols for HTTP, FTP, and email. It lays out standards for how a user's application should connect to network services and utilize the network. The operating system or apps are communicated with through layer 7, the application layer. It is in charge of the end user's data display and data format.

**Table 1:** OSI Model Diagram

| Layer | Name | Protocol |
|---|---|---|
| 7 | Application | HTTP, FTP, TELNET, SSH, DNS |
| 6 | Presentation | SSL, TLS |
| 5 | Session | APIS, SOCKETS, WINSOCK |
| 4 | Transport | TCP, UDP |
| 3 | Network | IP, ICMP, IPSEC, ARP |
| 2 | Data Link | ETHERNET. PPP, SWITCH, BRIDGE |
| 1 | Physical | ETHERNET, FIBER, WIRELESS, USB |

### Basic Security Measures

The three main pillars of security are availability, integrity, and confidentiality. These three concepts are the essential cornerstones of security, without which no safe network can be constructed.

### Confidentiality

The appropriate individuals will be given access to the material while maintaining its confidentiality. The use of this security feature ensures that unauthorized individual won't misuse information and other valuable sources. To guarantee secrecy, information must be safeguarded both during transmission and processing. Implementing robust encryption is necessary to enforce confidentiality. Security flaws can be exploited using scanning programs like Wireshark. Other ways that confidentiality may be

compromised include human error, such as missing settings during the implementation of security mechanisms or the use of malicious software (Kai-Hau Yeung, 2008).

**Integrity**

Integrity ensures that data is protected from unauthorized individuals adding, deleting, and changing it. Although the data is printed exactly as it was received (maintaining data integrity), the original integrity of the information has been compromised. To preserve the integrity, access to vital resources must be restricted. Two systems, known as detection and preventive mechanisms, make up integrity. Information is shielded from modification or deletion by unauthorized individuals using prevention devices. Information breaches by unauthorized parties are not stopped by detection methods. Monitoring systems alert the administrator if integrity is compromised. Detection methods keep an eye on activity to spot network issues. Additionally, they can identify the precise location in the network where integrity was compromised.

**Availability**

Availability refers to how quickly a system can provide users with the necessary data. Access to authorized sources should never be denied to authorized people. assaults that cause interruptions, such as Denial of Service (DoS) assaults, might jeopardize availability. Access to necessary information without delay is ensured via availability. Redundancy and backup should be offered in case of interruption. To retrieve the necessary information, access channels must function properly. To ensure availability, the security strategy must be robust enough.

**Issues with Data Link Layer Security**

**Poisoning of the Address Resolution Protocol (ARP)**

Despite operating at Data link layer, this protocol offers services to layer two switched networks, the basis for communication is the usage of MAC addresses. Using the ARP cache, network addresses (IP) are converted into physically similar addresses, such as Ethernet addresses. ARP is a stateless protocol. It is incapable of handling hostile hosts because there isn't enough verification. Host A has to know host B's MAC address, which corresponds to the network address (IP), to communicate with host B within the same Local Area Network (LAN).If the host B MAC address is not listed in the ARP cache table, the Area Network (LAN) will broadcast an ARP request containing the destination IP address, both the source IP address and the destination MAC address.

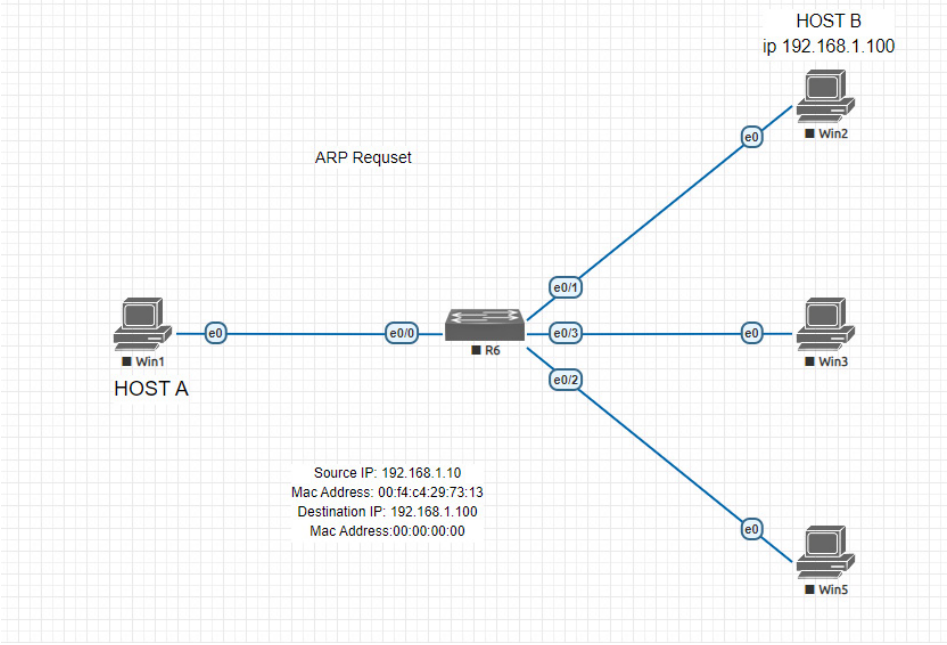


**Figure 1:** Make an ARP request
*Source: Developed by Author*

As shown in Figure 1 , only host B will provide the IP address and MAC address in response to host A's ARP request. The request won't receive a response from the other hosts. To minimize interactions, host A will keep track of host B MAC address in its ARP cache table. The saved MAC address will be used to establish communication between hosts A and B.

Malicious hosts may contaminate the ARP cache by sending fake ARP requests or answers due to a lack of authentication. An authentication method was not mentioned by the ARP protocol's creator. The ARP protocol therefore also allows for fictional queries and responses, which are all saved in the cache table. Faking a request or a response is another way to direct traffic to various servers. On a LAN network, attacks known as Man in the Middle (MITM) and Denial of Service (DoS) can be initiated by tampering with the victim host's ARP cache. By "poisoning" the ARP cache, an attacker

