**JSS MAHAVIDYAPEETHA**

**JSS SCIENCE AND TECHNOLOGY UNIVERSITY**

**SRI JAYACHAMARAJENDRA COLLEGE OF ENGINEERING**

JSS Technical Institutions Campus, Mysuru – 570 006

****

**ARP AND RARP PROTOCOLS**

**20IS530**

**Bachelor of Engineering in**

**INFORMATION SCIENCE AND ENGG**

**Submitted to**

**SINDHU A S**

**Assistant professor**

**Department of Information Science**

*by,*

**ANAND K S 01JST20IS007**

**P RAJAT BHANDARY 01JST20IS031**

**PRABHAT KUMAR MISHRA 01JST20IS033**

**RAMESH B S 01JST20IS058**

## 

**Contents**

[**Introduction 3**](#_Toc125472172)

[**What Does ARP Do and How Does It Work? 3**](#_Toc125472173)

[**What is address resolution protocol's relationship with DHCP and DNS? How do they differ? 4**](#_Toc125472174)

**Types of ARP…………………………………………………………………………...5**

[**What is ARP in Networking Useful For? 5**](#_Toc125472175)

[**What Is ARP Spoofing/ARP Poisoning Attack? 6**](#_Toc125472176)

[**Man-in-the-Middle (MTM) Attacks 6**](#_Toc125472177)

[**Denial-of-Service Attacks 6**](#_Toc125472178)

[**Session Hijacking 7**](#_Toc125472179)

[**What is RARP Protocol? 7**](#_Toc125472181)

[**Steps to Achieve the IP Address from RARP Server: 8**](#_Toc125472183)

**Program for Address Resolution Protocol (ARP) using TCP ………………………..9**

**Program for Reverse Address Resolution Protocol (RARP) using UDP ………….11**

**Simulation of ARP/RARP Protocol using Cisco Packet Tracer……………………..14**

**Conclusion….…………………………………………………………………………...19**

## 

## **INTRODUCTION**

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.

There is a networking model known as the Open Systems Interconnection (OSI) model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system. This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.

The MAC address is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place. The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.

## **What Does ARP Do and How Does It Work?**

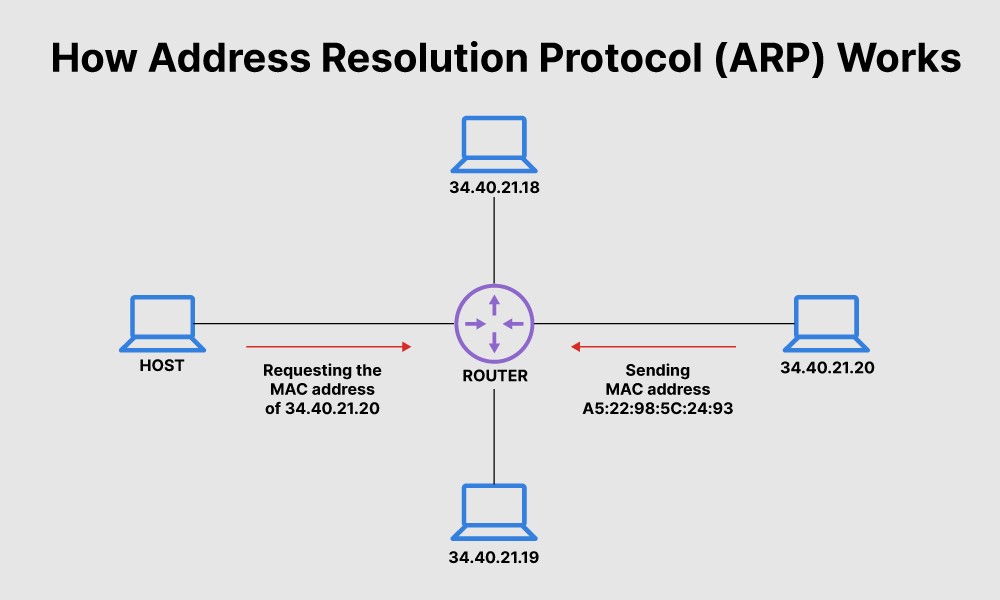
When a new computer joins a local area network (LAN), it will receive a unique IP address to use for identification and communication.

Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static [ARP table](https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/473534/arp-table) containing IP addresses and MAC addresses.

ARP caches are kept on all operating systems in an IPv4 [Ethernet network](https://www.fortinet.com/resources/cyberglossary/what-is-ethernet-switching). Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.

An ARP cache size is limited by design, and addresses tend to stay in the cache for only a few minutes. It is purged regularly to free up space. This design is also intended for privacy and security to prevent IP addresses from being stolen or spoofed by cyberattackers. While MAC addresses are fixed, IP addresses are constantly updated.

In the purging process, unutilized addresses are deleted; so is any data related to unsuccessful attempts to communicate with computers not connected to the network or that are not even powered on.



## **What is address resolution protocol's relationship with DHCP and DNS? How do they differ?**

ARP is the process of connecting a dynamic IP address to a physical machine's MAC address. As such, it is important to have a look at a few technologies related to IP.

As mentioned previously, IP addresses, by design, are changed constantly for the simple reason that doing so gives users security and privacy. However changes on IP addresses should not be completely random. There should be rules that allocate an IP address from a defined range of numbers available in a specific network. This helps prevent issues, such as two computers receiving the same IP address. The rules are known as DHCP or Dynamic Host Configuration Protocol.

IP addresses as identities for computers are important because they are needed to perform an internet search. When users search for a domain name or Uniform Resource Locator (URL), they use an alphabetical name. Computers, on the other hand, use the numerical IP address to associate the domain name with a server. To connect the two, a Domain Name System (DNS) server is used to translate an IP address from a confusing string of numbers into a more readable, easily understandable domain name, and vice versa.

**Types of ARP**

1. **Proxy ARP**

Proxy ARP is a technique by which a proxy device on a given network answers the ARP request for an IP address that is not on that network. The proxy is aware of the location of the traffic’s destination and offers its own MAC address as the destination.

1. **Gratuitous ARP**

Gratuitous ARP is almost like an administrative procedure, carried out as a way for a host on a network to simply announce or update its IP-to-MAC address. Gratuitous ARP is not prompted by an ARP request to translate an IP address to a MAC address.

1. **Reverse ARP (RARP)**

Host machines that do not know their own IP address can use the Reverse Address Resolution Protocol (RARP) for discovery.

1. **Inverse ARP(IARP)**

Whereas ARP uses an IP address to find a MAC address, IARP uses a MAC address to find an IP address.

## 

## **What is ARP in Networking Useful For?**

ARP is necessary because the software address (IP address) of the host or computer connected to the network needs to be translated to a hardware address (MAC address). Without ARP, a host would not be able to figure out the hardware address of another host. The LAN keeps a table or directory that maps IP addresses to MAC addresses of the different devices, including both endpoints and routers on that network.

This table or directory is not maintained by users or even by IT administrators. Instead, the ARP protocol creates entries on the fly. If a user's device does not know the hardware address of the destination host, the device will send a message to every host on the network asking for this address. When the proper destination host learns of the request, it will reply back with its hardware address, which will then be stored in the ARP directory or table.

If ARP is not supported, manual entries can be made to this directory.

## **What Is ARP Spoofing/ARP Poisoning Attack?**

ARP spoofing is also known as ARP poison routing or ARP cache poisoning. This is a type of malicious attack in which a cyber criminal sends fake ARP messages to a target LAN with the intention of linking their MAC address with the IP address of a legitimate device or server within the network. The link allows for data from the victim's computer to be sent to the attacker's computer instead of the original destination.

ARP spoofing attacks can prove dangerous, as sensitive information can be passed between computers without the victims' knowledge. ARP spoofing also enables other forms of cyberattacks, including the following:

### **Man-in-the-Middle (MTM) Attacks**

A man-in-the-middle (MITM) attack is a type of eavesdropping in which the cyberattacker intercepts, relays, and alters messages between two parties—who have no idea that a third party is involved—to steal information. The attacker may try to control and manipulate the messages of one of the parties, or of both, to obtain sensitive information. Because these types of attacks use sophisticated software to mimic the style and tone of conversations—including those that are text- and voice-based—a MITM attack is difficult to intercept and thwart.

