**COMP 3317 Computer Networks, Fall 2022**

**Instructor: Prof. Dr. Mehmet Ufuk Çağlayan**

**Term Report on**

**Address Resolution Protocol (ARP) and Secure Address Resolution Protocol (SARP)**

**Revision 1.0**

**20.11.2021**

**By: Erdoğan Eker**

**Student ID Number: 22240370156**

**E-mail: 19070001020@stu.yasar.edu.tr**

**Table of Contents**

[1. Introduction 3](#_Toc59625737)

[2. Address Resolution Protocol (ARP) 3](#_Toc59625738)

[2.1. Overview of ARP 3](#_Toc59625739)

[2.2. Architecture of ARP 3](#_Toc59625740)

[2.3. Limitations of ARP 3](#_Toc59625740)

[2.4. Defenes against ARP Spoofing 3](#_Toc59625740)

[2.5. Variations of ARP 3](#_Toc59625740)

[3. Secure Address Resolution Protocol (SARP) 3](#_Toc59625741)

[3.1. Overview of SARP 3](#_Toc59625742)

[3.2. Advantages of SARP 3](#_Toc59625743)

[3.3. Deployment of SARP 3](#_Toc59625743)

[3.4. Architecture of SARP 3](#_Toc59625743)

[4. Conclusions 3](#_Toc59625744)

[References 3](#_Toc59625745)

# 1. Introduction

The Address Resolution Protocol (ARP) is a fundamental networking protocol that is used to resolve network layer addresses (such as IPv4 addresses) to link layer addresses (such as MAC addresses) in a local area network (LAN). ARP is essential for communication between devices on a LAN and plays a crucial role in the operation of the Internet. However, the traditional ARP protocol is susceptible to spoofing attacks, in which an attacker can send fake ARP messages to the network in order to associate their own MAC address with the IP address of another device. This can allow the attacker to intercept and potentially modify the traffic intended for the victim device.

To address this security weakness, the Secure Address Resolution Protocol (SARP) was developed as a security extension to ARP. SARP uses public key cryptography to authenticate ARP messages and ensure that they are not tampered with or forged. It also includes mechanisms for detecting and mitigating ARP spoofing attacks. The goal of SARP is to enhance the security and integrity of the ARP protocol and protect against spoofing attacks in LAN environments.

In this term report, we will explore the basics of ARP and SARP, including their features and functionality. We will also discuss the advantages of using SARP over the traditional ARP protocol, the process of implementing SARP in a LAN, and real-world examples of SARP deployments. We will also compare SARP to other security measures that can be used to protect against spoofing attacks in LAN environments. Finally, we will consider the future potential and limitations of SARP as a solution to the security weaknesses of the traditional ARP protocol.

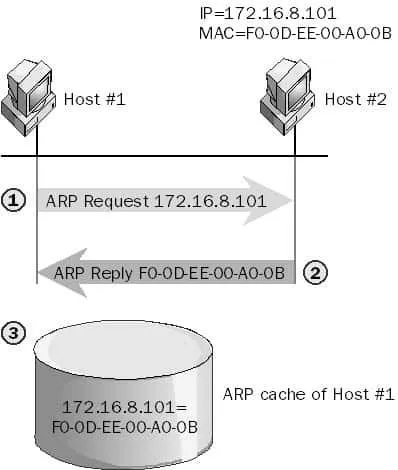
# 2. Address Resolution Protocol (ARP)

# 2.1. Overview of ARP

The Address Resolution Protocol (ARP) is a networking protocol that is used to resolve network layer addresses (such as IPv4 addresses) to link layer addresses (such as MAC addresses) in a local area network (LAN). ARP is essential for communication between devices on a LAN and plays a crucial role in the operation of the Internet.

When a device on a LAN wants to communicate with another device, it first needs to determine the MAC address of the destination device. It does this by sending an ARP request message to the LAN, which includes the IP address of the destination device. All devices on the LAN receive this message and check to see if they have the specified IP address. If a device has the specified IP address, it responds with an ARP reply message that includes its MAC address. The originating device then uses this MAC address to send the data to the destination device.

ARP is a simple and efficient protocol, but it has some limitations. One key weakness is that it is susceptible to spoofing attacks, in which an attacker can send fake ARP messages to the network in order to associate their own MAC address with the IP address of another device. This can allow the attacker to intercept and potentially modify the traffic intended for the victim device. To address this issue, the Secure Address Resolution Protocol (SARP) was developed as a security extension ARP.



