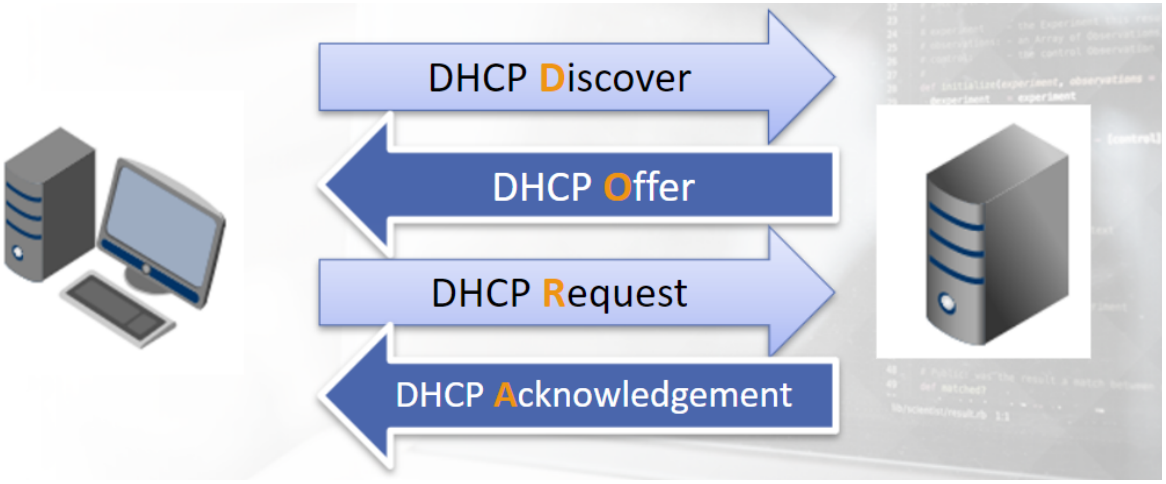
DHCP Traffic:

DHCP stands for Dynamic Host Configuration Protocol, DHCP assign IPs to nodes that connect to the network and allow them have an IP so they can be identified within the network and be able to communicate.

Few things to know about DHCP:

- Automatically assign IP addresses to nodes that connect to the network
- It also provide information like DNS servers, gateway… mean when a device connects, with DHCP when assigning IPs it will also tell the node about the gateway to use and DNS servers address they can use.
- DHCP uses the DORA process (DHCP Discover, Offer, Request, Acknowledgment)
- It uses UDP port 67 & 68

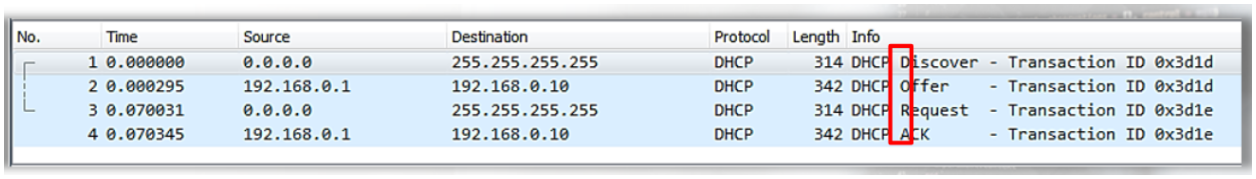
Here is the visualization of DORA:



So when a device connects, it will start with Discover request which is to Discover the DHCP server with the broadcast request (opportunity for the attacker to have a Rogue DHCP server and respond to this broadcast reqeust), the DHCP server will offer an IP address with DHCP Offer, and then the device will Send DHCP Request for that Offer, and then the DHCP server will acknowledge that, its like saying okey.