A MITM attack occurs when malware is distributed and takes control of a victim's web browser. The browser itself is not important to the attacker, but the data that the victim shares very much is because it can include usernames, passwords, account numbers, and other sensitive information shared in chats and online discussions.

Once they have control, the attacker creates a proxy between the victim and a legitimate site, usually with a fake lookalike site, to intercept any data between the victim and the legitimate site. Attackers do this with online banking and e-commerce sites to capture personal information and financial data.

### **Denial-of-Service Attacks**

A denial-of-service (DoS) attack is one in which a cyberattacker attempts to overwhelm systems, servers, and networks with traffic to prevent users from accessing them. A larger-scale DoS attack is known as a distributed denial-of-service (DDoS) attack, where a much larger number of sources are used to flood a system with traffic.

These types of attacks exploit known vulnerabilities in network protocols. When a large number of packets are transmitted to a vulnerable network, the service can easily become overwhelmed and then unavailable.

### **Session Hijacking**

Session hijacking occurs when a cyberattacker steals a user's session ID, takes over that user's web session, and masquerades as that user. With the session ID in their possession, the attacker can perform any task or activity that the user is authorized to do on that network.

Authentication occurs when a user tries to gain access to a system or sign in to a restricted website or web service. The session ID is stored in a cookie in the browser, and an attacker engaged in session hijacking will intercept the authentication process and intrude in real time.

**How Fortinet Can Help**

The Fortinet network access control (NAC) solution provides enhanced visibility across all devices in a network to keep up with the ever-evolving threat landscape. NAC is part of the zero-trust network access model for security, in which trust is not a given for users, applications, or devices, whether connected to the network or not, but has to be established. Each device in a network maintains a copy of the ARP cache, and the cache is cleaned every few minutes. As such, all devices connected to that network must be kept secure so that important data, including IP addresses, are not compromised. To further protect your network devices and servers, Fortinet Ethernet LAN switches safeguard an organization's infrastructure and even include a selector tool to identify the best switch to meet network requirements.

## **What is RARP Protocol?**

## RARP is an abbreviation for Reverse Address Resolution Protocol. RARP is a TCP/IP protocol that is responsible for the translation of Physical Address (e.g. – Ethernet address) to be translated into an IP address.

Hosts like diskless workstations only have their hardware interface addresses or MAC address, but not their IP addresses. They must discover their IP addresses from an external source, usually via RARP protocol. RARP is defined in RFC 903.

RARP protocol is described in Internet Engineering Task Force (IETF) publication RFC 903 It has been considered obsolete with inventing to new methodologies like the Bootstrap Protocol (BOOTP) and theDHCP.

