Bangladesh University of Engineering and Technology

CSE-406 Design Report

DHCP Spoofing

Submitted To:
Dr. Md. Shohrab Hossain
Associate Professor
Department of Computer Science and Engineering

Submitted By :
Afsara Benazir
1505118

1 Introduction

One of the Layer 2 attacks inside a LAN network that is very dangerous for information privacy and LAN integrity is spoofing attack. This is special kind of attack where attacker can gain access to network traffic by spoofing responses that would be sent by a valid DHCP server.

2 How DHCP Works?

A DHCP server is used to issue unique IP addresses and automatically configure other network information (the DNS domain name and the IP address of the default router, of the DNS server and of the NetBIOS name server).

This configuration, is allocated to the device only for a given time: the lease time.

Basically, mostly in homes and small networks, the DHCP Server is situated in the Router and in large organizational sectors, DHCP Server can be an individual computer also. A DHCP server provides this information to a DHCP client through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction.

A typical DHCP exchange is as follows :

1. `DISCOVER:` The client without IP address configured sends this query to obtain one from the DHCP server. As the client has no information whatsoever about the current network configuration, not even the address of the DHCPserver, the request is broadcasted on the local subnet. The client may already ask for a previously leased IP address.

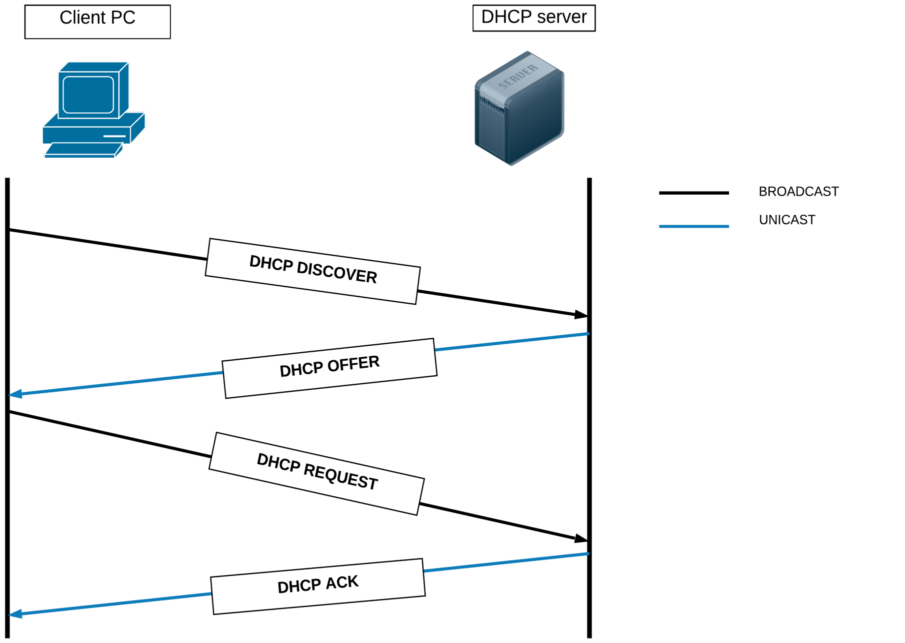
   The server search on its side for a free address he can allocate to the client. This usually involves two mechanisms: The server maintains a local database of leased and available IP addresses. Once an address candidate has been selected, depending on the server implementation the server may take great care that the IP is indeed not already used by sending one or two ARP requests with relatively large waiting time for any potential answer.

2. `OFFER:` The server proposes the address to the client. For availability purposes DHCP allows several servers to send concurrent offers, the client choosing the "best" one. This message is usually sent as unicast to the client MAC address.

3. `REQUEST:` The client broadcasts the address it has chosen. This allows all DHCP servers involved in this exchange to be aware of the client's decision.

Clients wanting to renew an already acquired lease first attempt to directly jump to this step of the discussion by sending a unicast DHCP REQUEST message to the DHCP server which issued the lease.

4. ACKNOWLEDGEMENT: The server acknowledges the client decision and provides him complementary network configuration settings



;

Figure 1: Timing diagram of the original protocol

3 Definition of the attack with topology diagram

In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage.

