1. **Objective**:

- ✓ Explore IP Addressing and Subnetting IPv4 & IPv6. Understand IP addressing and subnetting. Learn to create Subnets in natural masks, subnet mask, CIDR range, count usable and total hosts in an IP address range

- ✓ To understand the Basics of MAC Addressing Functionality of ARP & RARP.

2. Introduction

A network is a group of connected, communicating devices such as computers and printers. An internet is two or more networks that can communicate with each other. The most notable internet is called the "Internet" which is composed of hundreds of thousands of interconnected networks.
The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected to the Internet is called the Internet address or IP address. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet; an IP address is the address of the interface.
The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

3. MAC Address

MAC Addresses are unique 48-bit hardware numbers of a computer that are embedded into a network card during manufacturing.
To find MAC Address in windows: ipconfig /all
In macOS: TCP/IP Control Panel
The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done using either static or dynamic mapping.

Static Mapping: Static mapping means creating a table that associates a logical address with a physical Address

Dynamic Mapping: In dynamic mapping, each time a machine knows the logical address of another machine, it can use a protocol to find the physical address. Two protocols have been designed to perform dynamic mapping: Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).

Characteristic of MAC:

- MAC addresses are used in LAN (Local Area Network) environments
- MAC addresses are burned into the hardware of a network interface card (NIC) and cannot be changed
- The first 3 bytes of a MAC address represent the manufacturer ID
- MAC addresses are often used in conjunction with ARP

Types of MAC Address:

- **Unicast:**
  Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.

- **Multicast:**
  The multicast address allows the source to send a frame to a group of devices.

- **Broadcast:**
  Broadcast is also possible on the underlying layer (Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses.

4. ARP Protocol

It is responsible to find the hardware address of a host from a known IP address.
ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer.

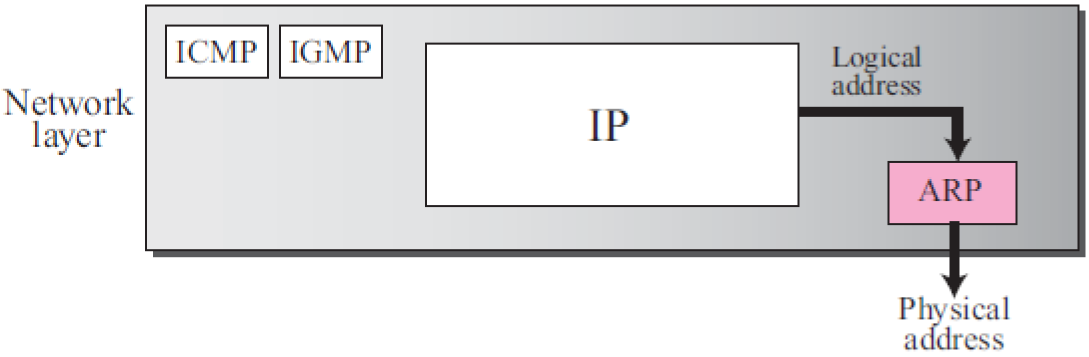
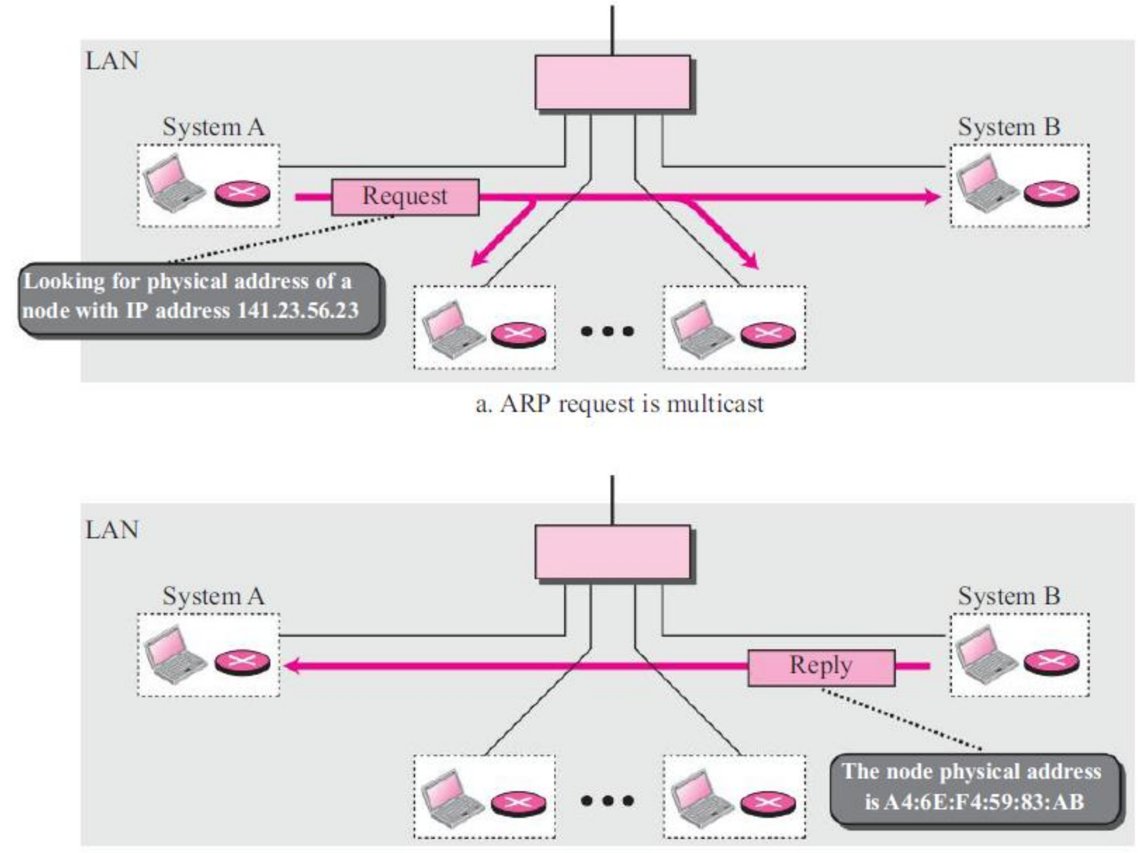