# 2.2. Architecture of ARP

The Address Resolution Protocol (ARP) is a networking protocol that is used to map a network address, such as an Internet Protocol (IP) address, to a physical address, such as a media access control (MAC) address. It is used to enable data communication between devices on a local area network (LAN) that use different network layer protocols, such as IPv4 and IPv6.

The architecture of ARP consists of several components, including:

1. ARP request and reply messages: ARP messages are used to communicate between devices on the LAN to resolve an IP address to a MAC address. An ARP request message is sent by a device that is trying to resolve the MAC address of another device, while an ARP reply message is sent by the target device to provide its MAC address.
2. ARP cache: Each device on a LAN maintains an ARP cache, which is a table that stores the IP-to-MAC address mappings for recently resolved addresses. This allows devices to avoid sending unnecessary ARP request messages and improves the efficiency of address resolution.
3. ARP protocols: There are several different ARP protocols that are used for different purposes, such as the Reverse Address Resolution Protocol (RARP) and the Inverse Address Resolution Protocol (InARP). These protocols allow devices to resolve MAC addresses to IP addresses or resolve addresses for devices that are connected to different LAN segments.

Overall, the architecture of ARP is designed to enable efficient and reliable address resolution between devices on a LAN, allowing them to communicate with each other using different network layer protocols.

# 2.3. Limitations of ARP

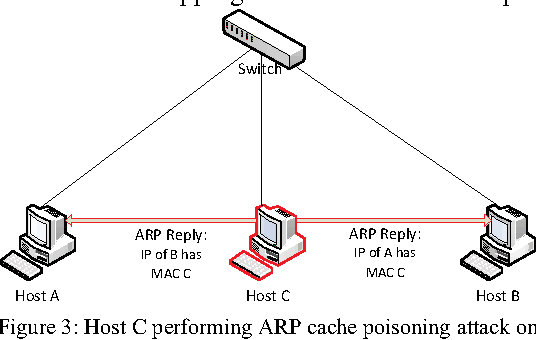
One of the main limitations of the traditional Address Resolution Protocol (ARP) is its vulnerability to spoofing attacks. In a spoofing attack, an attacker can send fake ARP messages to the network in order to associate their own MAC address with the IP address of another device. This can allow the attacker to intercept and potentially modify the traffic intended for the victim device.

ARP spoofing attacks are a common security threat in local area networks (LANs) and can have serious consequences, such as data theft, network disruption, and loss of confidentiality. For example, an attacker could use an ARP spoofing attack to intercept sensitive data transmitted over the network, or to redirect traffic to a malicious server.

ARP spoofing attacks can be difficult to detect, as they can involve the use of sophisticated techniques to manipulate the ARP cache on devices in the network. This can make it challenging for network administrators to identify and prevent such attacks. In addition, ARP spoofing attacks can be used to launch more advanced attacks, such as man-in-the-middle attacks or denial of service (DoS) attacks. For example, an attacker could use an ARP spoofing attack to intercept and modify traffic between two devices on the network, or to flood the network with fake ARP messages to disrupt communication.

Another limitation of ARP is that it relies on a centralized database of IP-to-MAC address mappings, known as the ARP cache. This database can become outdated or corrupted, which can cause communication problems on the network. For example, if a device on the network changes its IP address or MAC address, the ARP cache may not be updated to reflect this change. This can lead to communication issues between devices on the network, as they may not be able to resolve each other's addresses correctly.

Finally, the traditional ARP protocol does not provide any mechanism for verifying the authenticity of ARP messages, which makes it vulnerable to spoofing attacks. This is one of the main reasons why the Secure Address Resolution Protocol (SARP) was developed as a security extension to ARP. SARP uses public key cryptography to authenticate ARP messages and detect and mitigate spoofing attacks, which helps to improve the security and integrity of the network.

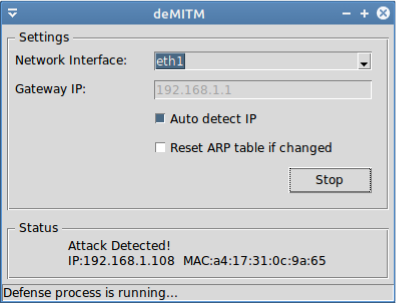


# 2.4. Defenses Against ARP Spoofing

One way to protect against man-in-the-middle attacks, including ARP spoofing, is to use prevention systems that aim to prevent the attack from occurring in the first place. These systems may include measures such as implementing strong authentication protocols, encrypting communication, and using firewalls to block unauthorized access. Additionally, implementing detection systems that trigger alarms or alerts when an attack is detected can help to quickly identify and mitigate potential threats. To achieve the best security, it is recommended to use both prevention and detection systems in a network.

