People's Democratic Republic of Algeria

Yahia Fares University of Médéa

# Study and Simulation of the Address Resolution Protocol (ARP)

---

Submitted as part of the module: **Computer Security**

**Submitted to:** Dr. Chergui Nadjah

**Prepared by:**

BENSALEM Loudjaine

MERABET Kawther

BSc in Computer Systems, Year 3

2024– 2025

## Abstract

This project presents a study and simulation of the Address Resolution Protocol (ARP), focusing on both Standard ARP and Proxy ARP. The objective is to demonstrate ARP's role in mapping IP addresses to MAC addresses and to evaluate its performance through simulated network scenarios.

**Keywords:** ARP, IP address, MAC address, network simulation

## Table des matières

## List of Figures

# 1. Introduction

Computer networks play an essential role in modern communication, enabling the fast and reliable exchange of information between devices.
In a computer network, each host (PC, router, printer, etc.) has two types of addresses:

- **IP address**: used for logical identification within the network.
- **MAC address**: used for physical identification at the hardware level.

When a host wants to send data to another, that data is encapsulated in an Ethernet frame as presented in Figure 1.1, which contains several fields, including the MAC address of the destination.
Thus, for the frame to be transmitted to the correct recipient, the sender must know its MAC address. This is where the ARP protocol is required.


**Figure 1.1** Ethernet frame

# 2. Overview of the ARP Protocol

## 2.1. Definition

The ARP (Address Resolution Protocol) is a communication protocol that allows finding the MAC address corresponding to an IP address within a local network.
It operates at Layer 2 (Data Link) of the OSI model and serves as a bridge between the network layer (IP) and the link layer (MAC).

## 2.2. Types of ARP Protocols

- **Standard ARP**:
  Used to resolve an IP address into a MAC address. It works in two steps:
  - **ARP Request**: A machine sends a broadcast request on the local network: "Who has IP address 192.168.1.1?"
  - **ARP Reply**: The concerned machine responds via unicast with its own MAC address.
- **Reverse ARP (RARP)**:
  Retrieves the IP address of a machine from its MAC address. Historically used for diskless machines.
- **Inverse ARP (InARP)**:
  Used in Frame Relay or ATM networks to obtain the IP address associated with a lower-layer identifier.
- **Proxy ARP**:
  Allows a router to respond to an ARP request on behalf of another host located on a different network.
- **Gratuitous ARP**:
  Allows a host to announce its own MAC address.

This project focuses on Standard ARP and Proxy ARP, which are the most commonly used in modern networks.

### 2.3. Role of the ARP Protocol

- **IP–MAC Association**
  Allows machines on a local network to associate an IP address with a MAC address.
- **Network Communication**
  Ethernet frames require the MAC address of the destination. ARP provides this information so communication can occur.
- **Traffic Optimization**
  ARP uses a cache (ARP table) to temporarily store IP–MAC mappings and avoid sending an ARP request for every communication.

### 2.4. ARP Table (or ARP Cache)

The ARP table is a local memory storing the known IP ↔ MAC mappings. It can contain:

- **Dynamic entries**:
  - Created automatically after an ARP request.
  - Expire after a certain time.
  - Update as needed.
  - Less secure, as they are vulnerable to attacks (e.g., ARP spoofing).
- **Static entries**:
  - Configured manually by the network administrator.
  - Permanent, unchanged without human intervention.
  - More secure.

## 3. Operational mechanisms of the ARP Protocol

### 3.1. Standard ARP

- **ARP Request**
  - Machine A wants to send data to Machine B but only knows its IP address.
  - It sends an ARP Request in broadcast: “Who has IP address 192.168.1.5?”
- **ARP Reply**
  - Machine B recognizes its IP and responds with a unicast ARP Reply containing its MAC address.
  - Machine A stores this information in its ARP table for future use.

### 3.2. Proxy ARP

Proxy ARP allows a router to respond to an ARP request on behalf of another host, enabling communication between different networks.

Example:

- PC1 wants to contact a host located on another subnet.
- It sends an ARP request on the local network.
- The router, connected to multiple subnets, intercepts this request.
- It checks its routing table. If the destination is reachable via one of its networks:
  - It responds with its own MAC address (of its interface on PC1’s local network).
  - It then forwards the packets to the destination network using its routing tables.
  - Otherwise, it sends the IP packets to the next router.