Both the new methods support a much greater feature set than RARP protocol**.**

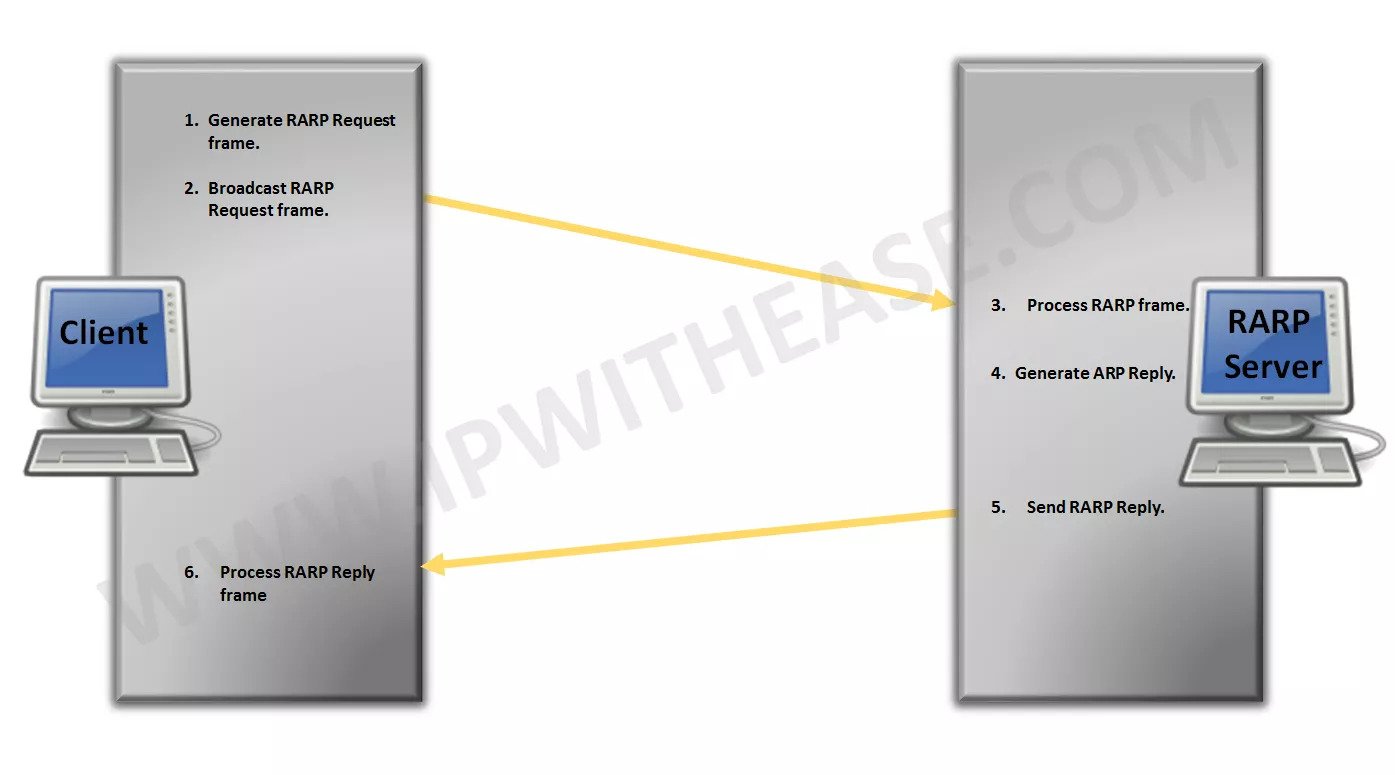
RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses.

Media Access Control (MAC) addresses need to be individually configured on the servers by an administrator.

RARP is limited to serving only IP addresses.

## **Steps to Achieve the IP Address from RARP Server:**

Below is the step by step procedure how **RARP** is responsible for the transaction of achieving the **IP address** from RARP server –



* **Source Device “Generates RARP Request Message”** – The source device generates a RARP Request message. The Source puts its own data link-layer address as both the Sender Hardware Address and also the Target Hardware Address. It leaves both the Sender Protocol Address and the Target Protocol Address blank.
* **Source Device “Broadcasts RARP Request Message”** – The source broadcasts the ARP Request message on the local network.
* **Local Devices “Process RARP Request Message**” – The message is received by each device on the local network and processed. Devices that are not configured to act as RARP servers ignore the message.
* **RARP Server Generates RARP Reply Message**: Any device on the network that is a RARP server responds to the broadcast from the source device. It generates a RARP Reply and sets the Sender Hardware Address and Sender Protocol Address to its own hardware and IP address of course. It then sets the Target Hardware Address to the hardware address of the original source device. It looks up in a table the hardware address of the source, determines that device’s IP address assignment, and puts it into the Target Protocol Address field.
* **RARP Server Sends RARP Reply Message**: The RARP server sends the RARP Reply message unicast to the device looking to be configured.
* **Source Device Processes RARP Reply Message**: The source device processes the reply from the RARP server. It then configures itself using the IP address in the Target Protocol Address supplied by the RARP server.

