DHCP Spoofing

Student's Name: **Zahin Ahmed**

Student ID: **1605057**

Introduction

DHCP spoofing attack is one of the dangerous attacks inside a LAN network which can easily violate information privacy and LAN integrity.

DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and tries to list themselves (spoofs) as the default gateway or DNS server, hence, initiates a man in the middle attack.

Definition of the attack with topology diagram

How DHCP works:

A typical DHCP conversation has 4 basic steps:

1. **DISCOVER**
   The client with no IP assigned, broadcasts a query for an IP address to the DHCP server as the client doesn't even know the server address.
   DHCP server maintains a local database to manage which IP addresses are already leased and which are currently available. After getting this query, DHCP server looks for an available IP in it's local database.

2. **OFFER**
   The server proposes an available address to the client. This is sent as unicast to the client MAC Address. Several servers can offer addresses to the client at the same time. The client is free to choose the 'best' one.

3. **REQUEST**

The client broadcasts the IP address it has chosen and all the servers in the network become aware of the client’s decision.

4. **ACKNOWLEDGEMENT**
   The chosen server acknowledges the client’s decision and provides the other important network settings.

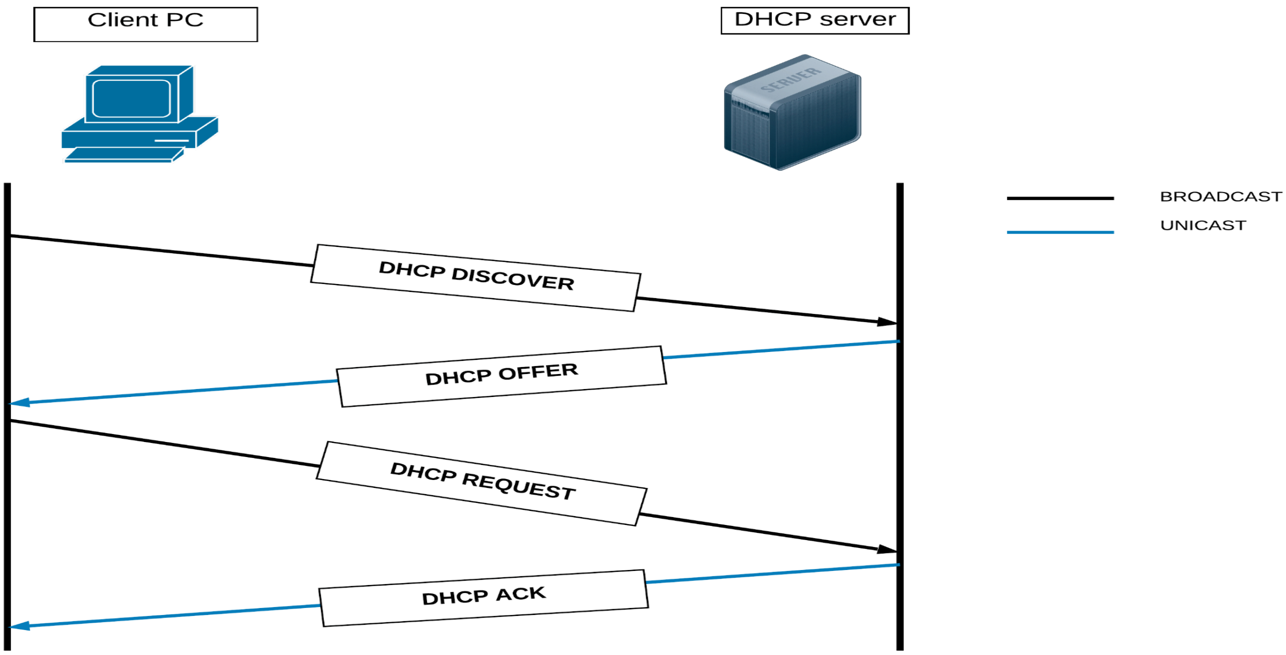


Fig. 1: Timing diagram of the original protocol

Rogue DHCP Server:

DHCP DISCOVER traffic is sent as broadcasts and an attacker connected in the broadcast network can observe these broadcasts and attempt to respond with an OFFER before the original server. The attacker can change the default gateway or DNS server value to redirect traffic through the attacker’s endpoint to create a man-in-the-middle attack. It can breach the client’s privacy by accessing and analyzing personal and sensitive information.

DHCP Starvation Attack:

DHCP Starvation attack is a sort of DHCP Flooding attack or DHCP Denial of Service attack where 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.