1. Prevention System:
   1. Static ARP table: The static ARP table is a method for defending against man-in-the-middle attacks by preventing spoofed ARP replies from affecting the table on the victim's machine. While this solution is effective, it can be difficult to implement and maintain in large networks due to the overhead required for network administrators to deploy and update the tables on each device.
   2. ARP filtering: The second method for defending against ARP spoofing involves monitoring and logging each ARP packet and dropping any ARP reply packets that were not requested. This method is less effective than using static ARP tables, as an experienced attacker can wait for an ARP request from the victim's machine and then send a spoofed ARP reply packet. This is possible because ARP requests are broadcast packets, which can be read by the attacker.
   3. Authentication: Authentication can be used as a countermeasure against ARP spoofing attacks by isolating malicious users and preventing them from accessing the network. However, it is more effective in small, closed organizational environments where user selection can be based on authentication policies. In larger, more open and public environments, it may be more difficult to maintain a circle of authenticated users and exclude unwanted malicious users. Additionally, it may not be straightforward to add authentication at the data link layer, where ARP operates.
2. Detection Systems: Detection systems are intended to be installed on devices used by individuals to monitor the ARP table on that device and detect any changes in the gateway entry. If such a change is detected, the system alerts the user that their device is being targeted in an attack. In contrast to prevention systems, detection systems are designed to be easily installed and used by regular users without requiring specialized knowledge of systems or networks. These types of systems can be used in any type of network

GUI of defense tool



# 2.5. Variations of ARP

There are several variations of the Address Resolution Protocol (ARP) that have been developed to address different needs and scenarios. Some of the main variations of ARP include:

1. Reverse Address Resolution Protocol (RARP): RARP is a protocol that allows a device to request its own IP address from a server, given its MAC address. This can be useful in situations where a device does not have a statically assigned IP address and needs to request one from a server.
2. Inverse Address Resolution Protocol (InARP): InARP is a protocol that allows a device to resolve the MAC address of a device on a different LAN segment, given its IP address. This can be useful in scenarios where devices on different LAN segments need to communicate with each other.
3. Gratuitous ARP: Gratuitous ARP is a special type of ARP message that is used to update the ARP caches of other devices on the LAN. It is typically sent by a device when it changes its IP address or MAC address, or when it wants to verify the uniqueness of its IP address on the LAN.
4. Proxy ARP: Proxy ARP is a technique that allows a device to act as a proxy for another device on the LAN, allowing it to communicate with devices on other LAN segments. This can be useful in situations where a device does not have direct access to the LAN, but needs to communicate with devices on it.
5. Dynamic ARP Inspection (DAI): DAI is a security feature that is used to protect against ARP spoofing attacks, in which an attacker sends fake ARP messages to redirect traffic to their own device. DAI works by inspecting ARP messages on the LAN and verifying their authenticity before allowing them to update the ARP cache.

Overall, these variations of ARP provide additional functionality and security for addressing and communication on a LAN.

# 3. Secure Address Resolution Protocol (SARP)

# 3.1. Overview of SARP

The Secure Address Resolution Protocol (SARP) is a security extension to the Address Resolution Protocol (ARP), which is used to resolve network layer addresses (such as IPv4 addresses) to link layer addresses (such as MAC addresses) in a local area network (LAN). SARP was developed to address the security weaknesses of the traditional ARP protocol, which is susceptible to spoofing attacks in which an attacker can send fake ARP messages to the network in order to associate their own MAC address with the IP address of another device. This can allow the attacker to intercept and potentially modify the traffic intended for the victim device.

To enhance the security and integrity of the ARP protocol, SARP uses public key cryptography to authenticate ARP messages. This involves the use of digital certificates and public key infrastructure (PKI) to verify the authenticity of ARP messages and ensure that they are not tampered with or forged. SARP also includes mechanisms for detecting and mitigating ARP spoofing attacks, such as the use of digital signatures and encryption to protect against tampering and forgery.

SARP is designed to be fully compatible with the traditional ARP protocol, so it can be easily deployed in existing LAN environments. However, the use of digital certificates and PKI can introduce additional complexity and overhead to the deployment and management of SARP in a LAN. This may require the use of additional hardware and software, as well as the implementation of appropriate security policies and procedures.