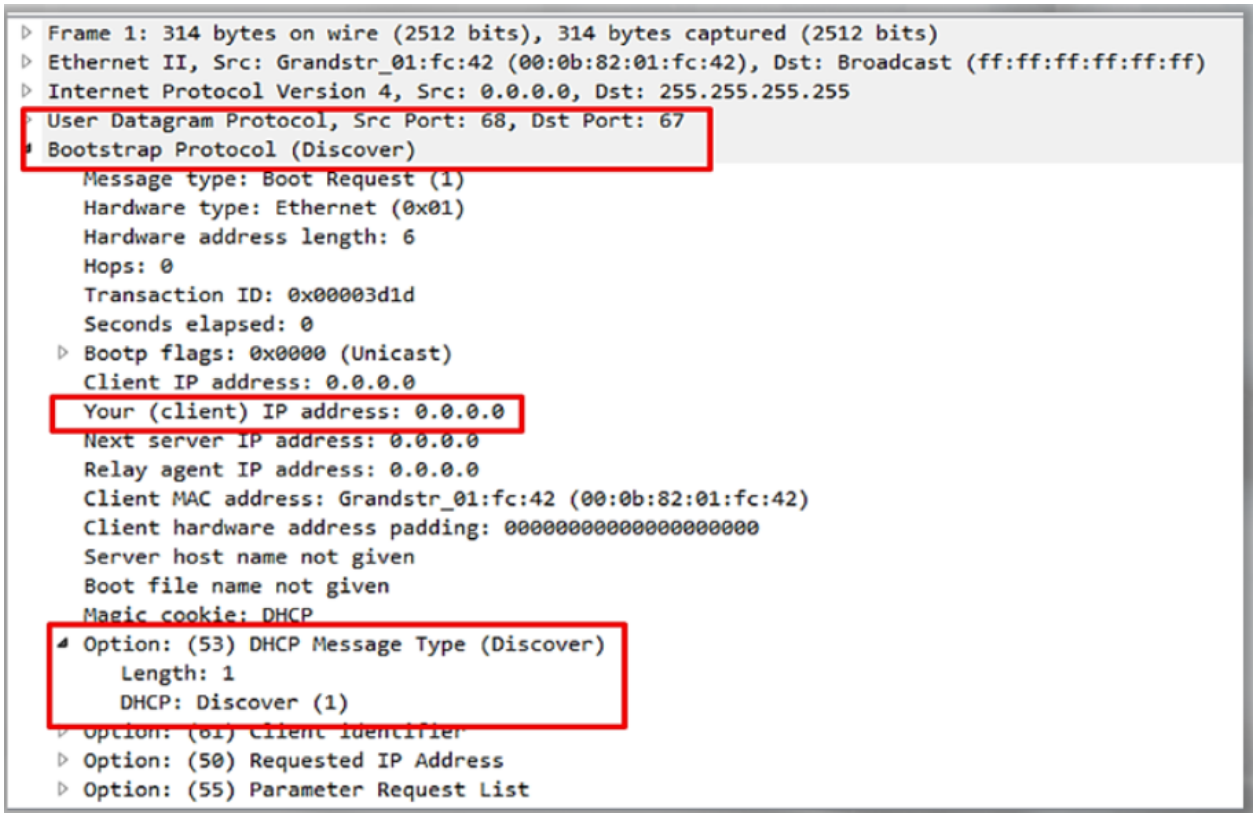
DHCP Normal:

Here we see the process of DORA in wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

Here is the Discover Request Packet:

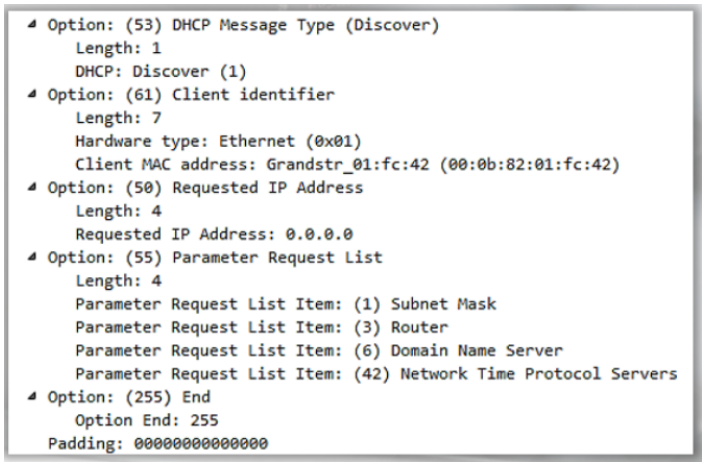


```
▷ Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
▷ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▷ User Datagram Protocol, Src Port: 68, Dst Port: 67
◢ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ◢ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  ▷ Option: (61) Client identifier
  ▷ Option: (50) Requested IP Address
  ▷ Option: (55) Parameter Request List
```

Here we see that the client IP is 0.0.0.0, mean it dosnt have an IP yet, and we see the Destination is 255.255.255.255 and its broadcast addresses as the node or the device dosnt know the DHCP server so it asks everyone in the network. we see the source port is 68 which is the host that request for IP and the dst port which is the DHCP server port.