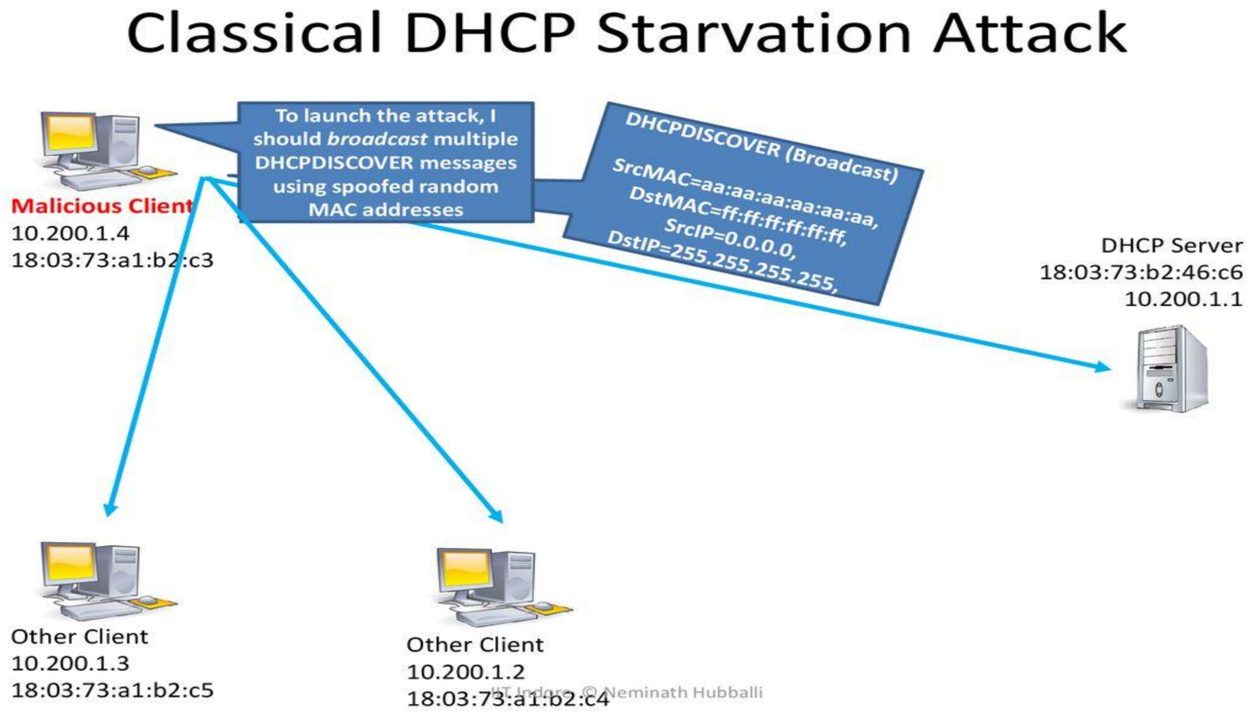

Classical DHCP Starvation Attack
To launch the attack, I should *broadcast* multiple DHCPDISCOVER messages using spoofed random MAC addresses
DHCPDISCOVER (Broadcast)
SrcMAC=aa:aa:aa:aa:aa:aa,
DstMAC=ff:ff:ff:ff:ff:ff,
SrcIP=0.0.0.0,
DstIP=255.255.255.255,
Malicious Client
10.200.1.4
18:03:73:a1:b2:c3
DHCP Server
18:03:73:b2:46:c6
10.200.1.1
Other Client
10.200.1.3
18:03:73:a1:b2:c5
Other Client
10.200.1.2
18:03:73:a1:b2:c4
IIT Indore © Neminath Hubballi

Fig. 2: DHCP Starvation Attack

In a DHCP starvation attack, an attacker broadcasts a large number of DHCP REQUEST messages with spoofed source MAC addresses. If the legitimate DHCP Server in the network starts responding to all these bogus DHCP REQUEST messages, available IP Addresses in the DHCP server scope will be depleted within a very short span of time. Once the available number of IP Addresses in the DHCP server is depleted, network attackers can then set up a rogue DHCP server and respond to new DHCP requests from network DHCP clients. By setting up a rogue DHCP server, the attacker can now launch a DHCP spoofing attack.

After a DHCP starvation attack and setting up a rogue DHCP server, the attacker can start distributing IP addresses and other TCP/IP configuration settings to the network DHCP clients. TCP/IP configuration settings include Default Gateway and DNS Server IP addresses. Network attackers can now replace the original legitimate Default Gateway IP Address and DNS Server IP Address with their own IP Address.