**Program for Address Resolution Protocol (ARP) using TCP**

**Client**

**1.** Start the program

**2.** Using socket connection is established between client and server.

**3.** Get the IP address to be converted into MAC address.

**4.** Send this address to the server.

**5.** Server returns the MAC address to the client.

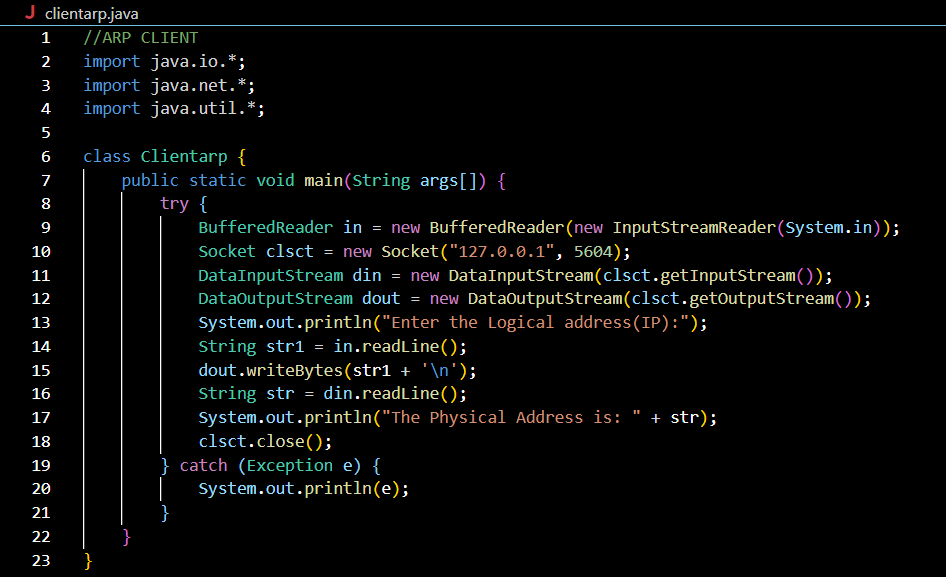
**Server**

1. Start the program

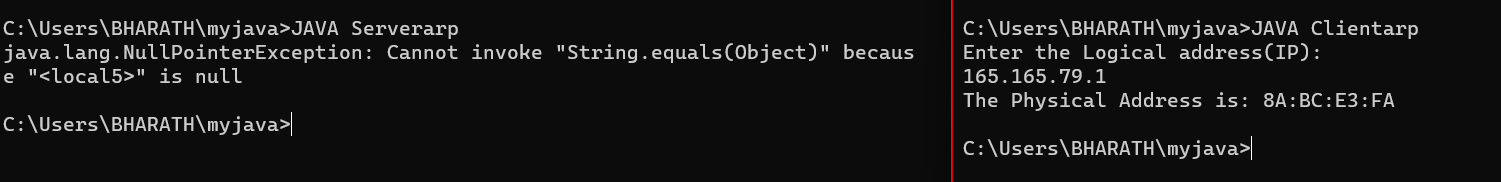
2. Accept the socket which is created by the client.

3. Server maintains the table in which IP and corresponding MAC addresses are stored. 4. Read the IP address which is sent by the client.

5. Map the IP address with its MAC address and return the MAC address to the client.

****

**Output:**



**Program for Reverse Address Resolution Protocol (RARP) using UDP**

**Client**

1.Start the program

2. using datagram sockets UDP function is established.

2.Get the MAC address to be converted into an IP address.

3.Send this MAC address to the server.

4.Server returns the IP address to the client.

**Server**

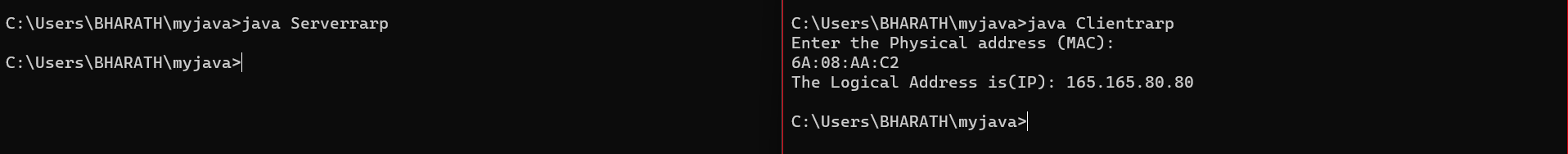
1. Start the program.