We see the destination IP is 255.255.255.255, which is asking everyone for the DHCP server, so here the attacker has the chance to act as a rogue DHCP and respond that it's the DHCP server.

In this packet we see the option which is sub info in them lets look into it:

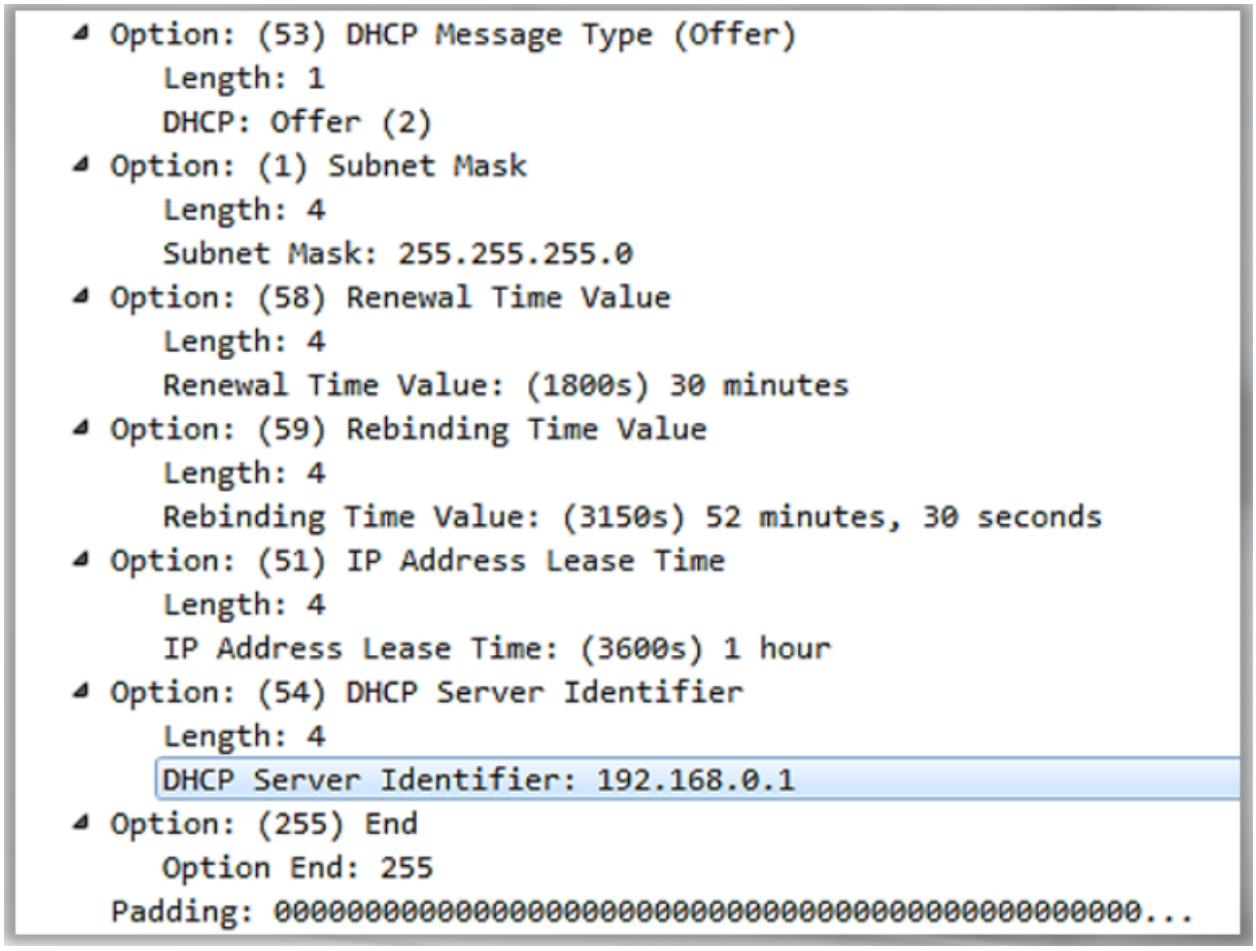


As we said before that the DHCP also provide info about the Gateway, DNS server… so here in the Discover the Client also asked the DHCP server to give it the Gateway (router), DNS info, Subnet mask, NTP so it can synchronize with the network.