Overall, the goal of SARP is to enhance the security and integrity of the ARP protocol and protect against spoofing attacks in LAN environments. By using public key cryptography and other security measures, SARP can help to ensure the authenticity and integrity of ARP messages and reduce the risk of spoofing attacks on the network.

# 3.2. Advantages of SARP

There are several key advantages to using the Secure Address Resolution Protocol (SARP) over the traditional Address Resolution Protocol (ARP):

1. Improved security: SARP uses public key cryptography to authenticate ARP messages and detect and mitigate spoofing attacks, which helps to improve the security and integrity of the network. This can reduce the risk of data theft, network disruption, and other security threats caused by spoofing attacks. For example, a hospital deploys SARP in its LAN to protect against spoofing attacks that could potentially compromise patient data.
2. Enhanced authentication: SARP includes additional security features, such as digital signing and encryption, to protect against tampering and forgery of ARP messages. This helps to ensure the authenticity and integrity of ARP messages and reduce the risk of spoofing attacks on the network. For example, a financial institution deploys SARP to protect against spoofing attacks that could potentially compromise sensitive financial transactions.
3. Compatibility with traditional ARP: SARP is designed to be fully compatible with the traditional ARP protocol, so it can be easily deployed in existing LAN environments. This means that SARP can be implemented without the need to modify or replace existing ARP-based systems. For example, a large enterprise deploys SARP in its LAN to enhance the security of its network without disrupting existing systems.
4. Reduced complexity: SARP includes mechanisms for detecting and mitigating spoofing attacks, which can help to reduce the complexity and overhead of managing ARP in a LAN environment. This can improve the efficiency and reliability of the network. For example, a small business deploys SARP to simplify the management of its LAN and reduce the risk of security breaches.
5. Improved traffic analysis: By using digital signatures and encryption to protect against tampering and forgery of ARP messages, SARP can help to improve the accuracy and reliability of traffic analysis tools. This can be useful for network administrators who need to monitor and troubleshoot the performance of the network. For example, a network administrator at a university uses traffic analysis tools to monitor the performance of the campus LAN and troubleshoot any issues that may arise. With SARP, the administrator can be confident that the traffic data being analyzed is accurate and has not been tampered with.
6. Enhanced privacy: The use of encryption and digital signing can help to protect the privacy of ARP messages and prevent unauthorized parties from accessing sensitive information transmitted over the network. For example, a government agency deploys SARP to protect the privacy of sensitive communications within its LAN.
7. Reduced maintenance: SARP includes mechanisms for detecting and mitigating spoofing attacks, which can help to reduce the maintenance and management overhead of ARP in a LAN environment. This can save time and resources for network administrators and improve the overall efficiency of the network. For example, a large corporation deploys SARP to streamline the management of its LAN and reduce the risk of security breaches.

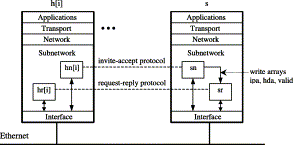
# 3.3. Deployment of SARP

The Secure Address Resolution Protocol (SARP) can be deployed in a local area network (LAN) in a number of ways. Some of the key considerations for deploying SARP include:

1. Compatibility with existing systems: SARP is designed to be fully compatible with the traditional Address Resolution Protocol (ARP), so it can be easily deployed in existing LAN environments. This means that SARP can be implemented without the need to modify or replace existing ARP-based systems.
2. Use of digital certificates and PKI: SARP uses public key cryptography to authenticate ARP messages and ensure their authenticity and integrity. This requires the use of digital certificates and public key infrastructure (PKI) to implement the security features of SARP. The deployment of SARP may therefore involve the use of additional hardware and software to support the use of digital certificates and PKI.
3. Security policies and procedures: The deployment of SARP may also require the implementation of appropriate security policies and procedures to ensure the security and integrity of the network. This may include measures such as access control, monitoring, and incident response.
4. Deployment planning: It is important to carefully plan the deployment of SARP to ensure that it is effective and efficient. This may involve testing SARP in a controlled environment before rolling it out to the entire LAN, as well as training network administrators and other personnel on the use and maintenance of SARP.
5. Testing and validation: Before deploying SARP in a production environment, it is important to test and validate the implementation to ensure that it is working as expected. This may involve testing SARP in a controlled environment with a small group of users or devices, and monitoring the performance and security of the network to identify any issues or problems.
6. Monitoring and maintenance: After deploying SARP, it is important to monitor the performance and security of the network on an ongoing basis. This may involve using monitoring tools and techniques to track the status and health of the network, as well as implementing incident response procedures to address any issues or problems that may arise.
7. Upgrades and updates: SARP may require periodic upgrades or updates to address security vulnerabilities or other issues. It is important to carefully plan and coordinate these upgrades or updates to ensure that they are smooth and do not disrupt the operation of the network.
8. Training and documentation: To ensure the effective deployment and use of SARP, it is important to provide training and documentation for network administrators and other personnel. This may include training on the use and maintenance of SARP, as well as documentation on the configuration and operation of SARP in the network.