Figure 8.2 *ARP operation*


LAN
System A
System B
Request
Looking for physical address of a node with IP address 141.23.56.23
LAN
System A
System B
Reply
The node physical address is A4:6E:F4:59:83:AB

a. ARP request is multicast

b. ARP reply is unicast

Important Terms Associated with ARP

- Reverse ARP
- Proxy ARP
- Gratuitous ARP

Reverse ARP

Reverse Address Resolution Protocol is a protocol that is used in local area networks (LAN) by client machines for requesting IP Address (IPv4) from Router's ARP Table.

Proxy ARP

Proxy Address Resolution Protocol work to enable devices that are separated into network segments connected through the router in the same IP to resolve IP Address to MAC Address.
In case, when the sender receives the MAC Address of the Proxy Router, it is going to send the datagram to Proxy Router, which will be sent to the destination device.

Gratuitous ARP

A gratuitous ARP is an ARP packet sent by a device announcing its own IP address to the network. This type of ARP is typically used when a device wants to update its IP address or inform other devices about a change in its network configuration.

An ARP request is broadcast; an ARP reply is unicast.

The following are four different cases in which the services of ARP can be used:
1) The sender is a host and wants to send a packet to another host on the same network.
2) The sender is a host and wants to send a packet to another host on another network.
3) The sender is a router that has received a datagram destined for a host on another network.
4) The sender is a router that has received a datagram destined for a host in the same network.