2. Server maintains the table in which IP and corresponding MAC addresses are stored. 3. Read the MAC address which is sent by the client.

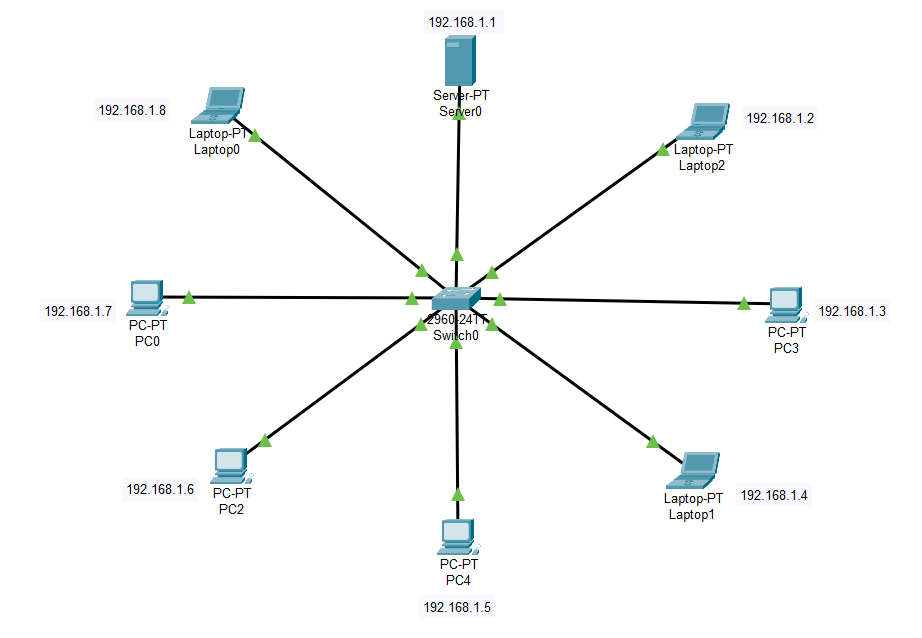
4. Map the IP address with its MAC address and return the IP address to the client.

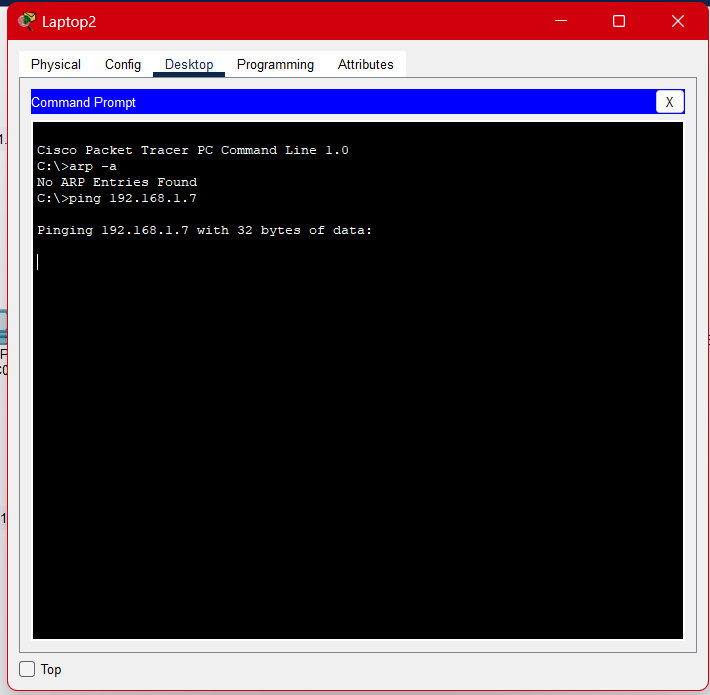
****

**Output:**



**SIMULATION OF ARP/RARP PROTOCOL USING CISCO PACKET TRACER**

****

****