What is RARP ?

Last Updated : 02 Apr, 2023

Introduction :

The Reverse Address Resolution Protocol (RARP) is a networking protocol that is used to map a physical (MAC) address to an Internet Protocol (IP) address. It is the reverse of the more commonly used Address Resolution Protocol (ARP), which maps an IP address to a MAC address.

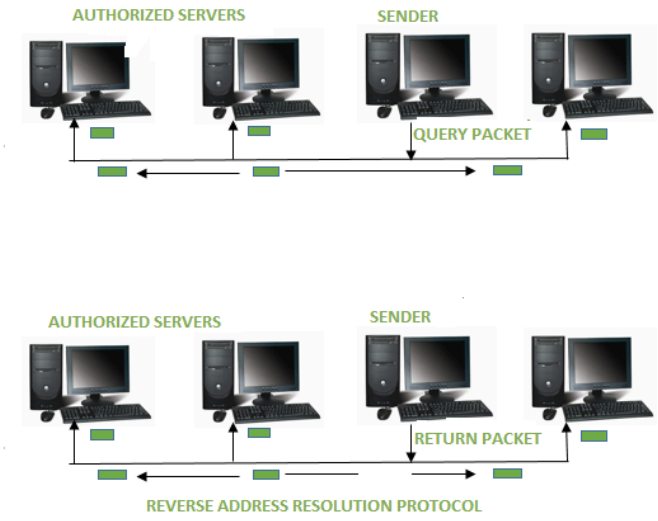
RARP was developed in the early days of computer networking as a way to provide IP addresses to diskless workstations or other devices that could not store their own IP addresses. With RARP, the device would broadcast its MAC address and request an IP address, and a RARP server on the network would respond with the corresponding IP address.

While RARP was widely used in the past, it has largely been replaced by newer protocols such as DHCP (Dynamic Host Configuration Protocol), which provides more flexibility and functionality in assigning IP addresses dynamically. However, RARP is still used in some specialized applications, such as booting embedded systems and configuring network devices with pre-assigned IP addresses.

RARP is specified in RFC 903 and operates at the data link layer of the OSI model. It has largely been superseded by ARP and DHCP in modern networks, but it played an important role in the development of computer networking protocols and continues to be used in certain contexts.

RARP is abbreviation of Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

This protocol is used to communicate data between two points in a server. The client doesn't necessarily need prior knowledge the server identities capable of serving its request. Media Access Control (MAC) addresses requires individual configuration on the servers done by an administrator. RARP limits to the serving of IP addresses only.
When a replacement machine is set up, the machine may or might not have an attached disk that may permanently store the IP Address so the RARP client program requests IP Address from the RARP server on the router. The RARP server will return the IP address to the machine under the belief that an entry has been setup within the router table.



History of RARP :

RARP was proposed in 1984 by the university Network group. This protocol provided the IP Address to the workstation. These diskless workstations were also the platform for the primary workstations from Sun Microsystems.

Working of RARP :

The RARP is on the Network Access Layer and is employed to send data between two points in a very network.

Each network participant has two unique addresses:- IP address (a logical address) and MAC address (the physical address).

The IP address gets assigned by software and after that the MAC address is constructed into the hardware.

The RARP server that responds to RARP requests, can even be any normal computer within the network. However, it must hold the data of all the MAC addresses with their assigned IP addresses. If a RARP request is received by the network, only these RARP servers can reply to it. The info packet needs to be sent on very cheap layers of the network. This implies that the packet is transferred to all the participants at the identical time.

The client broadcasts a RARP request with an Ethernet broadcast address and with its own physical address. The server responds by informing the client its IP address.

How is RARP different from ARP ?

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

RARP	ARP
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

Uses of RARP :

RARP is used to convert the Ethernet address to an IP address. It is available for the LAN technologies like FDDI, token ring LANs, etc.

Disadvantages of RARP :

The Reverse Address Resolution Protocol had few disadvantages which eventually led to its replacement by BOOTP and DHCP. Some of the disadvantages are listed below:

- The RARP server must be located within the same physical network.
- The computer sends the RARP request on very cheap layer of the network. Thus, it's unattainable for a router to forward the packet because the computer sends the RARP request on very cheap layer of the network.
- The RARP cannot handle the subnetting process because no subnet masks are sent. If the network is split into multiple subnets, a RARP server must be available with each of them.
- It isn't possible to configure the PC in a very modern network.
- It doesn't fully utilize the potential of a network like Ethernet.

RARP has now become an obsolete protocol since it operates at low level. Due to this, it requires direct address to the network which makes it difficult

to build a server.

Issues in RARP :

The Reverse Address Resolution Protocol (RARP) has several issues that limit its usefulness in modern networks:

1. Limited scalability: RARP does not scale well in large networks as it relies on broadcasting to communicate with clients. This can result in network congestion and performance issues, especially in networks with a high number of clients.
2. Security concerns: RARP does not provide any security mechanisms, such as authentication or encryption, which makes it vulnerable to attacks such as spoofing and denial of service.
3. Lack of flexibility: RARP provides only basic functionality and cannot be used to provide advanced network services such as assigning DNS server information or network gateway addresses.
4. Limited support: RARP is not supported by many modern operating systems and network devices, which makes it difficult to implement and maintain in modern networks.
5. Compatibility issues: RARP may not be compatible with newer networking protocols, such as IPv6, which can limit its usefulness in networks that require advanced features and functionality.