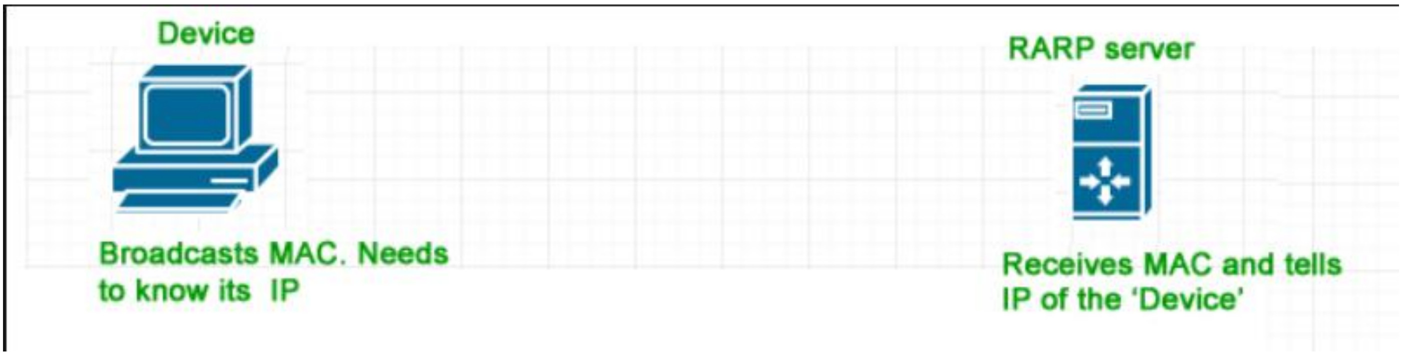
Importance of ARP:

1) Efficient Communication
2) Improved network performance
3) Enhanced security
4) Flexibility in network configuration
5) Simplified troubleshooting

5. RARP Protocol

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table.

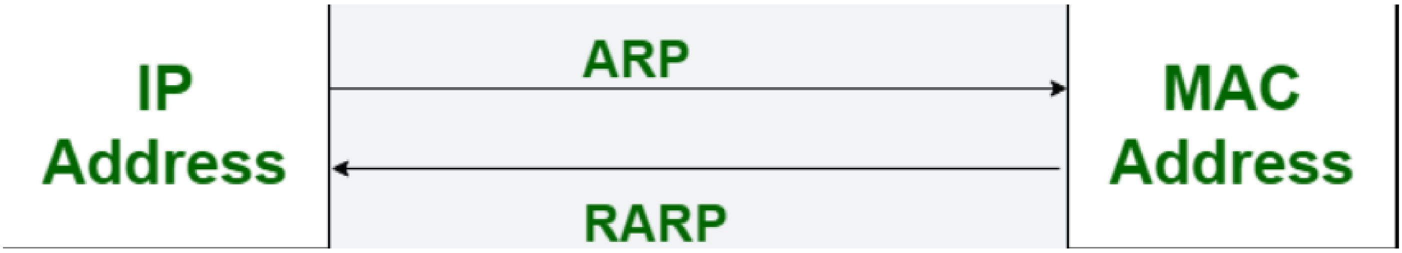
When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So, the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