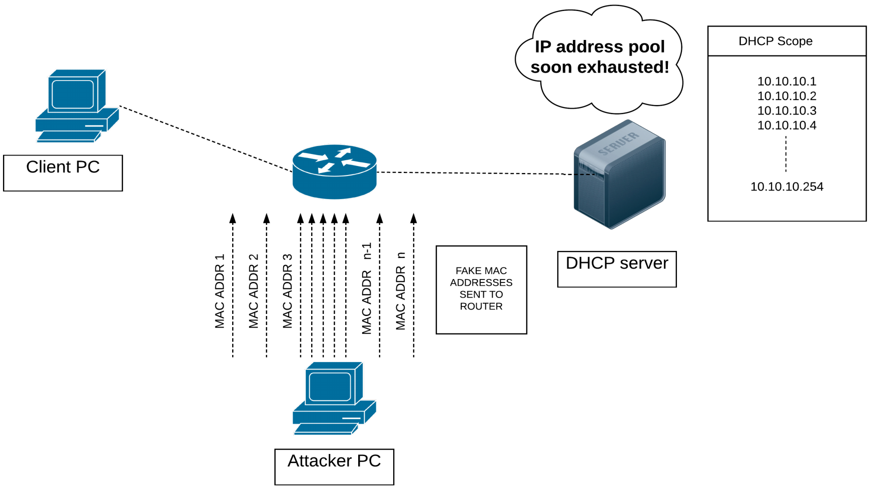
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke IP address resources.

3.1 Rogue DHCP Server :

DHCP Discover traffic are sent as broadcasts and are therefore observable to all devices on the LAN. An attacker connected to the broadcast domain can opportunistically listen for these broadcasts and attempt to respond with an Offer before the real server. This allows an attacker to feed endpoints malicious DHCP lease information that include changes such as an alternative default gateway or DNS server value in order to redirect traffic through the attacker's endpoint to create a man-in-the-middle attack. At the very least it would simply sniff the traffic to analyze it and look at its content, breaching the client's privacy

3.2 What is DHCP Starvation Attack?

DHCP Starvation Attack is a Attack Vector in which a Attacker Broadcasts large Number of DHCP Requests Packets with some spoofed MAC Address. DHCP Starvation Attack is called an attack on a computer network, in which the entire range of available DHCP IP addresses are given to a single client (the attacker). The automatic assignment of network addresses to other computers is thus made impossible. This is a sort of DHCP Flooding Attack or DHCP Denial of Service Attack in which all the IP Addresses of the IP Pool will be consumed by the attacker and no new client will be able to connect to the DHCP Server.



;

Figure 2: DHCP starvation

4 Attacking strategies and Attack timing diagram

4.1 Attacking strategies: Overview

- Attacker enables a rouge DHCP server on a network
- Attacker carries out DHCP starvation attack and depletes the IP address pool of the legal DHCP server.
- When the client broadcasts a DHCP DISCOVER message, the legal DHCP server cannot send an OFFER because it has no available IP address
- The fake DHCP server sends out DHCP OFFER acting as the original server
- Client carries out normal DHCP REQUEST and DHCP ACK operation with the fake server, without having any clue that it is an attacker.

