Assignment- 2

Summer Internship Assignment: MAC Addressing and ARP/RARP Protocol Analysis

Submitted by: Sanchit Mathur
Department: Cloud infra & Security

Executive Summary

This document presents an overview of MAC (Media Access Control) addressing and the operational functionality of the ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) within enterprise network environments. The primary objective is to understand their roles in communication within local area networks (LANs), identify potential vulnerabilities, and propose mitigation strategies applicable to modern IT infrastructure.

Key outcomes include:

- Improved understanding of Layer 2 network communication
- Insights into IP-MAC resolution processes
- Identification of ARP-related security vulnerabilities
- Recommendations for network monitoring and security enhancement

---

Assignment Objectives

Research Goals

1. Understand the architecture and role of MAC addressing in Layer 2 communication.
2. Analyze the mechanics of ARP and RARP protocols.
3. Identify common vulnerabilities related to ARP and evaluate mitigation techniques.
4. Provide practical alignment of protocol knowledge with enterprise networking practices.

Deliverables

- Technical summary of MAC and ARP/RARP functions
- Security vulnerability analysis
- Troubleshooting methodologies
- Network hardening recommendations

MAC Addressing: Structure and Relevance

Definition

A MAC address is a 48-bit hardware identifier assigned to network interface controllers (NICs), used for local network communication at the data link layer (Layer 2 of the OSI model).

Format: 00:1A:2B:3C:4D:5E (hexadecimal)
Structure:

- **Organizational Unique Identifier (OUI):** First 3 bytes, identifies the manufacturer
- **Device Identifier:** Last 3 bytes, unique per device

Types of MAC Addresses

Type	Description
Unicast	Addressed to a single recipient device
Multicast	Sent to a defined group of devices
Broadcast	Sent to all devices in a LAN (FF:FF:FF:FF:FF:FF)

Enterprise Applications

- Network asset inventory and tracking
- MAC-based access control and segmentation
- Troubleshooting Layer 2 communication issues
- Monitoring unauthorized devices or spoofed addresses

ARP Protocol: Overview and Function

Purpose

ARP is responsible for resolving IP addresses to MAC addresses within a local subnet. It enables IP-based communication by allowing devices to determine the MAC address associated with a destination IP address.

ARP Workflow

1. Host checks local ARP cache.
2. If no match found, it broadcasts an ARP Request on the network.
3. The destination host responds with an ARP Reply containing its MAC address.

4. The originating host updates its ARP cache for future use.

Example Commands

```
arp -a            # View ARP table (Windows)
ip neighbor show  # View ARP table (Linux)
```

Advantages

- Enables IP-to-MAC resolution essential for LAN communication
- Reduces overhead through caching
- Facilitates seamless communication within subnets

RARP Protocol: Purpose and Current Use

Function

RARP allows devices, typically those without local storage (such as diskless workstations), to determine their IP address from a known MAC address during boot-up.

Relevance Today

RARP is largely obsolete in modern networks. It has been replaced by more advanced protocols like DHCP (Dynamic Host Configuration Protocol), BOOTP, and PXE.

Protocol	Function
RARP	Resolves MAC address to IP address
DHCP	Dynamically assigns IP addresses
BOOTP	Predecessor of DHCP for boot devices

Troubleshooting and Optimization Practices

Common Issues Related to ARP

- High broadcast traffic from frequent ARP requests (ARP storm)
- Invalid or stale cache entries
- ARP-related delays in communication

Troubleshooting Tools

```
# Windows
arp -d *          # Clear ARP table
```

```
# Linux
ip neighbor flush all  # Clear neighbor/ARP cache
```

Optimization Guidelines

- Configure static ARP entries for critical infrastructure (e.g., servers, routers)
- Adjust ARP timeout values based on network conditions
- Segment LANs using VLANs to reduce broadcast domains and ARP traffic

---

ARP Security Risks and Mitigation

ARP Spoofing

A type of attack in which a malicious device sends falsified ARP replies to associate its MAC address with the IP address of another legitimate host, often the default gateway. This allows interception or disruption of network traffic.

Risk Type	Impact
ARP Spoofing	Man-in-the-middle attack, data theft
ARP Cache Poisoning	Traffic redirection, service disruption

Recommended Countermeasures

Method	Benefit
Static ARP entries	Prevent unauthorized ARP resolution
Dynamic ARP Inspection (DAI)	Verifies ARP replies using DHCP snooping table
VLAN segmentation	Reduces scope of broadcast and attack radius
Port security (MAC binding)	Prevents unauthorized device connections

---

Performance Metrics

Metric	Recommended Threshold
Average ARP resolution time	< 2 milliseconds
ARP-related broadcast traffic	< 10% of total LAN traffic
Network uptime	≥ 99.8%

Metric	Recommended Threshold
Security incident frequency	Zero ARP spoofing incidents

Summary and Recommendations

Conclusion

Understanding MAC addressing and ARP/RARP protocol operations is essential for managing enterprise-level networks. While RARP is largely historical, ARP remains critical for intra-network communication and must be secured against spoofing attacks. Proper management of ARP and MAC data enhances operational performance and mitigates security risks.

Actionable Recommendations

1. Implement ARP monitoring tools for better visibility.
2. Configure static ARP entries for high-priority systems.
3. Apply VLANs to limit broadcast domains.
4. Enable Dynamic ARP Inspection where supported.
5. Train technical staff on ARP troubleshooting and detection techniques.

Appendix

A. Common ARP and MAC Commands

```
# Windows
arp -a          # View ARP table
arp -d *        # Clear all entries

# Linux
ip neighbor show
ip neighbor flush all

# Cisco IOS
show arp
clear arp
```

B. Example PowerShell Script for ARP Logging

```
$ARPTable = Get-NetNeighbor | Where-Object {$_.State -eq "Reachable"}
$ARPTable | Export-Csv -Path "C:\Logs\ARP_Log.csv"
```