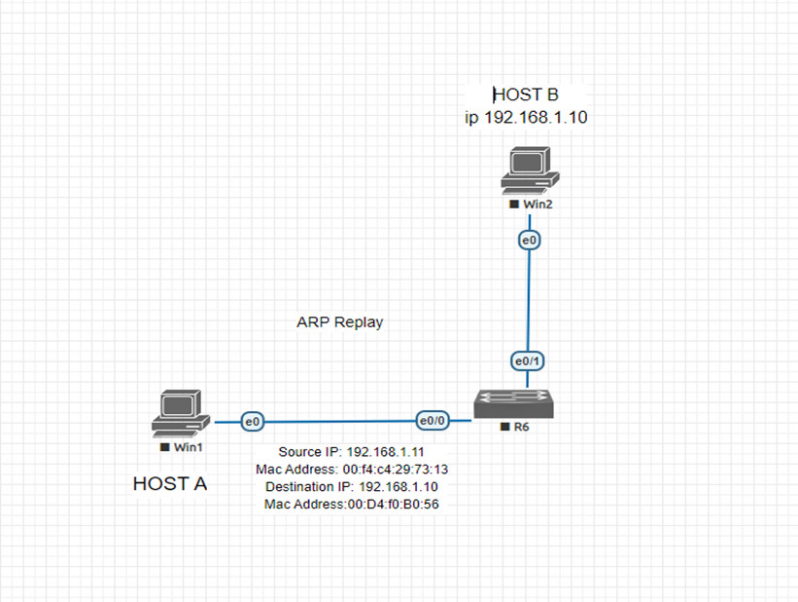


**Figure 2:** ARP Reaction
*Source: Developed by Author*

can control network traffic between two devices. By putting himself in between these two hosts, the attacker can spoof the IP addresses of two hosts and send all information in both directions. It is unknown to the victims that their traffic is being monitored. It is referred to as a "Man in the Middle Attack" (MITM). Poisoning the ARP cache is another method for initiating a denial-of-service attack. The victim is poisoned by employing faked MAC addresses and redirecting all traffic to the intruder host. The attacker blocks access to the internet.

**DHCP Starvation**

In LAN networks, IP addresses are assigned to computers either statically or dynamically for a predetermined period using the Dynamic Host Configuration Protocol (DHCP). Before a DHCP client may ask a DHCP server for setup information, it must first broadcast a DHCP DISCOVER packet across the local network. The DHCP server responds with a DHCP OFFER response if IP addresses are available. The DHCP client sends a DHC REQUEST to the DHCP server after accepting the offer. In response to this request, the DHCP server sends back a DHC PACK message. The DHCP client sends an ARP query to the local network to check if the IP address is already in use after getting the DHC PACK message. If an address is available, the client starts utilizing the configuration information provided by the DHCP server. If the DHCP server is not configured correctly, it may be attacked. An attacker uses the DHCP hunger approach to ping every DHCP address that is up for grabs. A denial-of-service attack and a network outage might result from this. A hacker can join their own rogue DHCP server and start giving clients IP addresses. Using the DHCP replies, an intrusive party can choose a new default gateway. All communication is directed to the modified default gateway, which now serves as an intruder's machine and is monitored by the network.

**VLAN Spoofing**

VLAN spoofing may occur if the switch port is configured with Dynamic Trucking Protocol or in trucking mode. In this attack, a hacker assumes the identity of a switch, connects to it as a trunk, and then utilizes the trunk port's 802.1q trunk tagging to gain access to all the VLANs. He is then free to "hop" into any available VLAN on the trunk. VLAN spoofing is widely used to spread Trojan horses, worms, and other malicious software through networks. Disable auto-negotiation and avoid using default VLANs on any ports to thwart this attack.

**Content Addressable Memory (CAM) Table Overflow**

A switch's MAC address database contains network data, such as the MAC addresses that are reachable on each physical switch port. There is a limit size for the MAC address table. It will overflow if more entries are added before the current one expires. Tens of thousands of fake entries can be added by a hacker to the MAC address database. If the MAC address table fills up, the switch enters hub mode, which floods all of the ports with traffic.

**Manipulation of the Spanning Tree Protocol (STP)**

STP is used to preserve the loop-free topology of the data link layer redundancy network. Loops are a useful tool for producing broadcast storms. Switches are pre-activated when they are placed. The switch that is designated as the Root Bridge is the one with the lowest configuration priority among the other switches. The switch with the lowest Mac address will designate itself as the Root Bridge if all switches have the same bridge ID.Once a switch chooses one, all other pathways to the Root Bridge will be closed and all data will be sent via the Root Bridge. Due to STP's lack of an authenticating mechanism for BPDU communications, an attacker can pretend to be the Root Bridge by sending bogus BPDU requests.

**Employee Training and Awareness**

Educating employees about security best practices, such as avoiding sharing network credentials and being cautious of social engineering attacks, can help mitigate the risk of insider threats and human error.

## MATERIALS AND METHODS

The OSI model's network layer is regarded as its weakest component. The data link layer (data connection layer), which is frequently disregarded and improperly handled, has the potential to be the weakest layer in the OSI model. To stop trojans, malicious emails, corrupted documents, and applications from the transport layer or the network layer, researchers have developed approaches. But rather than concentrating on the entire management system of a company, they overlook the data link layer and pay more attention to the security of the device itself. Although network managers frequently believe the data connection layer is secure, they frequently underestimate the attackers. Attacking the data link layer is not a simple process.

The following are typical ways that an attacker can influence IP and Wireless LANs. Any of the aforementioned attacks on the LAN or network of systems can have a major impact on an organization's overall security plan, vital electronic communication infrastructure, government management systems, and/or public institutions. Typically, mobile communication businesses and internet security service providers watch over a nation's key infrastructure. Denial-of-service (DoS) attacks, for instance, sometimes prevent the successful transmission of control information to the end devices. Due to the ease of access to commercially available frequency jamming devices, DoS attacks on Wireless LANs are simple to implement. Wi-Fi technology has developed incredibly quickly in recent years, and Wi-Fi 6 has reached its theoretical maximum speed of 9.6 Gbps. One might envision the future of Wi-Fi technology through this advancement in data transfer. There is a fundamental infrastructure of application software, protocols, and physical equipment that must connect across various wired and wireless networks, whether they are situated on Earth or in space. An international standard for communicating safely and confidently between various types of corporate networks while keeping the other OSI layers conversant with the presentation layer. Each OSI layer is distinct from the others, the entire network is extremely vulnerable to attack, especially the data link layer when compared to other layers. In contrast to other layers, Data link layer network security issues are typically not fully handled; instead, people concentrate on the security of the device for the entire management system. This paper succinctly and clearly discusses the problems with network security that arise from not doing data link layer hardening, and how this can increase the vulnerability of a local area network (LAN) or system of networks to various types of attacks, including denial-of-service (DoS), MAC flooding, ARP spoofing, VLAN hopping, DHCP attacks, and Spanning Tree Protocol. We require a brief overview of the data connection layer to fully comprehend the network security challenges and issues in this layer. The International Organization for Standards (ISO) designed the OSI seven-layer model so that various device types with various software programs loaded, unique physical properties, and interfaces can communicate with one another securely and confidently. The present layer serves all layers above it, and all layers above it depend on the functionality of the layer to which it is attached at the bottom.

