# DHCP Starvation Attack

By

Sk. Adit Aziz

1505079

## Introduction:

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider, reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.

The base DHCP does not include any mechanism for authentication. Because of this, it is vulnerable to a variety of attacks.

## DHCP Starvation Attack:

DHCP starvation attack is an attack vector in which an attacker broadcasts large number of DHCP requests packets with some spoofed MAC addresses with the intent of exhausting all available IP addresses that can be allocated by the DHCP server. The automatic assignment of network addresses to other legitimate computers is thus made impossible. Then if other computers request for an IP address the server cannot assign any IP address for them.

## Topology:

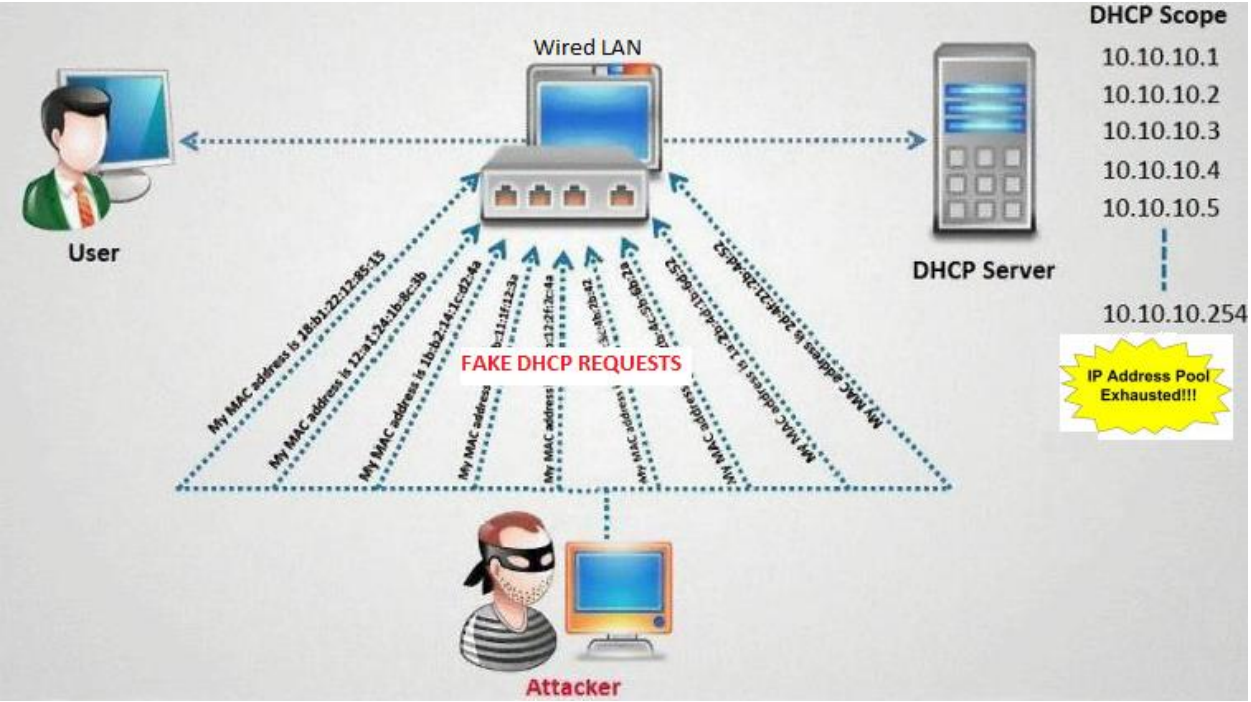


Figure 1: Topology of the network

## Timing Diagram:

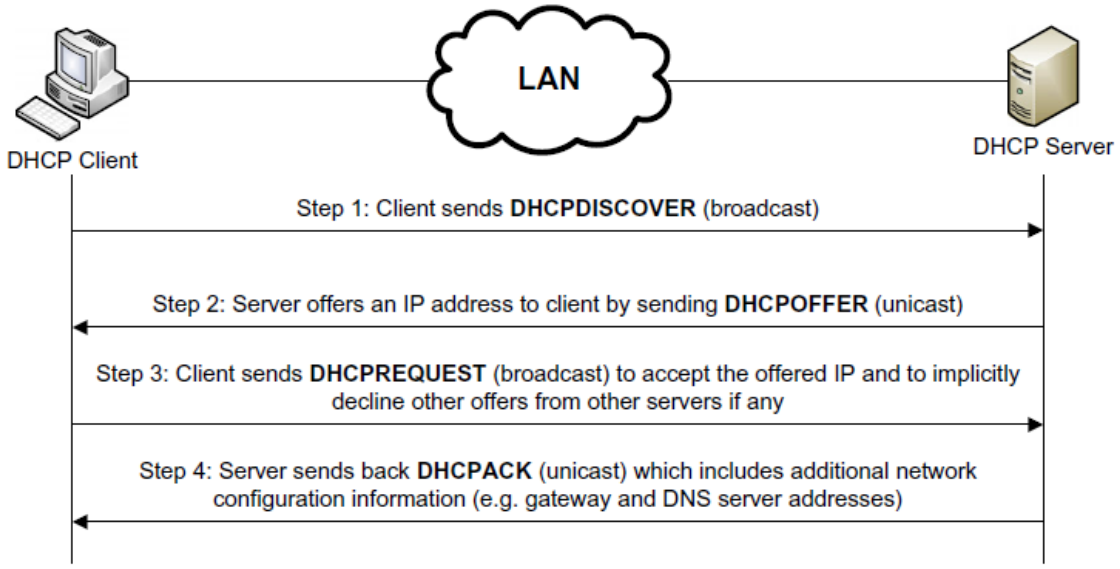


Figure 2: DHCP timing diagram

In DHCP the client has to broadcast a ‘DISCOVERY’ message to the network. Then the DHCP server offers an IP address to client by sending ‘OFFER’ message. After that the client sends ‘REQUEST’ message to accept the IP and in return the server confirms by sending ‘ACK’ message.

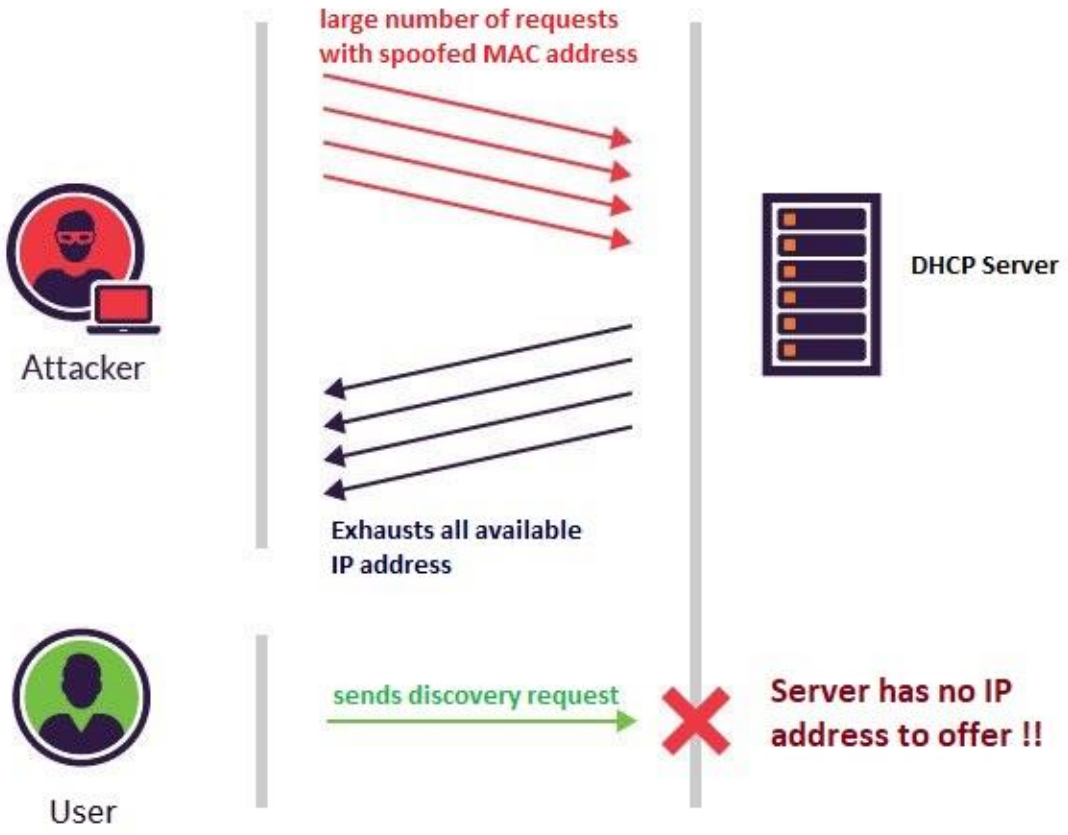


Figure 3: Attack timing Diagram

## My Attacking Strategies:

The strategies of my attack is described in the steps below:

1. First large number of spoofed MAC address need to be generated in the attacker's computer.

2. DHCPDISCOVERY messages with those MAC addresses need to be sent in the LAN as if the server thinks the requests are coming from different machines. So that it replies after assigning with an IP address for each of the MAC addresses.

3. Then after receiving DHCPOFFER message from the server I need to request by DHCPREQUEST message with that MAC address which is inside the DHCPOFFER message for every offers.

## Packet Details:

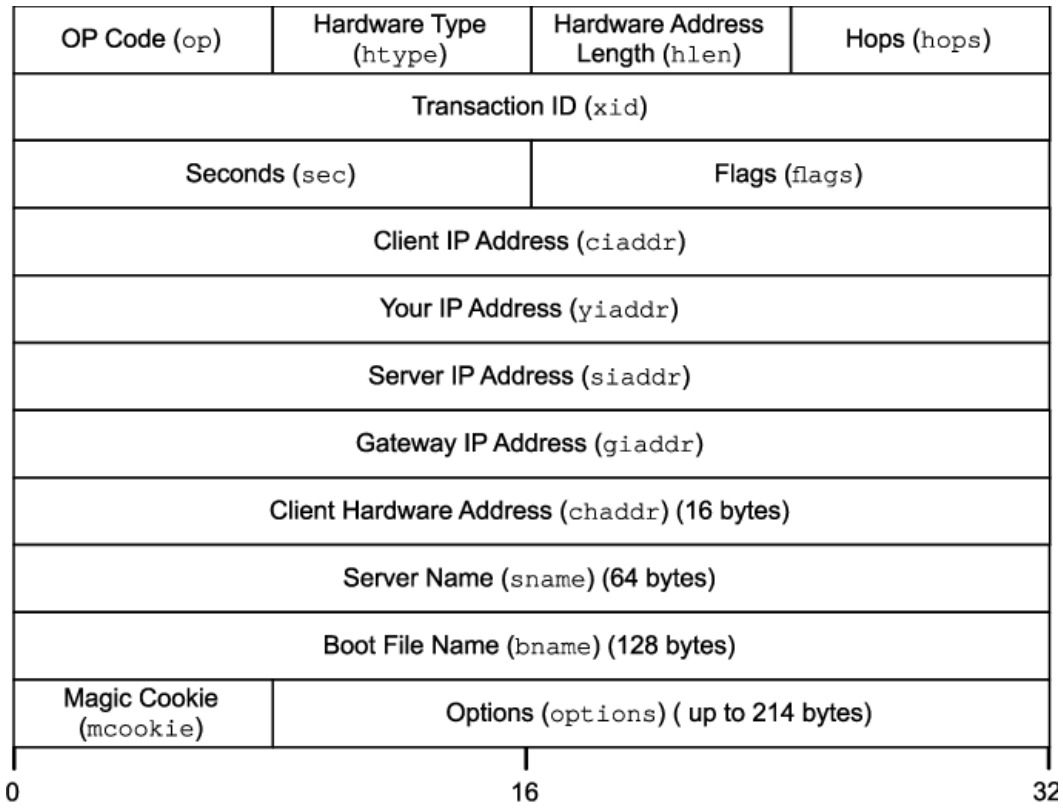


Figure 4: Attack packet details

In the attack packet we have to set the Client Hardware Address (chaddr) field with our spoofed MAC addresses.

## Justification:

If I send DHCPDISCOVERY message to the DHCP server with different MAC addresses, the server would not recognize that all the requests are coming from a single machine. Then it would assign different IP address against each of the MAC addresses. By sending a large number of requests I can acquire all the IP addresses available to the server. Then server would not able to serve any IP address to any legitimate machine's discovery message as it would be thinking that all my IP addresses are being used by different clients or users. Thus I think my attack to the DHCP server to starve other clients would be successful.