4.2 Attacking strategies: Detailed process

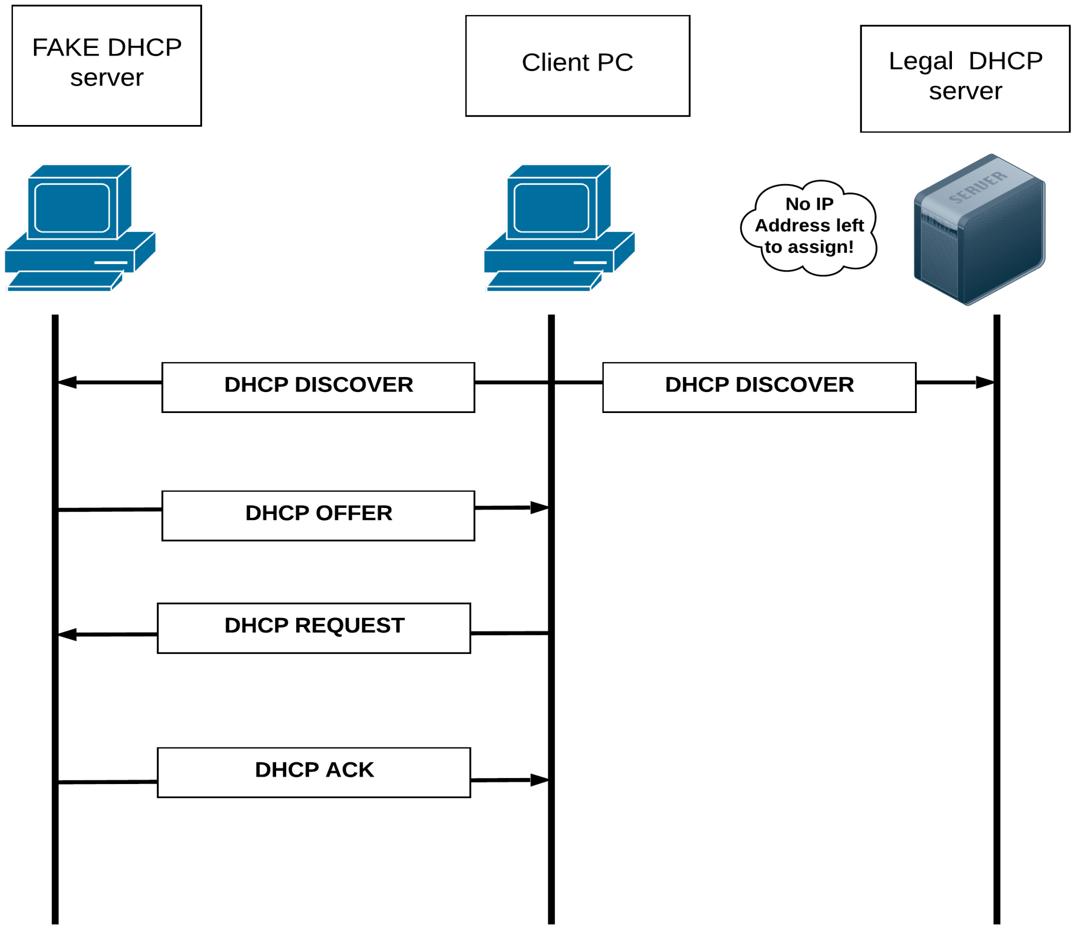
1. The attacker constructs a DHCP packet with its own MAC address and the DHCP server's IP address and sends the packet to the DHCP client.
2. After receiving the packet, the DHCP client learns the middleman's MAC address. As a result, all the packets sent from the DHCP client to the server

pass through the middleman.

3. Alternatively, the middleman constructs a DHCP packet with its own MAC address and the DHCP client's IP address and sends the packet to the DHCP server.

4. After receiving the packet, the DHCP server learns the middleman's MAC address and thinks of it as the client.

Thus, the DHCP server considers that all packets are sent to or from the DHCP client, and the DHCP client considers that all packets are sent to or from the DHCP server. Packets, however, have been processed on the middleman.