## RESULTS AND DISCUSSION

**ARP Poisoning (also known as ARP Spoofing)**

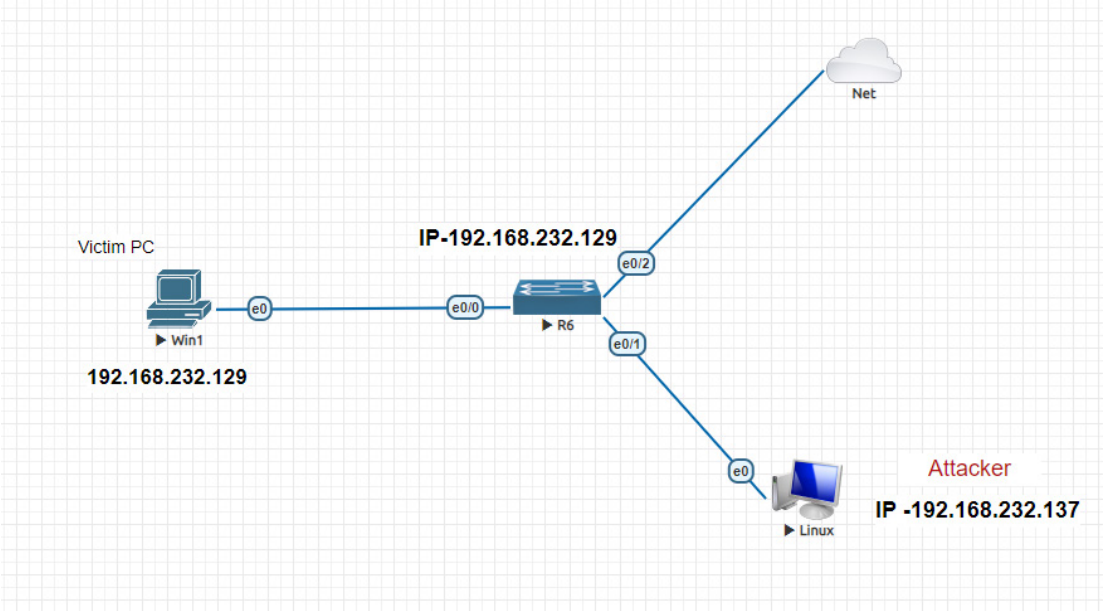


**Figure 3:** Example of an ARP cache poisoning attack
*Source: Developed by Author*

An illustration of an ARP cache poisoning attack can be found in Figure 3 The attacker's PC is directly connected to the switch. A perpetrator of this attack used the attack tool Ettercap to carry it out. With the use of the sniffer program Bettercap, a Man-in-the-Middle attack on a local area network is often carried out. Man-in-the-middle attacks are made possible by poisoning the ARP cache. Since we are connected via cable and the attacker PC has access to both Ethernet and WIFI, "e0/1" is selected. A list of all hosts on the local network as well as the host scanning actions performed by Ettercap will be presented. Select the host that will be the object of the attack, and then start sniffing on it. Starting We start the Ettercap menu of ARP poisoning. A sniffing program called Wireshark is launched at the same
time to catch and analyze the packets.

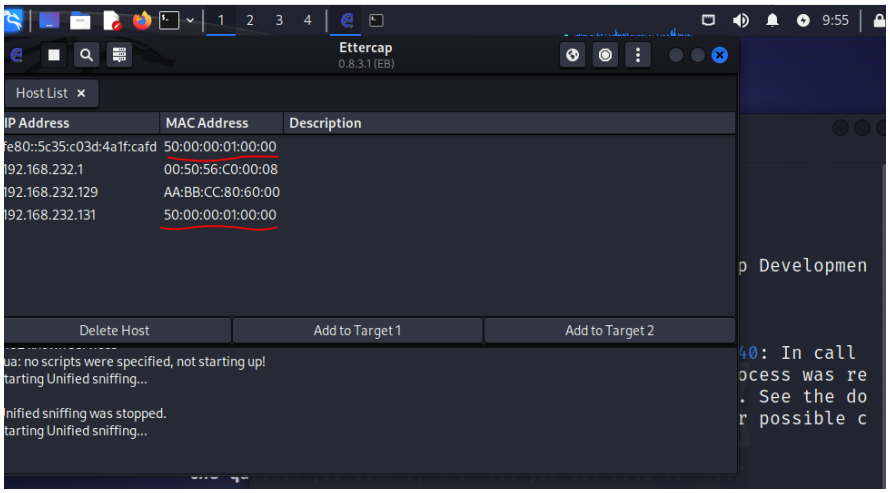


**Figure 4:** The poisoning of the ARP Cache
*Source: Developed by Author*

Figure 4 shows how an attacker delivered his MAC address to both targets. Both the victim PC1 and the switch advertised the MAC address 50.00.00.01.00.00, as shown in Figure 4. The same MAC address is broadcast with the intention of routing network traffic to the attacker's device. The attacker's PC achieved his objective of recording the dialogue between the two gadgets.

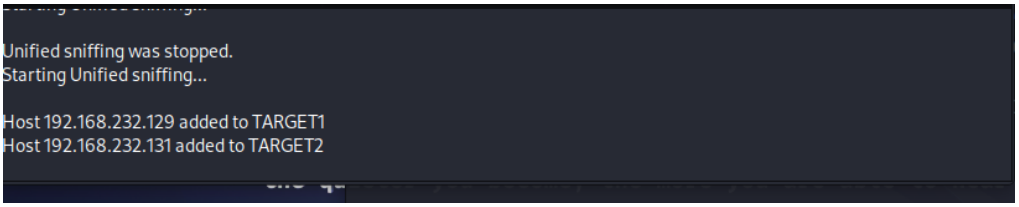


**Figure 5:**
*Source: Developed by Author*

Figure 5 shows how an attacker delivered his MAC address to both targets. The switch and the victim PC1 were both using the MAC address 50.00.00.01.00.00, as shown in Figure 5. The same MAC address can be used by an attacker to direct network traffic to their device. The communication between the two devices was successfully intercepted by the attacker's PC.