Once the Default Gateway IP Address of the network devices is changed, the network clients start sending the traffic destined to outside networks to the attacker's computer. The attacker can now capture sensitive user data and launch a man-in-the-middle attack. This is called a DHCP spoofing attack.

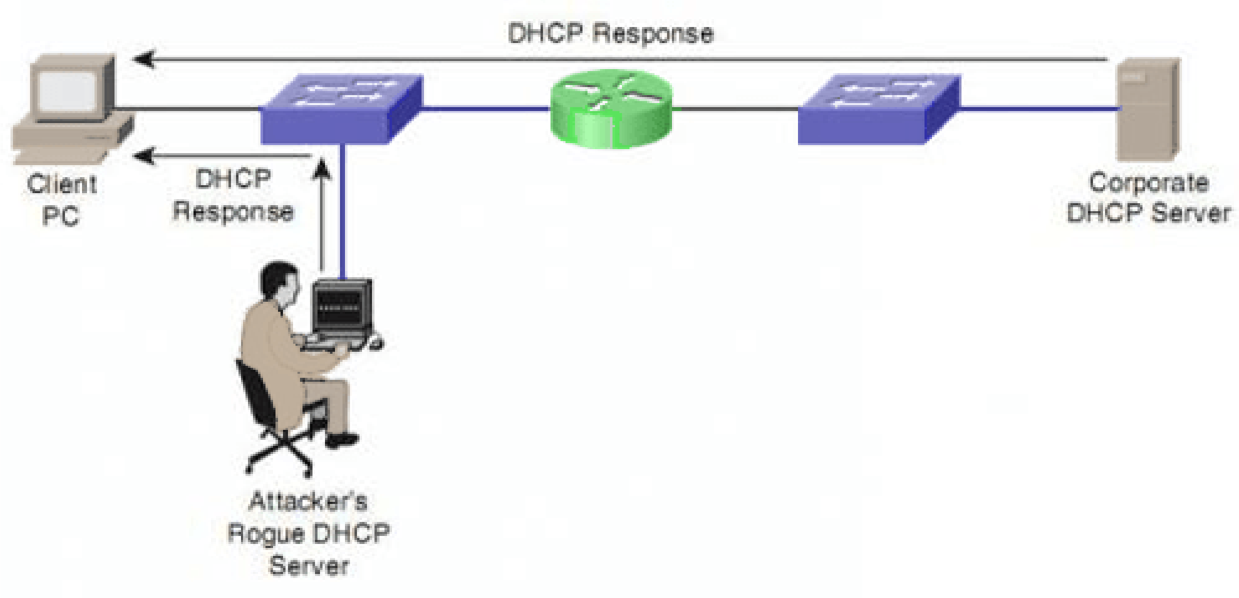


Fig. 3: DHCP Spoofing Attack(1)

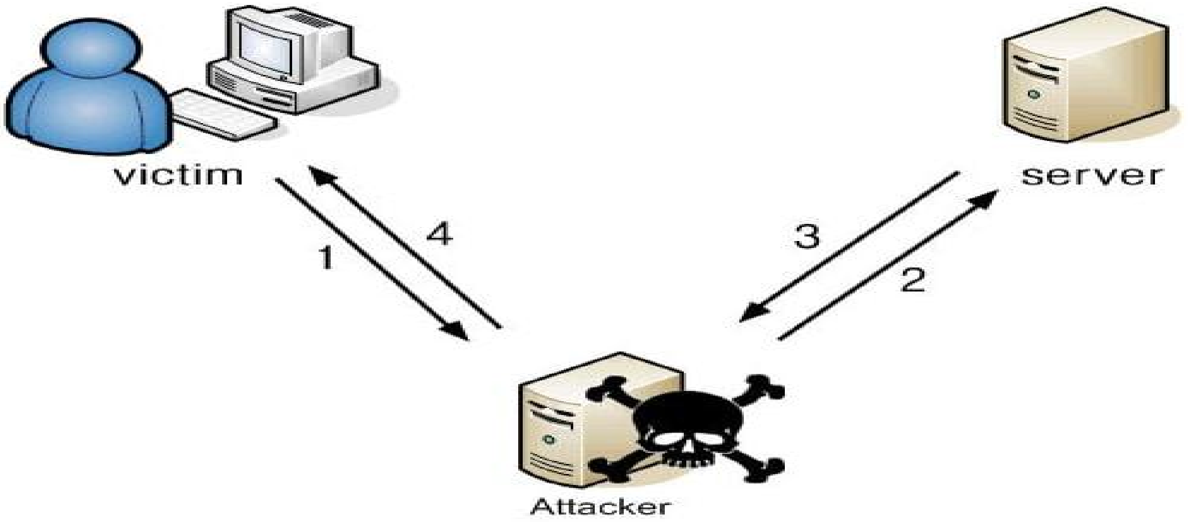


Fig. 4: DHCP Spoofing Attack(2)

