Name: Divij Shukla

Institute Name: Chandigarh University

Department: BE-CSE(H) – INFO. SECURITY

Domain: Cloud Infra. & Security

Submission Date: 15-06-25

Assignment Title 2: (ii) Prepare R&D Document on Basics of MAC Addressing and Functionality of ARP & RARP

#INTRODUCTION

In computer networking, efficient communication between devices requires accurate addressing mechanisms. MAC addressing, ARP, and RARP are foundational technologies in this space, enabling seamless data transmission at the data link and network layers of the OSI model.

#OBJECTIVE

- To understand the concept and structure of MAC addresses.
- To study how ARP helps in mapping IP addresses to MAC addresses.
- To analyze the functionality and relevance of RARP in network communication.
- To understand the evolution of these protocols and their modern alternatives.

#SCOPE

This document is focused on:

- Basic MAC addressing concepts used in Ethernet-based networks.
- Operational details of ARP and RARP.
- Real-world applications and limitations of these protocols.
- The relevance of these protocols in today's networking infrastructure.

#METHODOLOGY

The research is conducted through:

- Review of standard networking textbooks and RFC documentation.
- Analysis of protocol structures and communication flows.
- Comparison between legacy and current address resolution methods.
- Observation of ARP cache and RARP simulation through network tools.

#Theory and Conceptual Understanding

MAC Addressing

A MAC (Media Access Control) address is a unique 48-bit hardware identifier assigned to the NIC (Network Interface Card) by the manufacturer.

Format:

- 48-bit (6 bytes), usually displayed in hexadecimal.
- Example: 00:1A:2B:3C:4D:5E

Structure:

- First 3 bytes (24 bits): Organizationally Unique Identifier (OUI).
- Last 3 bytes (24 bits): Device-specific identifier.

Types:

- Unicast – for single devices.
- Multicast – for group communication.
- Broadcast – for all devices on the LAN (FF:FF:FF:FF:FF:FF).

Address Resolution Protocol (ARP)

ARP is a network layer protocol used to map a known IP address to its MAC address within a local network.

Working Steps:

1. Host checks its ARP cache for the MAC address.
2. If not found, it broadcasts an ARP Request.
3. The destination host responds with its MAC address.
4. The sender updates its ARP cache and sends data.

ARP Packet Fields:

Field	Description
Hardware Type	Type of network (Ethernet = 1)
Protocol Type	Protocol used (IPv4 = 0x0800)
Hardware Size	Length of MAC (6 bytes)
Protocol Size	Length of IP (4 bytes)
Opcode	Request (1) or Reply (2)
Sender MAC/IP	Sender information
Target MAC/IP	Receiver information

ARP Cache:

A temporary table storing recently resolved IP-to-MAC mappings.

Reverse Address Resolution Protocol (RARP)

RARP is used by a host to discover its IP address when only its MAC address is known, typically during the booting process of diskless machines.

Working Steps:

1. Device sends a RARP request with its MAC address.
2. RARP server replies with the corresponding IP address.
3. Device configures itself with the received IP.

Use Case:

- Used in legacy systems (diskless workstations).
- Mostly replaced by DHCP in modern networks.

#Analysis and Comparison

Feature	**ARP**	**RARP**
Direction	IP → MAC	MAC → IP
Broadcast Type	Broadcast request	Broadcast request
Reply Type	Unicast reply	Unicast reply
Usage	Communication on LAN	Booting diskless machines
Current Status	Actively used	Largely obsolete (replaced by DHCP)

#Applications

- **MAC Addressing**:

  Network interface identification, MAC filtering, network security.

- **ARP**:

  IP-MAC resolution, LAN communication, ARP spoofing detection.

- **RARP**:

  (Historical) assignment of IP addresses in early diskless networks.