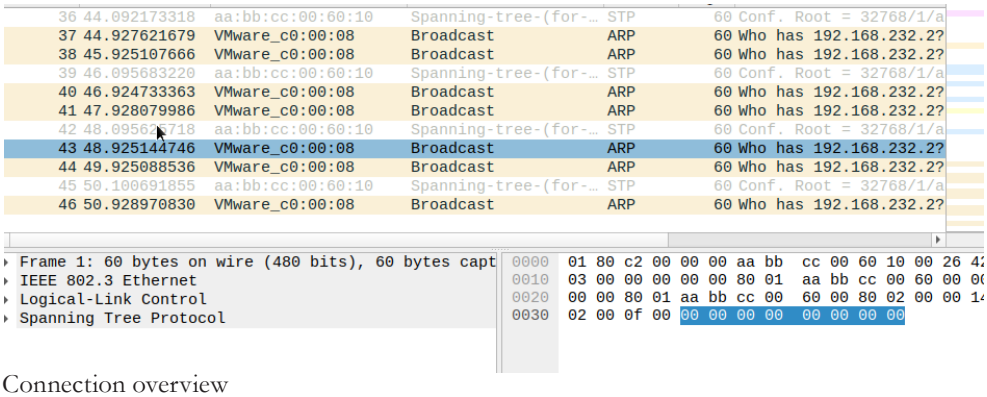


**Figure 6:** Connection overview
*Source: Developed by Author*

Figure 6 shows the password that was entered by the victim, PC1, to create a telnet connection. As seen in image 6, the password is visible to the PC that is being attacked. The creation of a link between two devices and the recording of communication between PC1 and the switch are both shown in Figure 6.

**CDP Attack**

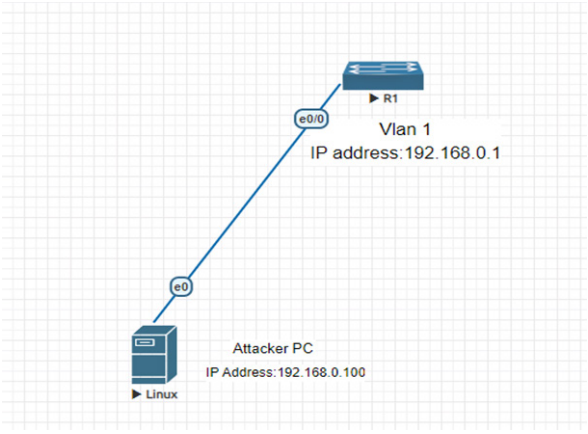


**Figure 7:** Scenario For A CDP Attack
*Source: Developed by Author*

In Figure 7, we show how to carry out a CDP assault. The switch is directly connected to the attacker's PC. This attack can be carried out by an attacker utilizing an IPRPAS attack tool. This utility was created to target switches and routers. As seen in Figure 8, the assaulting tool IRPAS is installed and launched on the attacker's machine to launch the attack.
A spoofing and flood attack can be launched using the IRPAS tool. We can create a spoof entry to carry out a spoofing attack by using the command that follows.


**Figure 8:** CDP attack information
*Source: Developed by Author*

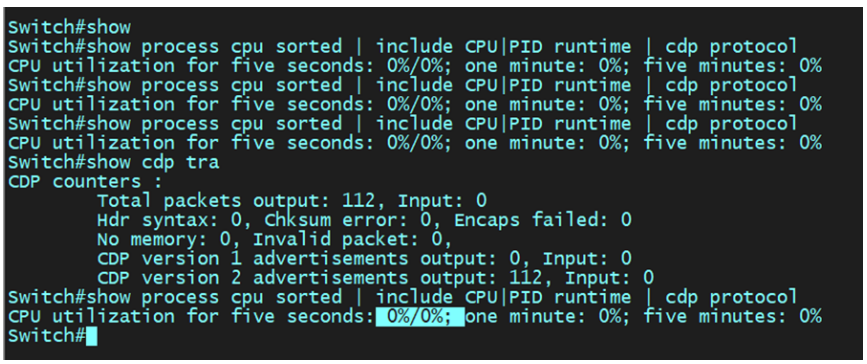


**Figure 9:**
*Source: Developed by Author*

The successful transmission of false information by an attacker is seen in CDP image 9. The CDP displays the wrong neighbor's data. There is no means of authentication for CDP. The network is not negatively impacted by this attack, but the network administrator may become confused and upset. of the attack's outcome

```
uniAsia#show cdp neighbors detail

Device ID: Switch
Entry address(es):
Platform: cisco PT3000, Capabilities: Switch
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 172

Version :
Cisco Internetwork Operating System Software
IOS (tm) PT3000 Software (PT3000-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: Switch
Entry address(es):
Platform: cisco PT3000, Capabilities: Switch
Interface: FastEthernet0/2, Port ID (outgoing port): FastEthernet0/1
Holdtime: 132

Version :
Cisco Internetwork Operating System Software
IOS (tm) PT3000 Software (PT3000-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
```

**Figure 10:** Neighbors Details
*Source: Developed by Author*

Figure 10 depicts the outcome and demonstrates how the switch memory was nearly full when the switch functionality crashed owing to memory fragmentation.

**DHCP Starvation**

we showed how to exploit a DHCP server. Figure 11 shows two linked PCs, a Layer 3 router, and a Data Link

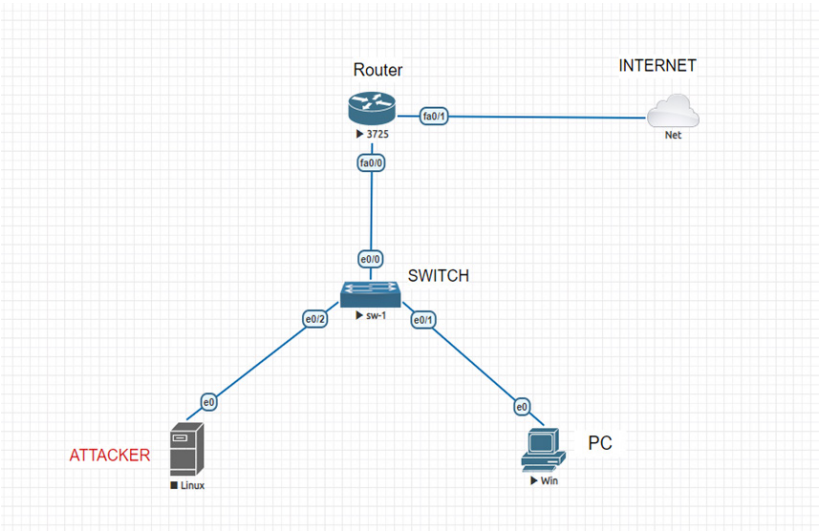


**Figure 11:** Example of DHCP Starvation Attack
*Source: Developed by Author*

Layer switch. IP addresses are automatically assigned to clients thanks to a technology called dynamic host control protocol (DHCP). In order to assign IP addresses to clients, the router is configured with a DHCP server. The DHCP server is not a secure protocol and does not have any security safeguards. An attacker can connect his attacker machine to a server and launch the assault from there if the switch is not set up properly to defend against DHCP hunger attacks. The DHCP hunger attack was carried out by an attacker using the Yersinia tool. Yersinia frequently uses fictitious MAC addresses to send discovery packets over a DHCP server. Up until it uses up all of the IP addresses in its DHCP IP pool, the DHCP server responds with ACK packets. The attacking

machine has leased all of these IP addresses. It may benefit the attacker if they carry out a man-in-the-middle attack or bring about network failures.