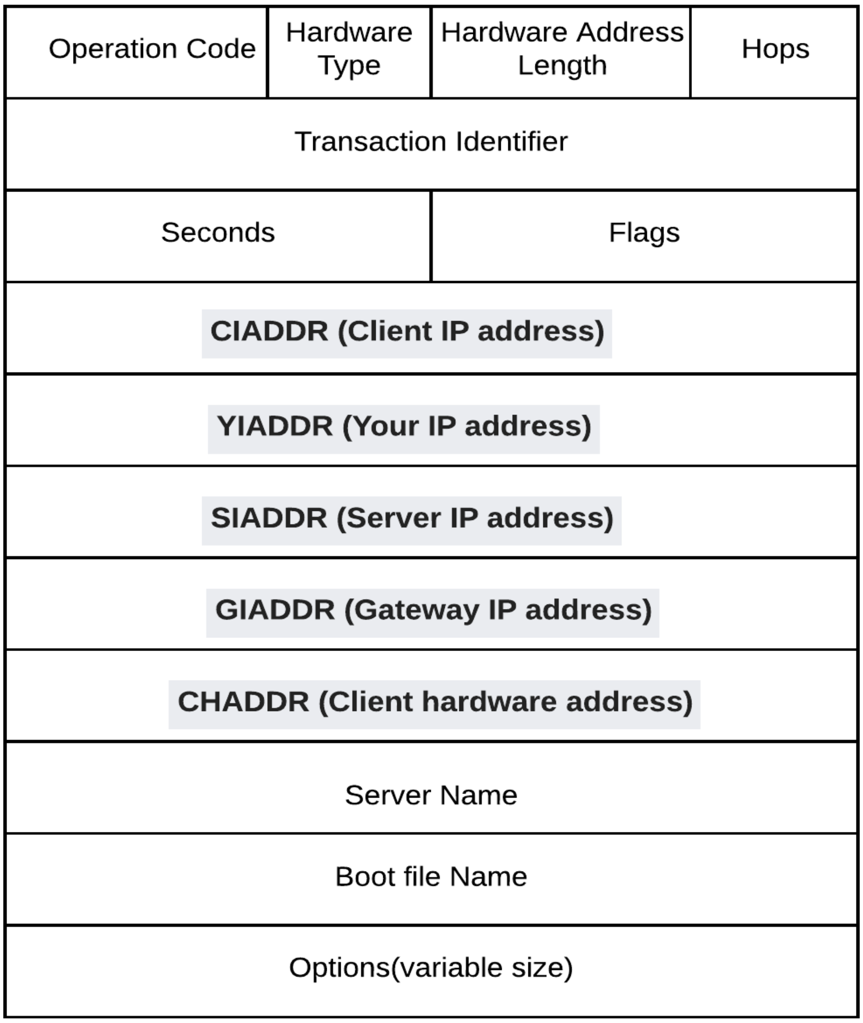


;

