LEKHRAJ JADON
2 WEEK Assignment

ARP, Reverse ARP (RARP), Inverse ARP (InARP), Proxy ARP, and Gratuitous ARP

Introduction

This document provides an in-depth exploration of the Address Resolution Protocol (ARP) family, which includes ARP, Reverse ARP (RARP),
Inverse ARP (InARP), Proxy ARP, and Gratuitous ARP. These protocols are essential for network communication, particularly in the mapping
of IP addresses to physical MAC addresses and vice versa.

1. Address Resolution Protocol (ARP)

ARP is a network layer protocol used to discover the physical address (MAC address) associated with a given IP address. This process is
crucial for the delivery of packets within a local network.

- Operation:
  1. The sender broadcasts an ARP request packet to all hosts in the network.
  2. The host with the matching IP address responds with an ARP reply, containing its MAC address.
  3. The sender updates its ARP cache and uses this information to send unicast messages to the destination.

- Example Scenario:
  When a computer wants to communicate with another computer in the same network, it first needs to know the MAC address of the destination
  computer. If it doesn't have this information, it sends an ARP request, and the destination computer responds with its MAC address.

2. Reverse Address Resolution Protocol (RARP)

RARP allows a machine to request its IP address from a gateway-server using its MAC address.

- Operation:
  1. A machine sends a RARP broadcast packet containing its MAC address.
  2. The RARP server on the network responds with the corresponding IP address.

- Usage:
  RARP was used primarily in diskless workstations to determine their IP address upon booting. However, RARP has largely been replaced by more advanced protocols like BOOTP and DHCP.

3. Inverse Address Resolution Protocol (InARP)

InARP performs the reverse of ARP, mapping a known MAC address to an IP address.

- Operation:
  1. InARP is used in Frame Relay and ATM networks to dynamically discover the IP address associated with a known DLCI (Data Link Connection Identifier) or MAC address.

- Usage:
  InARP is critical in environments where the IP address is not known but the MAC address or other layer 2 identifier is known.

4. Proxy ARP

Proxy ARP allows a router to respond to ARP requests on behalf of another machine.

- Operation:
  1. A device sends an ARP request for an IP address that belongs to a different subnet.
  2. The router (proxy ARP) responds with its own MAC address.

3. The sending device then sends packets to the router, which forwards them to the correct destination.

- Usage:
  Proxy ARP is used to enable communication between hosts in different subnets as if they were on the same subnet. This is useful in network
  segments connected by a router.

5. Gratuitous ARP

Gratuitous ARP is used to update other devices' ARP tables with the sender's IP and MAC address.

- Operation:
  1. A device sends an ARP request with its own IP address as the target.
  2. This updates the ARP tables of all receiving devices.

- Usage:
  Gratuitous ARP is used to detect IP conflicts and update ARP tables after changes in the network, such as IP address changes.

ARP Poisoning (ARP Spoofing)

ARP spoofing is a malicious attack where an attacker sends false ARP messages to associate their MAC address with the IP address of another
device, typically the gateway.

- Impact:
  1. The attacker intercepts, modifies, or stops traffic intended for the legitimate device.
  2. Can lead to Man-in-the-Middle (MITM) attacks, Denial of Service (DoS), and session hijacking.