Attack timing diagram with attack strategies:

Attack Strategies:

☐ Attacker sets up a rogue DHCP server on the network.

☐ Attacker does a DHCP Starvation Attack to the original DHCP server so that all the IP addresses of the IP pool gets occupied by the attacker so no new client’s DHCP DISCOVER request can be replied with a DHCP OFFER request by the original DHCP server.

☐ Attacker replies to the DHCP DISCOVER request with a DHCP OFFER request to the client acting like the original server.

□ The client carries out the DHCP REQUEST step with the attacker not knowing whether it’s the actual server or not and the attacker performs the DHCP ACKNOWLEDGEMENT step in disguise of the original server.

□ The attacker constructs a packet using it’s own MAC address and with the original DHCP server’s IP address. The client gets the attacker's MAC address thinking it is the original server. The attacker also constructs packets with it’s own MAC address and the client’s IP address and sends it to the actual server. The original server gets the attacker's MAC address thinking it is the client’s address.

□ Thus all packets sent from the original server to the client and vice versa are processed by the middleman, the attacker while the actual server and the client is completely unaware of that.

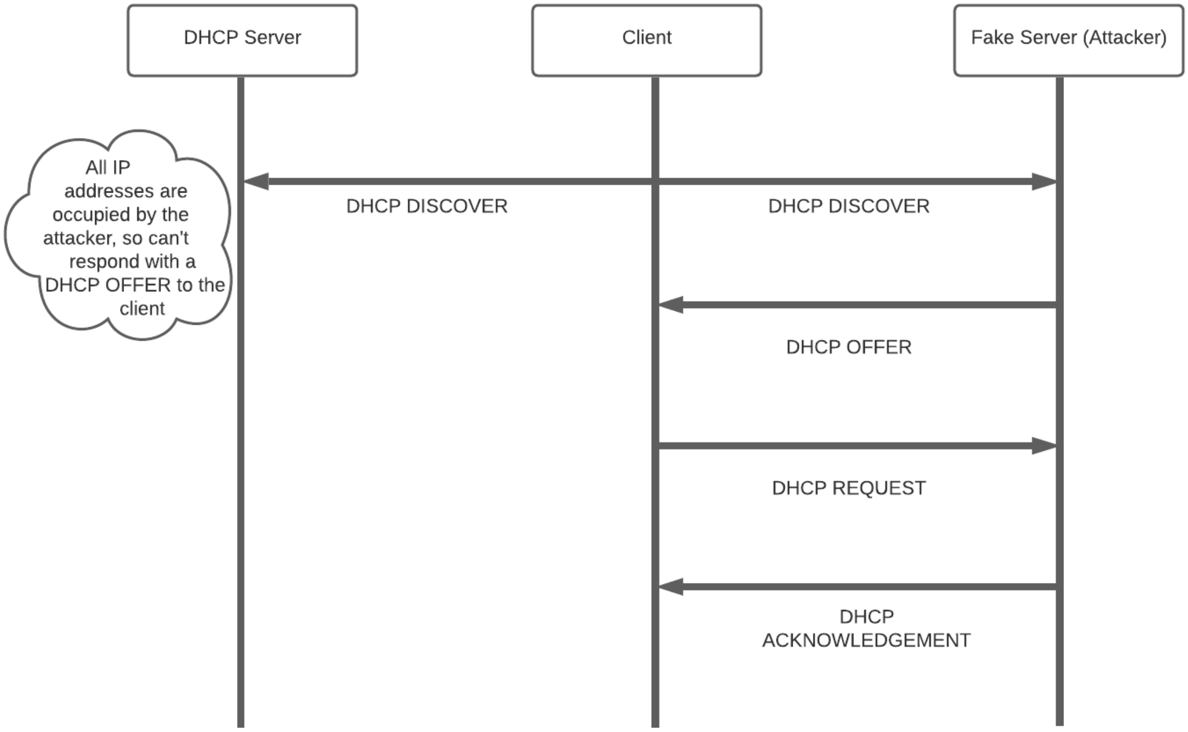
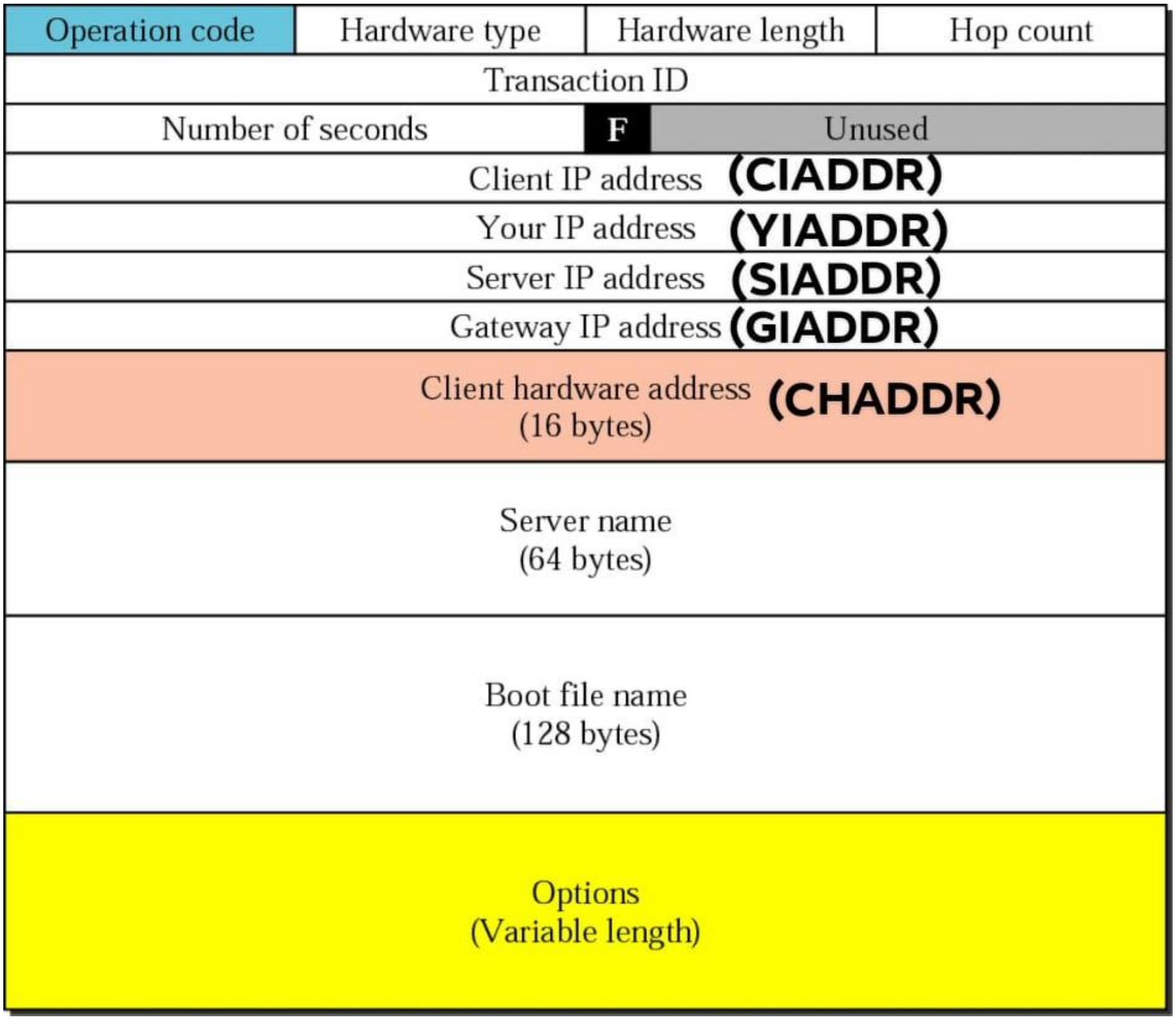