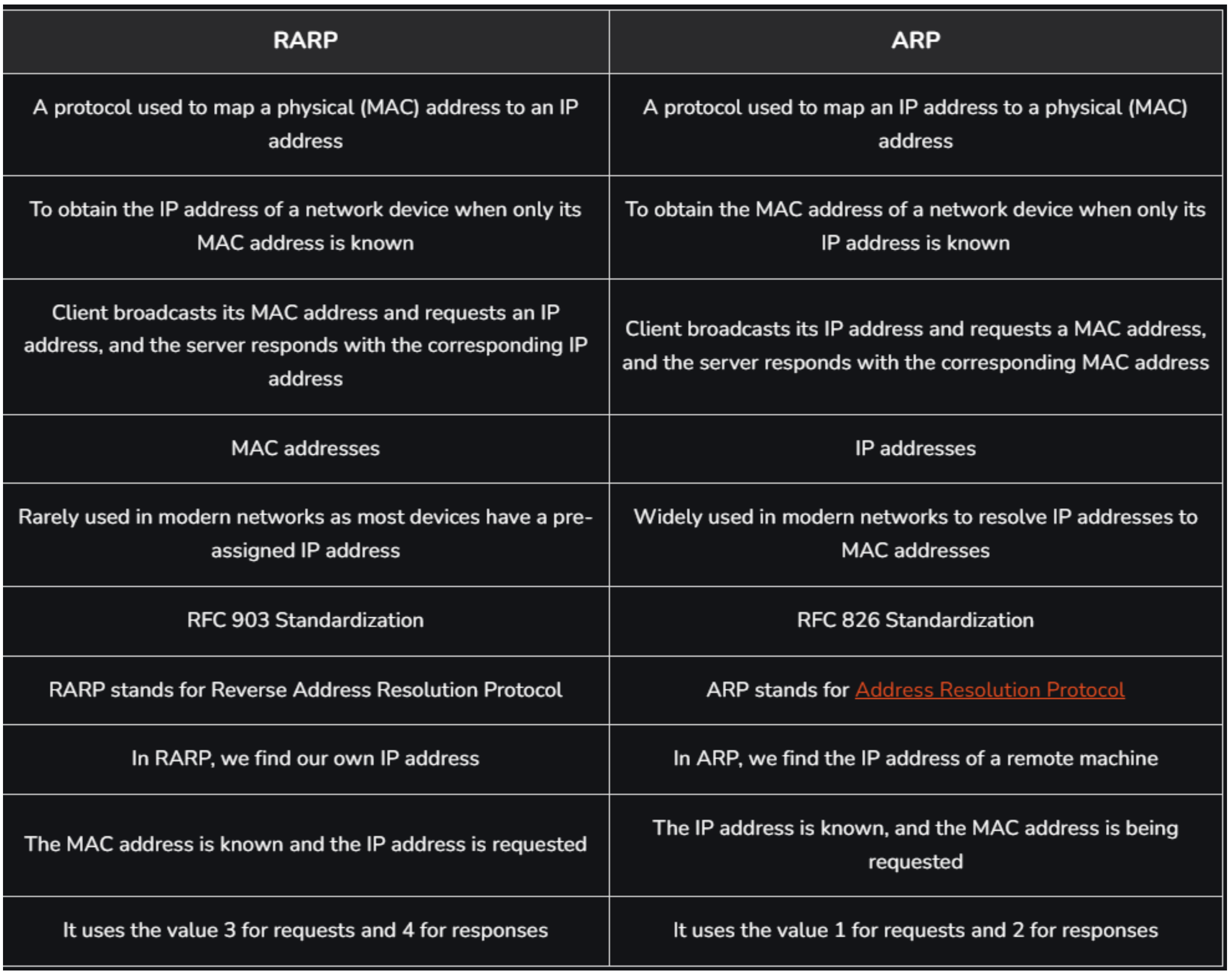

Device
Broadcasts MAC. Needs to know its IP
RARP server
Receives MAC and tells IP of the 'Device'

Working

1. A client machine that needs an IP address sends a broadcast message, known as a RARP request, to the network.
2. The gateway router contains an ARP table that maps the MAC addresses to their corresponding IP addresses.
3. When a RARP request is received, the RARP server (which can be a regular computer in the network) checks its ARP table.
4. Upon receiving the IP address, the client machine configures itself with the new IP address.

6. Difference Between ARP and RARP





RARP	ARP
A protocol used to map a physical (MAC) address to an IP address	A protocol used to map an IP address to a physical (MAC) address
To obtain the IP address of a network device when only its MAC address is known	To obtain the MAC address of a network device when only its IP address is known
Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address	Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address
MAC addresses	IP addresses
Rarely used in modern networks as most devices have a pre-assigned IP address	Widely used in modern networks to resolve IP addresses to MAC addresses
RFC 903 Standardization	RFC 826 Standardization
RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

7. Conclusion

ARP and RARP provide similar purposes in terms of address resolution, ARP is far more common and important in modern networking. ARP translates IP addresses to MAC addresses, facilitating local network communications. On the other hand, RARP, although historically important, has largely been replaced by more advanced protocols like IP address assignment.

MAC addressing, along with ARP and RARP, ensures that devices can find each other on local networks—bridging the gap between logical (IP) and physical (MAC) addressing.

8. References

- **https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/**
- **https://www.geeksforgeeks.org/mac-address-in-computer-network/**
- **https://www.geeksforgeeks.org/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/**
- **https://www.geeksforgeeks.org/difference-between-arp-and-rarp/**
- **TCP/IP Protocol Suite by Behrouz A. Forouzan**