Figure 3: Attack Timing Diagram

5 Frame details for the attack with modification

5.1 DHCP Frame:

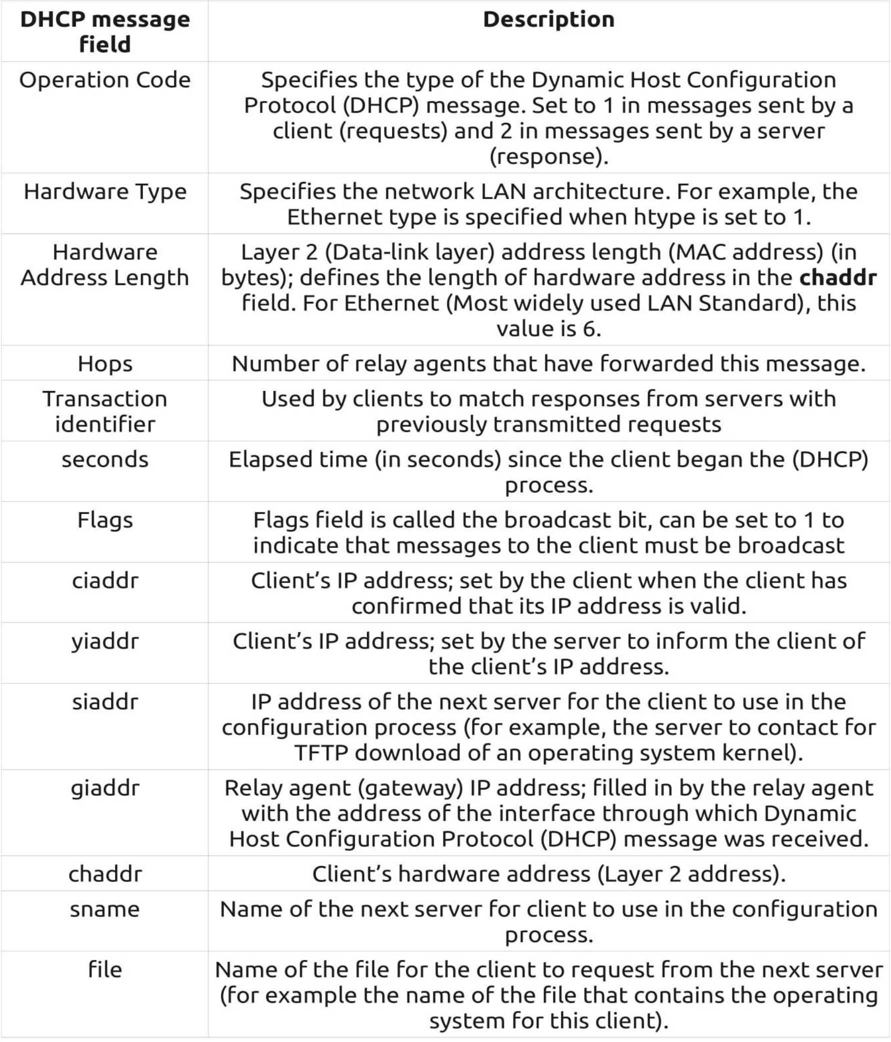


Operation Code	Hardware Type	Hardware Address Length	Hops
Transaction Identifier			
Seconds		Flags	
CIADDR (Client IP address)			
YIADDR (Your IP address)			
SIADDR (Server IP address)			
GIADDR (Gateway IP address)			
CHADDR (Client hardware address)			
Server Name			
Boot file Name			
Options(variable size)			

;