# 4. Simulation and Results

## 4.1. Simulation Setup

- **Tool:** Cisco Packet Tracer
- **Scenarios:**
  - Standard ARP
  - Proxy ARP
- **Modes tested:**
  - Real-Time Mode
  - Simulation Mode (with only ICMP and ARP filters enabled)
- **Topology:**
  - **Subnet 1:** 192.168.1.0/24 (PC0, PC1, Server0, PC2)
  - **Subnet 2:** 192.168.2.0/24 (PC3, PC4, PC5, PC6)
  - **Router0:**
    Fa0/0 → 192.168.1.5 (Subnet 1)
    Fa0/1 → 192.168.2.5 (Subnet 2)
  - **Configuration:** Devices were connected using Ethernet cables, and IP addressing was manually assigned.
    Figure 4.1 illustrates the topology.
- **Procedure:** Each scenario was executed twice: first with an empty ARP table, then with an updated ARP table (after the first ping).

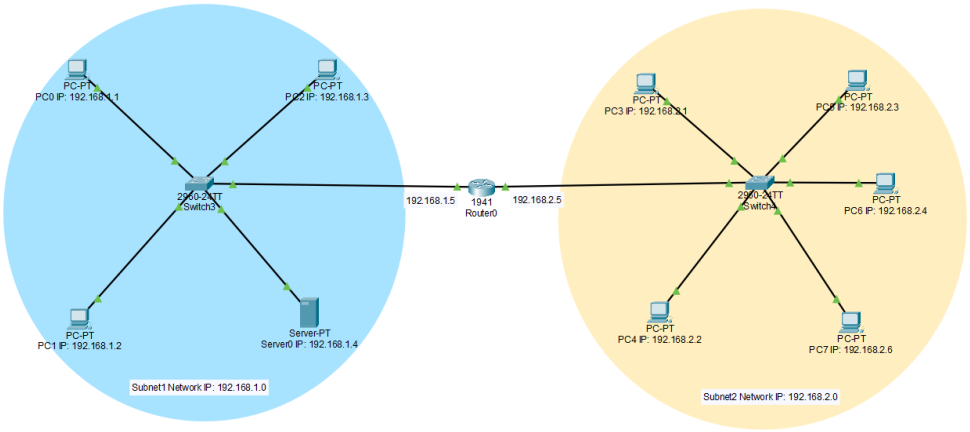


**Figure 4.1** Simulation topology

## 4.2. Standard ARP Simulation (sender: PC0, recipient: Server0)

**a. Real-Time Mode**

- **First test:**
  - PC0 and Server0 ARP tables: empty
  - Ping average response time: ~3 ms
- **Second test:**
  - PC0 ARP table: contains Server0 IP and MAC
  - Server0 ARP table: contains PC0 IP and MAC
  - ARP type: dynamic
  - Ping average response time: 0 ms

Figure 4.2 shows the results of both tests in real time.

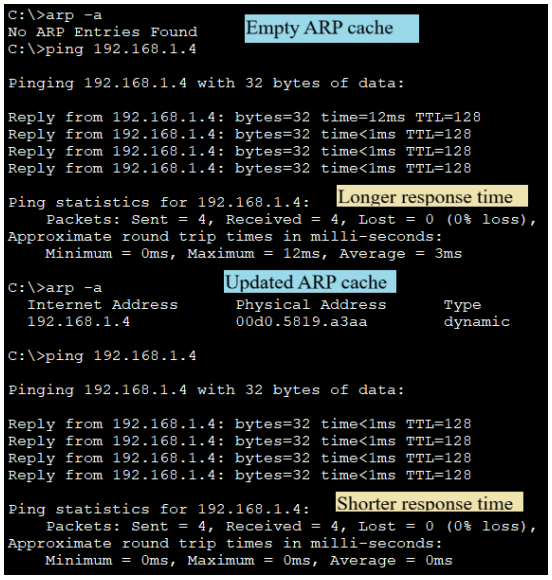


**Figure 4.2** Standard ARP Real-Time simulation results

**b. Simulation Mode**

- **First test:**
  - ARP request broadcast to all subnet devices via the switch (except the sender)
  - Only Server0 responded with an ARP reply (unicast)
  - Ping sent only to Server0; Server0 resent packets to PC0 (unicast)
- **Second test:**
  - No ARP request
  - PC0 sent ICMP packets directly to Server0; Server0 replied (unicast)

Figure 4.3 illustrates the ARP request in the first test.