**VLAN Spoofing**

The results of our VLAN spoofing attack on a Data link layer switch are provided in Appendix B. We showed

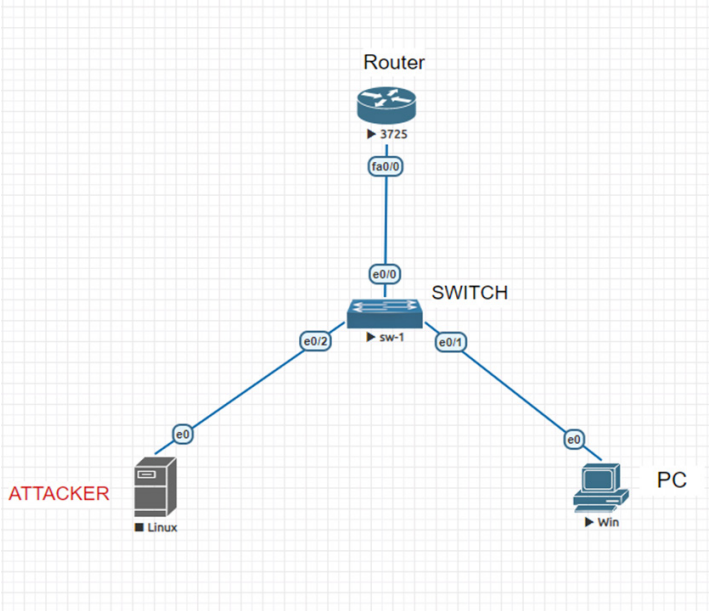


**Figure 12:** Example of a VLAN spoofing attack
*Source: Developed by Author*

how to do it in Figure 12. One Data link layer switch and one linked attacker PC are shown in the diagram. All VLAN information on the switch is transmitted via a trunk port. Automatic VLAN updates are sent from switch to switch or switch to the router via VTP (VLAN Trunking Protocol). An attacker can plug his attacker machine into a switch and begin attacking that machine if the switch is improperly configured to defend against a VLAN spoofing attack. This attack was carried out by an attacker utilizing the "Yersinia" attack tool. Ports on Cisco Catalyst switches should always be in auto mode during Trunking. All ports are described as being in "dynamic desirable" mode, and should they receive Dynamic Trunking Protocol (DTP) frames. Using this method, he can sniff all of the traffic across all VLANs. This type of attack may reveal the login and password information. He can also use this method to change all information about VTP with his data and remove all information about VTP.

```
Switch>show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch>show vlan bri
Switch>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch>
```

**Figure 13:** Example of a VLAN spoofing attack
*Source: Developed by Author*

**Cam Table Overflow**

We identify the security flaws to explain the CAM overflow attack. The results of our CAM table overflow attack on a Data link layer switch are provided in Appendix E. We described how to do this in Figure 14. One Data link layer switch and two connected computers are shown in Figure 14. The switch contains a fixed-size CAM table to store MAC address information. The switch is directly connected to the attacker's PC. In this instance, the attacker used an attack tool named "sniff" to carry out the attack. The switch's CAM table gets filled up by a massive number of phony MAC addresses sent by this attack tool. The entire number of MAC Address spaces that were accessible before the attack is shown in Figure 15. Figure 15 shows the total number of available MAC Address spaces before the attack.

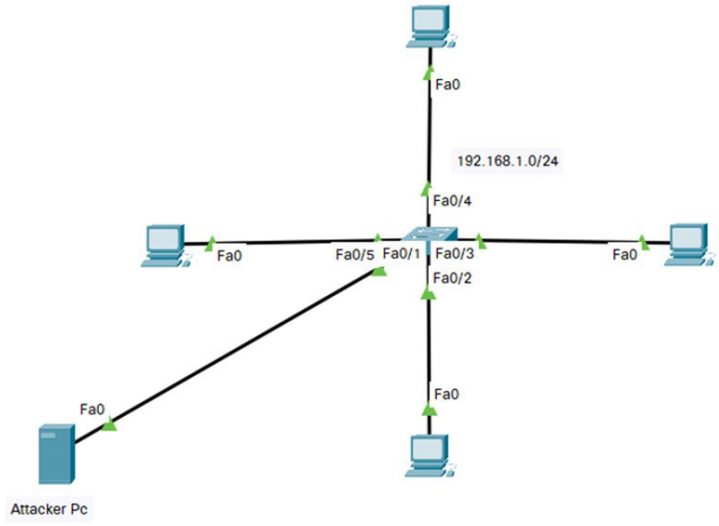


**Figure 14:** Cam Table Overflow Scenario
*Source: Developed by Author*

```
*May 10 08:51:31.936: %SYS-5-CONFIG_I: Configured from console by console
uniAsia#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 1
Static  Address Count  : 0
Total Mac Addresses    : 1

Total Mac Address Space Available: 176842276

uniAsia#
```

**Figure 15:** Cam Table Available Space
*Source: Developed by Author*

Two MAC addresses on Port 5 and one MAC address on PC1 are dynamically learned by the switch. The PC's MAC address and Kali OS's MAC address are the two MAC addresses on Port 5. On EVE-NG, the Kali OS has been installed. By entering a command into the attacking machine's terminal, we started the attack. The memory of the cam table, as illustrated in Appendix E, is filled with hundreds of phony MAC addresses sent by this attacking tool. The cam table in Figure 16 became overpopulated with erroneous MAC entrie

```
uniAsia(config)#end
uniAsia#
*May 10 08:58:33.395: %SYS-5-CONFIG_I: Configured from console by console
uniAsia#sho
uniAsia#show mac
uniAsia#show mac add
uniAsia#show mac address-table cou
uniAsia#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 1
Static  Address Count  : 0
Total Mac Addresses    : 1

Total Mac Address Space Available:0

uniAsia#
```

**Figure 16:** Cam Table Overflow Result
*Source: Developed by Author*

The difference between a hub and a switch is that a switch conveys a message directly between two devices that are already conversing, However, a hub communicates with any device that will listen via a network. We can see from the cam table attack that we force the switch to run out of memory when learning new addresses. In this scenario, the switch will behave like a hub and flood all ports with packets. Anyone can then capture the switch's packets at that point.

