R&D Document On Basics of MAC Addressing and Functionality of ARP & RARP

Prepared by: Debleena Maity

Domain: Cloud infra & Security

Intern, Celebal Technologies

Date: 08 June 2025

ABSTRACT

In modern networked systems, especially within cloud infrastructure, the need for fast, reliable, and secure device communication is important. A main element in this communication is the ability to identify devices accurately and resolve addresses across layers of the networking model. This is where MAC addressing, Address Resolution Protocol, and Reverse Address Resolution Protocol play very important roles in the smooth working of the underlying network fabric.

The MAC (Media Access Control) address uniquely determines each network interface within a local environment. Devices often communicate using IP addresses, requiring a protocol like ARP to solve the corresponding MAC address before data can be sent. In cloud environments, where dynamic and virtualized networking is common, ARP helps manage traffic and maintain 28performance.

RARP was developed to help devices identify their IP address when only the MAC address was known. Though RARP has been deprecated in approval of modern solutions like DHCP (Dynamic Host Configuration Protocol), understanding its concept is essential for grasping address resolution fundamentals. These mechanisms are also important from a security standpoint to defend against threats like ARP spoofing in cloud networks.

INTRODUCTION

In cloud infra and security, reliable communication between instances, containers, and physical servers is essential. This communication depends on correct addressing and address resolution. When a cloud instance sends data, it must identify the destination's hardware address, especially within the same physical network.

Two major concepts come into play here: MAC addressing, which provides device-level identity, and protocols like ARP and RARP, which bridge the gap between logical (IP) and physical (MAC) addressing. These are essential in managing internal routing, virtual networks (VPCs), and container communication in cloud systems.

Understanding how MAC addressing, ARP, and RARP work within local networks and how they apply to cloud environment is key to build secure, scalable infrastructure. These concepts not only support functionality but also help detect and prevent certain network-level attacks in cloud security.

MAC ADDRESSING

A MAC (Media Access Control) address is a unique hardware identifier assigned to every network interface controller (NIC), such as those found in physical devices like laptops, routers, and also in virtual devices like cloud-based VMs. It operates at the Data Link Layer of the OSI model and is essential for local network communication. A MAC address is typically represented as a 48-bit (6-byte) hexadecimal number, for example: 00:1A:2B:3C:4D:5E. The first 3 bytes of the address are assigned to the hardware manufacture while the remaining 3 bytes are uniquely assigned by the manufacturer.

MAC addresses are mostly permanent and hardcoded into the NIC, though they can sometimes be changed via software. They are locally significant, meaning they are primarily used within a Local Area Network (LAN) or a cloud subnet. Within these environments, MAC addresses play a crucial role in enabling devices to identify each other and ensure that frames are delivered to the correct recipient on the local network.

In cloud infrastructure, MAC addressing is vital for internal communication within Virtual Private Clouds. It ensures that virtual machines, containers, and other instances maintain unique network identities. Additionally, MAC addresses are used in overlay networks to maintain tenant isolation and to support dynamic routing between virtualized services.

FUNCTIONALITIES OF ADDRESS RESOLUTION PROTOCOL(ARP)

The Address Resolution Protocol (ARP) is a fundamental network protocol used to map an IP address (Layer 3) to its corresponding MAC address (Layer 2) within a local network. When a device wants to communicate with another device on the same network, it must first determine the MAC address of the destination using ARP. It does this by broadcasting an ARP request packet to all devices on the network, asking, “Who has this IP address?” The device with the matching IP address responds with its MAC address, which is then stored in the sender's ARP cache for future use.

In cloud infrastructure, ARP is critical in virtual networks such as Virtual Private Clouds (VPCs), where cloud VMs and containers need to resolve peer addresses before transmitting data. Though physical broadcasting is abstracted away in cloud environments, hypervisors and virtual switches handle ARP requests internally to maintain seamless communication between instances. Efficient ARP resolution contributes to low latency and high availability in software-defined networks (SDNs), which are the backbone of cloud platforms.

From a security perspective, ARP can be a point of vulnerability. Techniques such as ARP spoofing or poisoning are commonly used in man-in-the-middle (MITM) attacks to intercept or redirect traffic. This makes ARP monitoring and protection crucial in cloud security setups. Cloud providers implement controls like ARP inspection, isolation policies, and network ACLs to prevent malicious manipulation of ARP tables, ensuring secure communication between virtual machines in multi-tenant environments.

FUNCTIONALITIES OF REVERSE ADDRESS RESOLUTION PROTOCOL (RARP)

Reverse Address Resolution Protocol is a network protocol used to map a known MAC address to an IP address, generally performing the reverse function of ARP. It was designed for diskless devices or systems that knew their hardware address but needed to discover their IP address upon startup. When a device sends a RARP request, it asks a RARP server on the network that what will be IP address of given this MAC address. The server responds with the appropriate IP address,enathe device to join the network.

In the context of modern cloud infrastructure, RARP is largely considered obsolete and has been replaced by more flexible protocols like DHCP .Understanding RARP provides insight into the evolution of network bootstrapping mechanisms. For example, cloud instances that boot over the network may still rely on similar low-level address resolution processes, even if not using RARP directly.

From a security standpoint, RARP’s simplicity and lack of authentication made it vulnerable in open networks, which is one reason it was phased more secure provisioning systems. In the cloud, identity management, encryption, and trusted provisioning workflows have taken its place. Although not actively used today, RARP remains a foundational concept in understanding how network identity and addressing were originally managed in distributed systems and how these ideas have matured in secure cloud environments.

CONCLUSION

MAC addressing, ARP, and RARP form the foundational building blocks of local and cloud network communication. MAC addresses act as unique hardware-level identifiers that enable devices whether physical or virtual to be recognized within a local segment. ARP complements this by allowing devices to resolve IP addresses to MAC addresses dynamically, ensuring efficient data transmission. While RARP is now largely replaced by advanced protocols like DHCP, it served as an early solution to dynamic IP assignment challenges.

In cloud environments, these technologies take on new significance. Within Virtual Private Clouds , virtual machines, containers, and serverless components all depend on accurate MAC-level identification and address resolution to establish secure and consistent communication. Virtual switches, and SDN controllers emulate and manage ARP-like behavior behind the scenes, ensuring seamless network connectivity without user intervention. Although RARP is outdated, its principles continue to influence how cloud systems provision and allocate IP addresses at boot time.

From a security point of view, understanding these protocols is essential for mitigating network threats such as ARP spoofing or MAC flooding, which can compromise cloud workloads. Cloud professionals equipped with a strong grasp of MAC, ARP, and RARP can better architect secure and scalable infrastructures. Ultimately, mastering these Layer 2 and Layer 3 concepts ensures not only network efficiency but also resilience against evolving cyber threats in multi-tenant cloud environments.

REFERENCES

- https://www.geeksforgeeks.org/computer-networks/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/

- https://www.techtarget.com/searchnetworking/definition/Reverse-Address-Resolution-Protocol