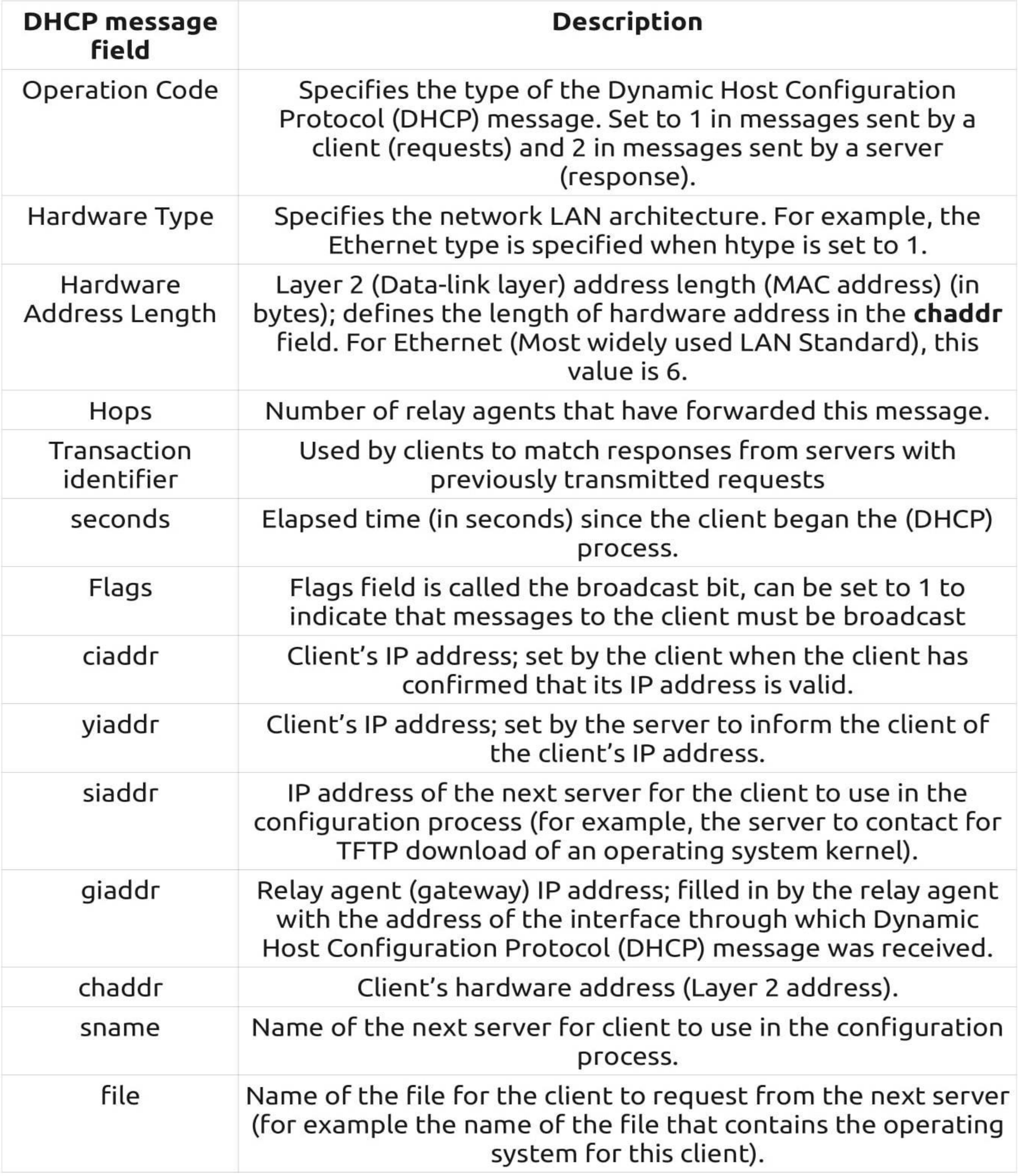
Fig 5: Attack Timing Diagram

DHCP Message Format:



Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds		F	Unused
Client IP address **(CIADDR)**			
Your IP address **(YIADDR)**			
Server IP address **(SIADDR)**			
Gateway IP address **(GIADDR)**			
Client hardware address (16 bytes) **(CHADDR)**			
Server name (64 bytes)			
Boot file name (128 bytes)			
Options (Variable length)			

Description of 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).

Justification:

The victim and the attacker’s PC will be simulated using the same laptop and the household router will act as a DHCP server (routers have built in servers). This attack will be successful if -

- At first, the attacker has to carry out a DHCP Starvation Attack on the router. So, the attacker has to create fake IP requests successfully so that the router can’t detect it.
- Then, the attacker has to perform the DHCP Starvation.
- After that, the attacker has to be able to access the IP address pool of the router.
- Finally, the attacker has to disguise in a way so that the client PC can’t detect it.

If the above mentioned steps can be carried out successfully, the attack can be implemented without fail.