**Wireless Local Area Network Security**

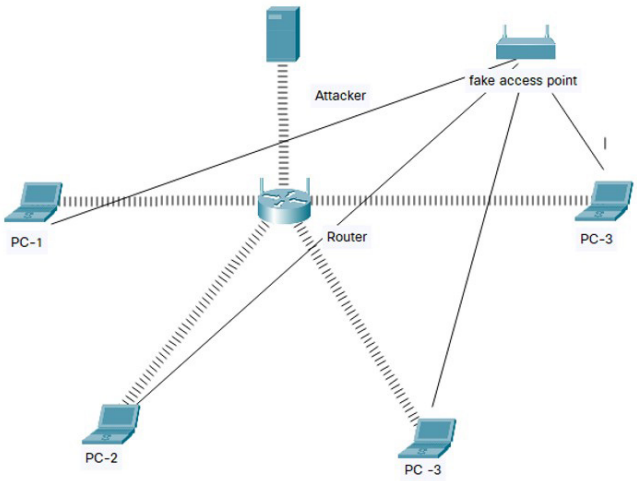


**Figure 17:** Wireless Local Area Network Security
*Source: Developed by Author*

IEEE 802.11 defines the optional protocol known as Wired Equivalent Privacy (WEP), which is based on the stream cipher RC4 encryption technology (wireless LAN medium access control (MAC) and physical layer). The WEP was designed to provide wireless networks with the same level of confidentiality as a traditional wired network. Nevertheless, studies have shown that IEEE 802.11's techniques are not trustworthy.

In order to improve wireless LAN security, the IEEE 802.11i amendment including MAC security enhancements for the IEEE 802.11 standard was approved in 2004. Wi-Fi Protected Access 2, or IEEE 802.11i, introduces a new security architecture called the Robust Security Network (RSN) (WPA2).The IEEE 802.1X standard (EAPOL) for access control and the Advanced Encryption Standard (AES) for encryption are the two areas where the 802.11 architecture is to be improved in this amendment. The new standard also defines a Transient Security Network (TSN) that enables the simultaneous operation of RSN and WEP systems, as well as improvements to increase the security of pre-RSN hardware through software upgrades.

Temporal Key Integrity Protocol (TKIP) for pre-RSN WLAN devices and the AES-based Counter-Mode/ Cipher Block Chaining Message Authentication Code (CBC-MAC) protocol (CCMP) are the two data privacy protocols that RSN defines in the IEEE 802.11i standard. The Wi-Fi Alliance chose TKIP, the WEP upgrade, before the 802.11i standard. WPA is another name for this portion of the RSN architecture.

**New Data link layer Architecture Security**

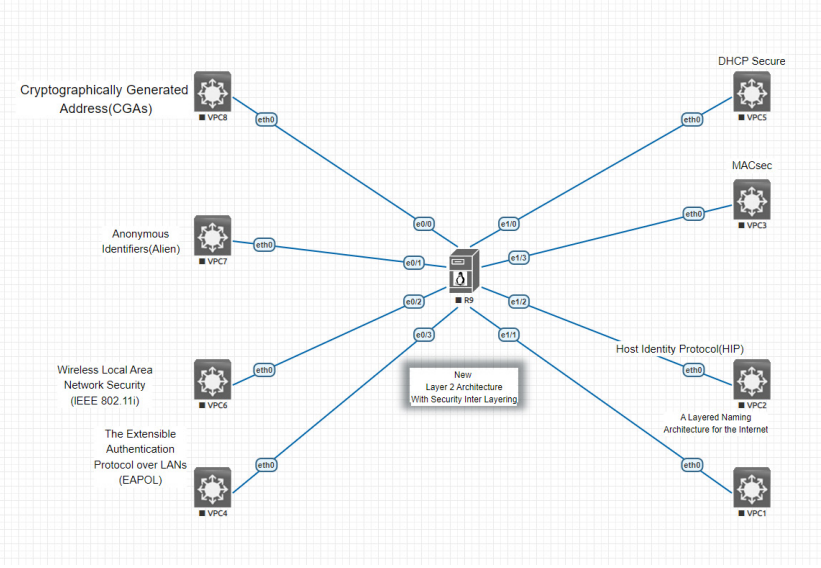


**Figure 18:** New Data link layer Architecture Security
*Source: Developed by Author*

**Discussion**

**ARP Poisoning**

we used Dynamic Arp Inspection (DAI). Before configuring the DHCP snooping, we enabled it. After setting up DAI, we reran the assault and obtained the outcome depicted in Figure 19.