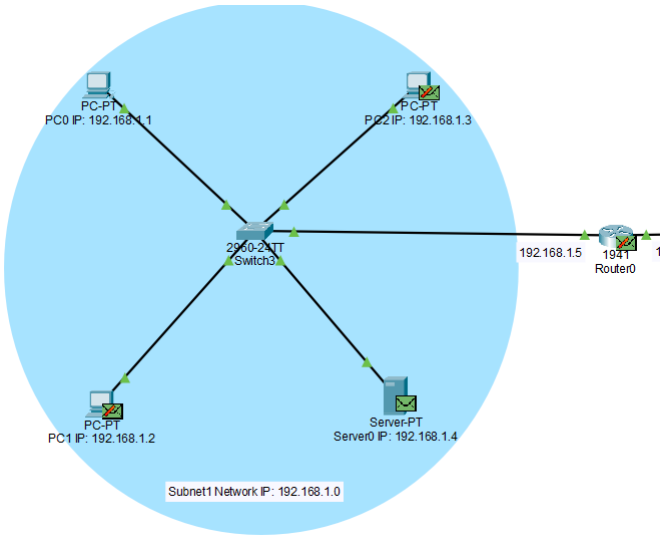


**Figure 4.3** ARP request in simulation mode

**4.3. Proxy ARP Simulation** (sender: PC0, recipient: PC3)

**a. Real-Time Mode**

- **First test:**
  - PC0 and PC3 ARP tables: empty
  - Router0 ARP table: contains Fa0/0 and Fa0/1 IP and MAC addresses

- Ping average response time: ~5 ms
- 1 packet lost

- **Second test:**
  - PC0 ARP table: contains Router0 Fa0/0 IP and MAC (Figure 4.4)
  - PC3 ARP table: contains Router0 Fa0/1 IP and MAC
  - Router0 ARP table: contains PC0, PC3, Fa0/0, and Fa0/1 IP and MAC addresses
  - ARP type: dynamic
  - Ping average response time: 0 ms
  - All packets successfully sent and received

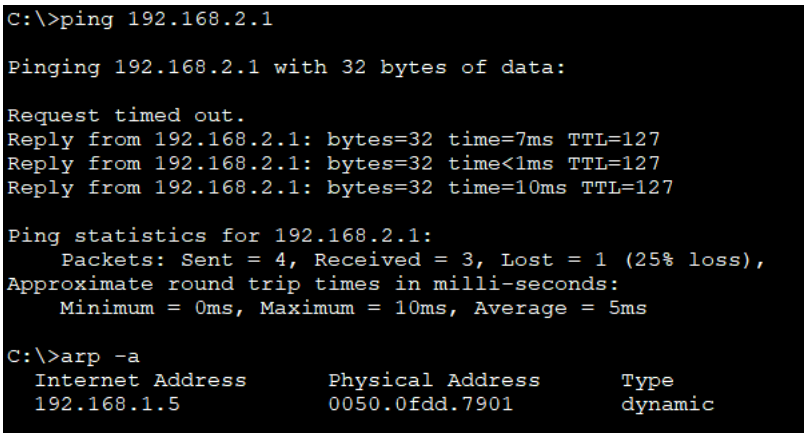


**Figure 4.4** ARP Proxy Real-Time simulation results

**b. Simulation Mode**

- **First test:**
  - PC0 sent a broadcast ARP request
  - Router0 responded
  - Router0 sent an ARP request in Subnet 2
  - PC3 responded
- **Second test:**
  - ICMP packets sent directly from PC0 to Router0, and from Router0 to PC3

### 4.4. Discussion

The simulations conducted for both Standard ARP and Proxy ARP highlight the essential role of the ARP protocol in network transmissions and explain the performance of the protocol in a network.

- **Standard ARP**

  • **Response time delay**: The first ping took more time because of ARP discovery; however, the second ping was faster because the ARP table contained the recipient's MAC address from the last ARP discovery.

  • **Dynamic update of ARP cache**: After each ARP process, the ARP table is updated dynamically without interruption.
- **ARP Proxy**

  • **Role of Router0**: Since ARP is a local protocol, a device cannot broadcast a request to a remote network. The router acted as a proxy because the destination (PC3) was on a different subnet.

  • **Loss of ICMP packet**: A packet was lost because the initial communication

involved a multi-step ARP discovery process.

• **Response time delay**: The initial ping had a longer delay than the standard ARP test because of the longer ARP discovery process.

The simulation results provide a clear explanation for why ARP is a critical and multi-step protocol.

## 5. Conclusion

The ARP protocol is essential for the proper functioning of local networks. It links IP addresses to MAC addresses, enabling data delivery at the Data Link layer.

However, due to its lack of security mechanisms, ARP is exposed to certain vulnerabilities:

- **Causes**:
  - No authentication: any machine can respond to an ARP request.
  - No encryption: ARP messages are sent in cleartext.
  - Automatic updating of the ARP table without verification.
  - Use of broadcast, making it visible to all machines on the network.
- **Example of attack**:
  - **ARP Spoofing:** An attacker sends fake ARP replies to redirect network traffic.
- **Solutions**:
  - Use static ARP entries for critical devices.
  - Deploy ARP traffic monitoring systems (such as IDS/IPS).
  - Use secure protocols (VPN, HTTPS, etc.) to encrypt data, even though ARP itself remains unsecured.