Figure 4: Example Frame

5.2 DHCP message fields

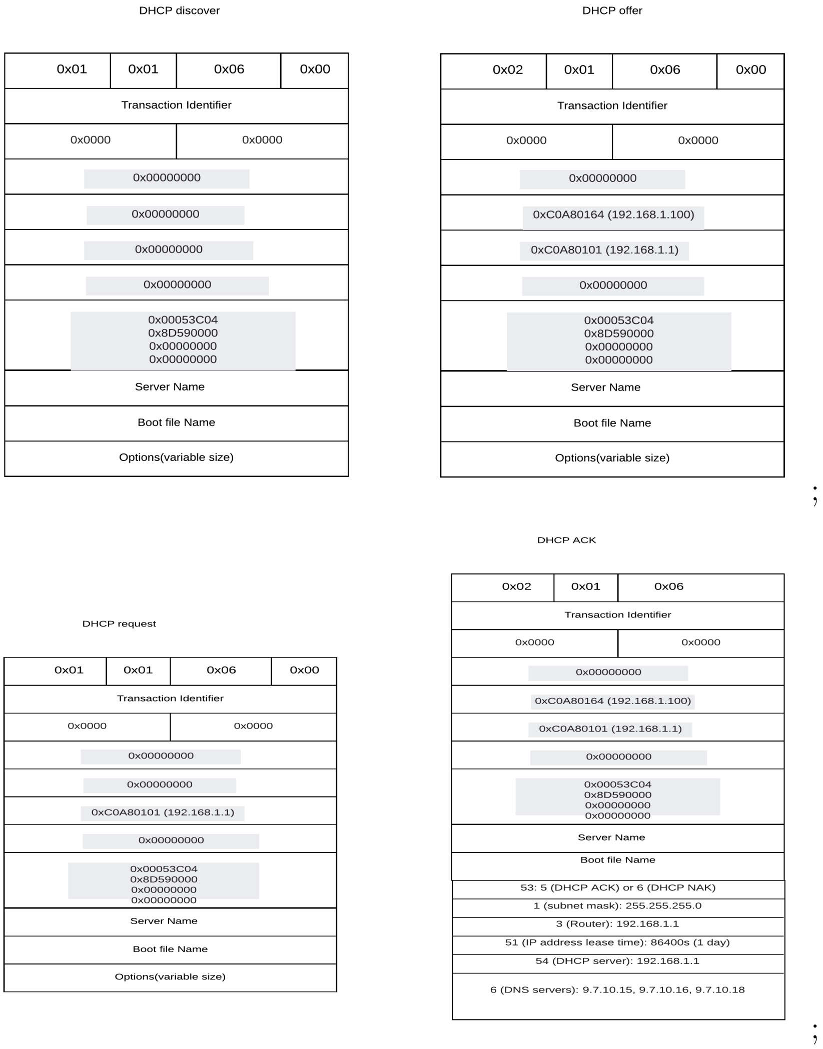


DHCP message field	Description
Operation Code	Specifies the type of the Dynamic Host Configuration Protocol (DHCP) message. Set to 1 in messages sent by a client (requests) and 2 in messages sent by a server (response).
Hardware Type	Specifies the network LAN architecture. For example, the Ethernet type is specified when htype is set to 1.
Hardware Address Length	Layer 2 (Data-link layer) address length (MAC address) (in bytes); defines the length of hardware address in the **chaddr** field. For Ethernet (Most widely used LAN Standard), this value is 6.
Hops	Number of relay agents that have forwarded this message.
Transaction identifier	Used by clients to match responses from servers with previously transmitted requests
seconds	Elapsed time (in seconds) since the client began the (DHCP) process.
Flags	Flags field is called the broadcast bit, can be set to 1 to indicate that messages to the client must be broadcast
ciaddr	Client's IP address; set by the client when the client has confirmed that its IP address is valid.
yiaddr	Client's IP address; set by the server to inform the client of the client's IP address.
siaddr	IP address of the next server for the client to use in the configuration process (for example, the server to contact for TFTP download of an operating system kernel).
giaddr	Relay agent (gateway) IP address; filled in by the relay agent with the address of the interface through which Dynamic Host Configuration Protocol (DHCP) message was received.
chaddr	Client's hardware address (Layer 2 address).
sname	Name of the next server for client to use in the configuration process.
file	Name of the file for the client to request from the next server (for example the name of the file that contains the operating system for this client).

;

Figure 5: DHCP message fields

5.3 Example exchange of frames



DHCP discover

0x01 | 0x01 | 0x06 | 0x00
Transaction Identifier
0x0000 | 0x0000
0x00000000
0x00000000
0x00000000
0x00000000
0x00053C04
0x8D590000
0x00000000
0x00000000
Server Name
Boot file Name
Options(variable size)

DHCP offer

0x02 | 0x01 | 0x06 | 0x00
Transaction Identifier
0x0000 | 0x0000
0x00000000
0xC0A80164 (192.168.1.100)
0xC0A80101 (192.168.1.1)
0x00000000
0x00053C04
0x8D590000
0x00000000
0x00000000
Server Name
Boot file Name
Options(variable size)

;

DHCP request

0x01 | 0x01 | 0x06 | 0x00
Transaction Identifier
0x0000 | 0x0000
0x00000000
0x00000000
0xC0A80101 (192.168.1.1)
0x00000000
0x00053C04
0x8D590000
0x00000000
0x00000000
Server Name
Boot file Name
Options(variable size)

DHCP ACK

0x02 | 0x01 | 0x06
Transaction Identifier
0x0000 | 0x0000
0x00000000
0xC0A80164 (192.168.1.100)
0xC0A80101 (192.168.1.1)
0x00000000
0x00053C04
0x8D590000
0x00000000
0x00000000
Server Name
Boot file Name
53: 5 (DHCP ACK) or 6 (DHCP NAK)
1 (subnet mask): 255.255.255.0
3 (Router): 192.168.1.1
51 (IP address lease time): 86400s (1 day)
54 (DHCP server): 192.168.1.1
6 (DNS servers): 9.7.10.15, 9.7.10.16, 9.7.10.18

;

Figure 6: Example exchange of frames. Here 0xC0A80101 (192.168.1.1) is the real DHCP IP address which the fake server is using, meanwhile the real server cannot do anything since its IP pool is empty

6 Justification

The victim and attacker's PC will be simulated using the same laptop and a household router will be used as a DHCP server (all routers have built in servers). If the attacker is able to successfully carry out the DHCP starvation attack, the IP pool of the router is emptied. Once this check is done, the attacker can distribute its own DHCP messages acting as the router. The process will work if -

- The attacker is able to generate fake IP requests successfully without getting detected by the router.
- The attacker performs the DHCP starvation.
- The attacker possess the pool of IP address of the router.
- The Client PC fails to detect the attacker PC and thinks of it as its original router.