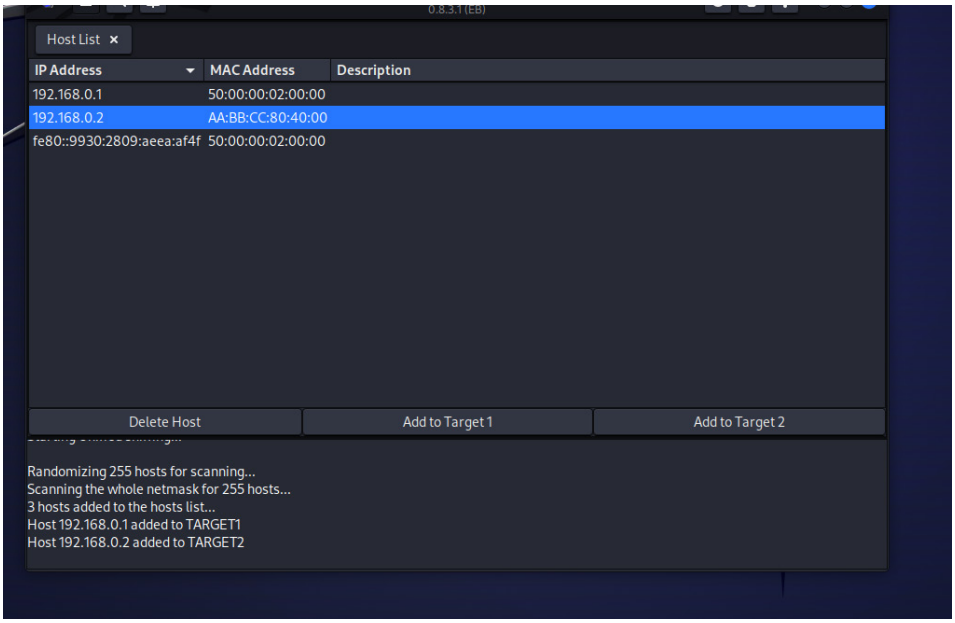


**Figure 19:** Result after configuring DAI
*Source: Developed by Author*

Figure 19 demonstrates an attempt to send an ARP packet by a host with the IP address 192.168.0.1. Because the packet was received over an untrusted interface, the DAI intercepted it. The packet was deleted as indicated in Figure 19 because it did not fit the IP-Mac binding table. ARP packets are verified using DAI, a security feature. All VLANS have DAI and DHCP snooping turned off by default. Since DAI needs the DHCP snooping database, DHCP snooping must be enabled before DAI is implemented. The APR packets that are received on untrusted ports are examined by DAI. When it intercepts an ARP packet, it checks the received packets against the IP-Mac binding table and drops them if they don't match. Additionally, it may verify packets that are part of a user-created static ACL. DAI gives the statics ACL priority over the DHCP snooping binding database table. The static ACL table and the DHCP snooping binding database are checked by DAI against ARP packets. Another method for preventing an ARP spoofing attack is to add static ARP entries to the client hosts. This method prevents an attacker from including fake ARP entries. Static ARP entries are, however, very challenging to maintain, especially in big networks. To identify ARP spoofing attacks, many Intrusion Detection Systems (IDS) can be deployed, including snort, ARP cache watch, and Decaffeinate ID. Any change in the MAC addresses can be promptly detected by them. Additionally, if any changes in the MAC addresses are found, they notify the user via messaging. These IDS are only capable of detection; they cannot guard against ARP spoofing assaults. The disadvantage of this method is that the attacker can quickly accomplish their objectives before the network administrator responds to the attack [4]. The best method for thwarting a cam table overflow attack is Dynamic ARP Inspection (DAI) and DHCP snooping, according to a comparison of the aforementioned predetermined solutions. All of the solutions mentioned above are not just applicable to Cisco switches. These can also be used in switches made by manufacturers like HP, Juniper Networks, Netgear, and Huawei, among others.

**CDP Attack**

A CDP attack can be lessened by turning off CDP. Disabling CDP globally or for each interface is the recommended approach. Every device on the local network should be running CDP if CDP is being utilized for security or troubleshooting operations. On interfaces connected to the external network, such as internet service provider (ISP) interfaces, it should be disabled, but. This attack can only be carried out on Cisco equipment because CDP is a proprietary protocol that only operates on hardware made by Cisco. An identical defense against the CDP attack is offered by Steve A. Rouille and Sean Convey as well (Saurabh Malgaonkar & Rohan Patil, 2017).

**DHCP Starvation**

we introduced port security to prevent connections from illegal devices. One of the most crucial security features in Cisco Data link layer switches is port security. On Cisco Data link layer switches, where we tested this port security, we obtained the best protection for the switch against this DHCP starvation attack. If the switch ports are bound to the maximum number of MAC addresses, an attacker

will not be able to connect his computer to the switch. Juniper Networks offers a similar method to counteract DHCP starvation attacks. Another method that can be used to counteract DHCP assault is DHCP snooping. Rogue DHCP server assaults can be prevented with this technique. Port security is ineffective at preventing attacks on rogue DHCP servers. A host connected to the switch is an example of an untrusted equipment whose DHCP communications are monitored and managed via DHCP snooping. Information from intercepted DHCP conversations is used to generate and update a database table for DHCP snooping. Network access is granted to hosts with the appropriate bindings. Roui (2008) and Bhaiji (2005) discussed how to counteract this attack by putting port security measures in place on all network switches, like capping the amount of MAC addresses that can be connected to a port. These answers resemble our answers.

**CAM Table Overflow**

"Port security" is a defense against the cam table overflow attack that is presented in the Blackhat research report. It serves as a typical and fundamental defense against a cam table overflow attack.