# 3.4 Architecture of SARP

The Secure Address Resolution Protocol (SARP) is a protocol designed to provide secure address resolution in an Ethernet network. It is designed to protect against various types of attacks, such as message loss, message modification, and message replay, that may be launched by an adversary on the network. SARP consists of two protocols: the invite-accept protocol and the request-reply protocol. The invite-accept protocol allows computers on the Ethernet to communicate their IP addresses and hardware addresses to a secure server, while the request-reply protocol allows computers to resolve the IP addresses of other computers to their hardware addresses. To tolerate adversary actions, SARP uses mechanisms such as timeouts, shared secrets, and nonces. Timeouts allow a process to resend a message if it does not receive a reply within a certain time period. Shared secrets are used to compute an integrity check that is added to each message sent between the secure server and a computer on the Ethernet, allowing the receiver to detect any modifications made to the message by the adversary. Nonces are unique integers that are attached to a message and its reply, allowing the sender to detect any replay attacks. SARP also includes additional security features such as digital signing and encryption to protect against tampering and forgery of messages. Overall, SARP aims to provide a secure and reliable method for address resolution in Ethernet networks, protecting against various types of attacks that may be launched by an adversary.



# 4. Conclusions

The Address Resolution Protocol (ARP) is a widely used protocol for resolving network layer addresses (such as IPv4 addresses) to link layer addresses (such as MAC addresses) in a local area network (LAN). ARP plays a critical role in enabling devices on a LAN to communicate with each other by translating between the different types of addresses used at different layers of the networking stack.

However, the traditional ARP protocol is susceptible to spoofing attacks in which an attacker can send fake ARP messages to the network in order to associate their own MAC address with the IP address of another device. This can allow the attacker to intercept and potentially modify the traffic intended for the victim device, which can pose a serious security threat to the network.

To address the security weaknesses of ARP, the Secure Address Resolution Protocol (SARP) was developed as a security extension to ARP. SARP uses public key cryptography to authenticate ARP messages and detect and mitigate spoofing attacks, which helps to improve the security and integrity of the network. SARP also includes additional security features, such as digital signing and encryption, to protect against tampering and forgery of ARP messages.

SARP is designed to be fully compatible with the traditional ARP protocol, so it can be easily deployed in existing LAN environments. However, the use of digital certificates and public key infrastructure (PKI) can introduce additional complexity and overhead to the deployment and management of SARP in a LAN. This may require the use of additional hardware and software, as well as the implementation of appropriate security policies policies and procedures.

Overall, the Secure Address Resolution Protocol (SARP) offers a number of advantages over the traditional Address Resolution Protocol (ARP), including improved security, enhanced authentication, compatibility with traditional ARP, and reduced complexity. While the deployment of SARP may require additional resources and planning, the benefits of enhanced security and integrity can outweigh the costs for many organizations.

# References

1. Gouda, M. G., & Huang, C.-T. (2003). A secure address resolution protocol. *Computer Networks*, *41*(1), 57–71. https://doi.org/10.1016/s1389-1286(02)00326-2
2. Goralski, W. (2017). Address Resolution Protocol. The Illustrated Network, 175–195. <https://doi.org/10.1016/b978-0-12-811027-0.00006-0>
3. Al Sukkar, G., Saifan, R., Khwaldeh, S., Maqableh, M., & Jafar, I. (2016). Address resolution protocol (ARP): Spoofing attack and proposed defense. *Communications and Network*, *08*(03), 118–130. https://doi.org/10.4236/cn.2016.83012
4. Ataullah, M., & Chauhan, N. (2012). ES-ARP: An efficient and secure Address Resolution Protocol. 2012 IEEE Students’ *Conference on Electrical, Electronics and Computer Science*. <https://doi.org/10.1109/sceecs.2012.6184794> (only referance to figure 3)
5. Al Sukkar, G., Saifan, R., Khwaldeh, S., Maqableh, M., & Jafar, I. (2016). Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense. *Communications and Network*, 08(03), 118–130. https://doi.org/10.4236/cn.2016.83012