**Experiment 8**

**Date:** 23-09-2021

**Aim:** To simulate the ARP protocol in the CISCO Packet Tracer.

**Software Used:** Cisco Packet Tracer.

**Theory:**

**About ARP -**

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 containing IP addresses and MAC addresses.

ARP caches are kept on all operating systems in an IPv4 Ethernet network. 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 cyberattacks. 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.

**ARP in CISCO Packet Tracer –**

1. Make a sample network and assign IP addresses to the end devices.
2. Open the command prompt of any one of the PC that is **PC0** and open the **simulation mode** of cisco packet tracer.
3. To check for **ARP table**, enter **arp -a** command in command prompt initially you will see that there's no ARP entries showed.
4. Now, enter the **ping** command in the command prompt along with the destination IP address let's say we are taking the **IP address of PC4**, and press enter. You will see that in the Simulation Panel, there is a one packet which is **ICMP** and there is another package which is of an **ARP**.
5. Paly the simulation and observe the movement of an **ARP packet**. As soon as ARP packet gets acknowledged to the ***source PC*** that is a **PC0**, then pause the simulation and click on the **magnifying glass icon** on the on the left corner of the CISCO Packet Tracer and then right click on the source PC. A drop-down menu having the ARP table option will be shown. Click on the ARP table option, the **ARP table** consisting of the destination IP address and MAC address will be shown.
6. Replay the simulation so that all the packets will be transferred successfully. After that, in the command prompt of the source PC enter **arp -a** command and press enter you will see an **ARP table** having a **destination IP address** as well as a **MAC address** that is of **PC4.**

**Observations:**

1. **Network Simulation:**

Diagram

Description automatically generated

1. **ARP Packet in Simulation Panel:**

Graphical user interface

Description automatically generated

1. **PDU Information at Source PC:**

Graphical user interface, application, email

Description automatically generated

1. **ARP Table:**

**Graphical user interface, application

Description automatically generated**

1. **APR Table in Command Prompt:**

Graphical user interface, text

Description automatically generated

**Results and Conclusion:** The simulation of the ARP protocol in the CISCO Packet Tracer has been done successfully.