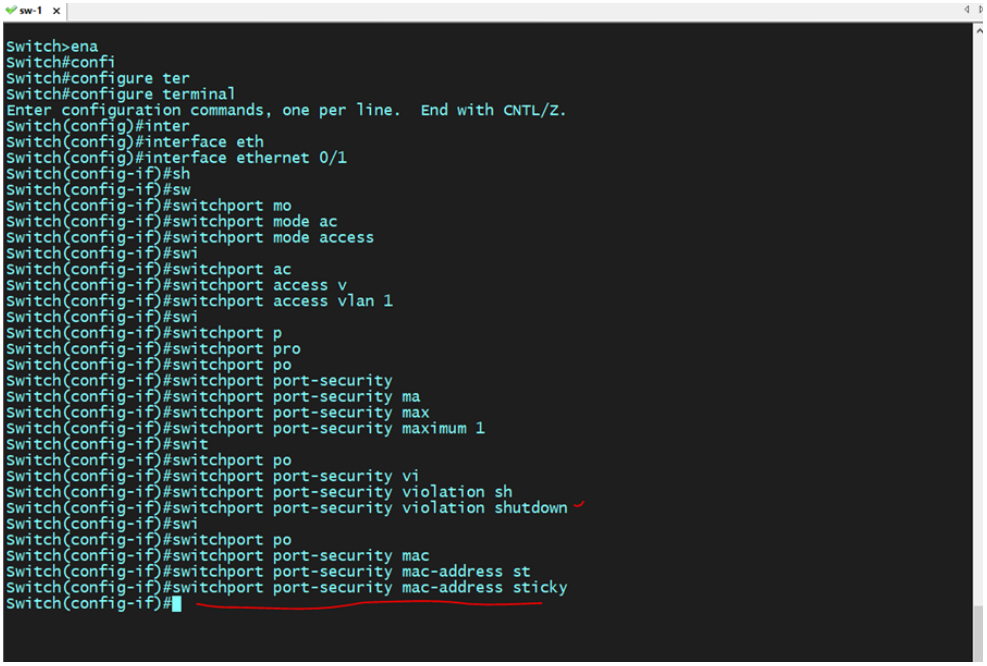


**Figure 20:** Port Security configure
*Source: Developed by Author*

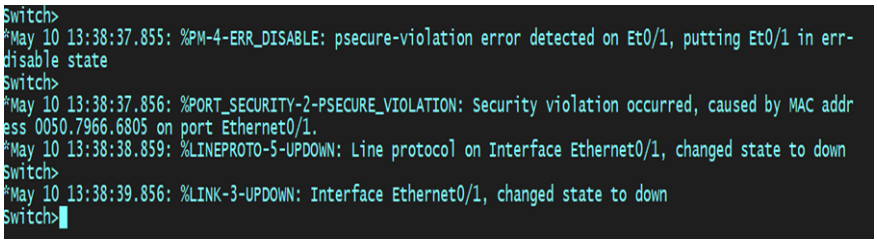


**Figure 21:** Result after configuring port security
*Source: Developed by Author*

After configuring port security, we conducted an attack, and port interface et0/1 discovered more MAC addresses than permitted, as shown in Figure 21. This causes the port et0/1 in Figure 21 to be switched to err-disable and shut down, as seen there. In Appendix E, there are further figures related to the CAM overflow attack. Port security is one of the most important security features of Cisco Data link layer switches. Switch ports are designed to prevent overflow attacks on the CAM table by implementing MAC address communication limits. The following secure MAC addresses are configurable: Secure, fixed MAC addresses: With the switch port, port security MAC address interface configuration command, they can statically configure each secure MAC address. The switch's operating configuration will be updated using these MAC addresses, which will also be kept in the address table. Dynamic secure MAC addresses: The port can safely learn the MAC addresses of connected devices dynamically; these addresses are only stored in address tablesAll addresses that are dynamically learned are removed if the port is linked down. Secure MAC addresses that stick: These can then be saved in

the operating configuration of the address table, either explicitly defined or dynamically learnt.Ports won't have to learn these addresses again even if the switch restarts if we store them in configuration files. The identical solution is offered in a research paper published in the SANS Institute InfoSec Reading Room, and the same outcome is obtained. Other switches like Juniper, HP, and Netgear can also employ this strategy. Combining DHCP snooping with Dynamic ARP Inspection (DAI) is a different way to stop a cam table overflow attack. This method can be used to mitigate several Data link layer attacks.

## CONCLUSION

Most Data link layer protocols lack authentication, which makes them insecure. If Data link layer devices are not properly secured, an attacker can use a variety of attack tools to exploit security flaws. In this Research, we argued that the optimal method for identifying vulnerabilities and securing a network is to conduct attacks for learning and testing purposes. A network administrator can benefit from the techniques and methodologies mentioned in this Research when performing security testing. In this Research report, we used the "port security" approach to prevent CAM table overflow, the "dynamic ARP inspection solution to prevent ARP poisoning, and the "root guard" and "BPDU guard" to prevent STP manipulation. Furthermore, this Research paper presents the results of these attacks. To obtain the results, the solutions are tested using the attacking tools Yersinia, sniff, Ettercap, and IPRPAS. By carefully deploying the security setup, network threats can be reduced. None of the solutions are exclusive to Cisco switches. Other switch manufacturers, such as HP, Juniper Networks, Netgear, and Huawei, among others, can incorporate these. However, each switch vendor has somewhat different configuration commands. The CDP attack only works on Cisco devices because CDP is a Cisco proprietary protocol that only operates on devices made by Cisco. Mitigating, Data link layer attacks involves implementing various security measures, such as robust access control mechanisms to prevent unauthorized devices from connecting to the network. Regularly updating and patching network devices to address known vulnerabilities. Enforcing robust authentication and encryption protocols to safeguard confidential information while it's in transit. Monitoring network traffic and detecting anomalies or suspicious behavior. Configuring switches and network devices with security and best practice settings. effectively using VLANs and network segmentation to reduce the impact of possible attacks. Educating network administrators and users about the risks and countermeasures related to Data link layer attacks. It is crucial to stay up to date with the latest security practices and consult with cybersecurity experts for the most current information on mitigating Data link layer attacks.

## REFERENCE


Altunbasak, H. C. (2006, November 20). *Data link layer security inter-layering in networks.* Retrieved from http://hdl.handle.net/1853/13974

Chung, C. J. (n.d.). *Network attacks.* Retrieved from https://www.uniteng.com/wiki/lib/exe/fetch.php?media=classlog:computernetworksecurity:12-network_attackslayer4-and-above.pdf

Chanthati, S. R. (2024). Artificial intelligence-based cloud planning and migration to cut the cost of cloud. *American Journal of Smart Technology and Solutions, 3*(2). https://doi.org/10.54536/ajsts.v3i2.3210

Khan, H. M., & S. M. (2024). Detecting security system misconfiguration threats in cloud computing environments. *American Journal of Innovation in Science and Engineering, 3*(2). https://doi.org/10.54536/ajise.v3i2.3272

Mohsin, S. M. (2020). Network security issues of data link layer. *Proceedings of the 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* 1–7. https://doi.org/10.1109/ICOMET46343.2020.9105242

Mustafa, A. S. (2015). *Data link layer security problems and solutions.* Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-27574

Nasir Siddique, M. A. (2015). *Data link layer security problems.* Digitala Vetenskapliga Arkivet. Retrieved from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A825849

Phys, G. L. (2020). Research on computer network security problems and protective measures. *IOP Conference Series: Materials Science and Engineering, 12.*

Santos, G. M., & Marcillo, P. A. (n.d.). *Security in the data link layer of the OSI model on LANs wired Cisco.* Retrieved from https://www.researchgate.net/publication/323369974_Security_in_the_data_link_layer_of_the_OSI_model_on_LANs_wired_Cisco

Saurabh Malgaonkar, A. R. (2017). Research on Wi-Fi security protocols. *International Journal of Computer Applications, 162*(7), 1–8. https://doi.org/10.5120/ijca2017913335

Senecal, L. (n.d.). *Data link layer attacks and their mitigation.* Department of Computer Science. Retrieved from https://www.cs.dartmouth.edu/~sergey/me/netreads/L2-security-Bootcamp.pdf

Szabó, T. (n.d.). *Network security problems on data link layer.* Retrieved from Hadmernok.hu: http://hadmernok.hu/2013_1_szabot_1.pdf

Vyncke, E., & Paggen, C. (n.d.). *Security in the data link layer of the OSI model on LANs wired Cisco.* Retrieved from https://shorturl.at/sQpVs

Yeung, K.-H. (2008). Tools for attacking data link layer. *International MultiConference of Engineers and Computer Scientists, II,* 1–7.