DHCP offer packet:

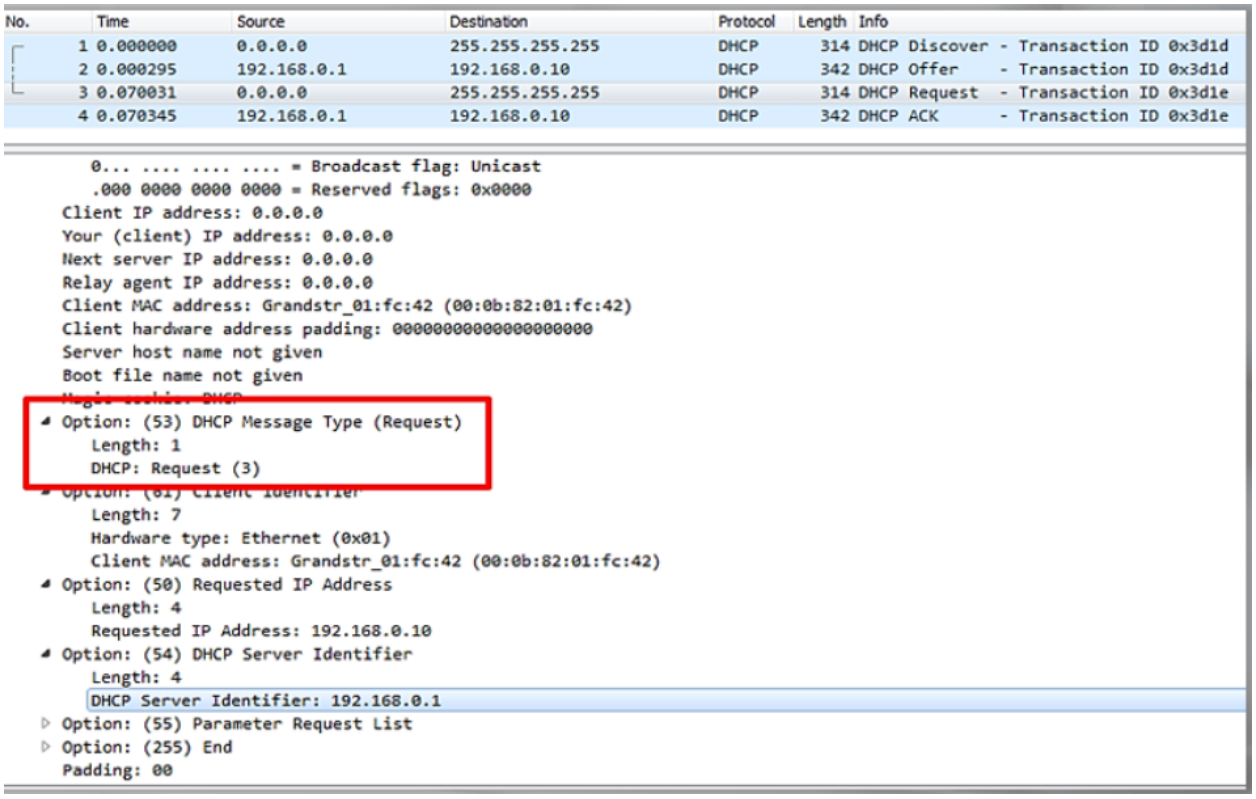
Here the DHCP server is offering an IP to the node that was looking for DHCP server with the Discover request. Here we the IP that was offered is 192.168.0.10 by the 192.168.0.1 which this is the address of the router where the DHCP server is usually.

Here is the rest of the packet:



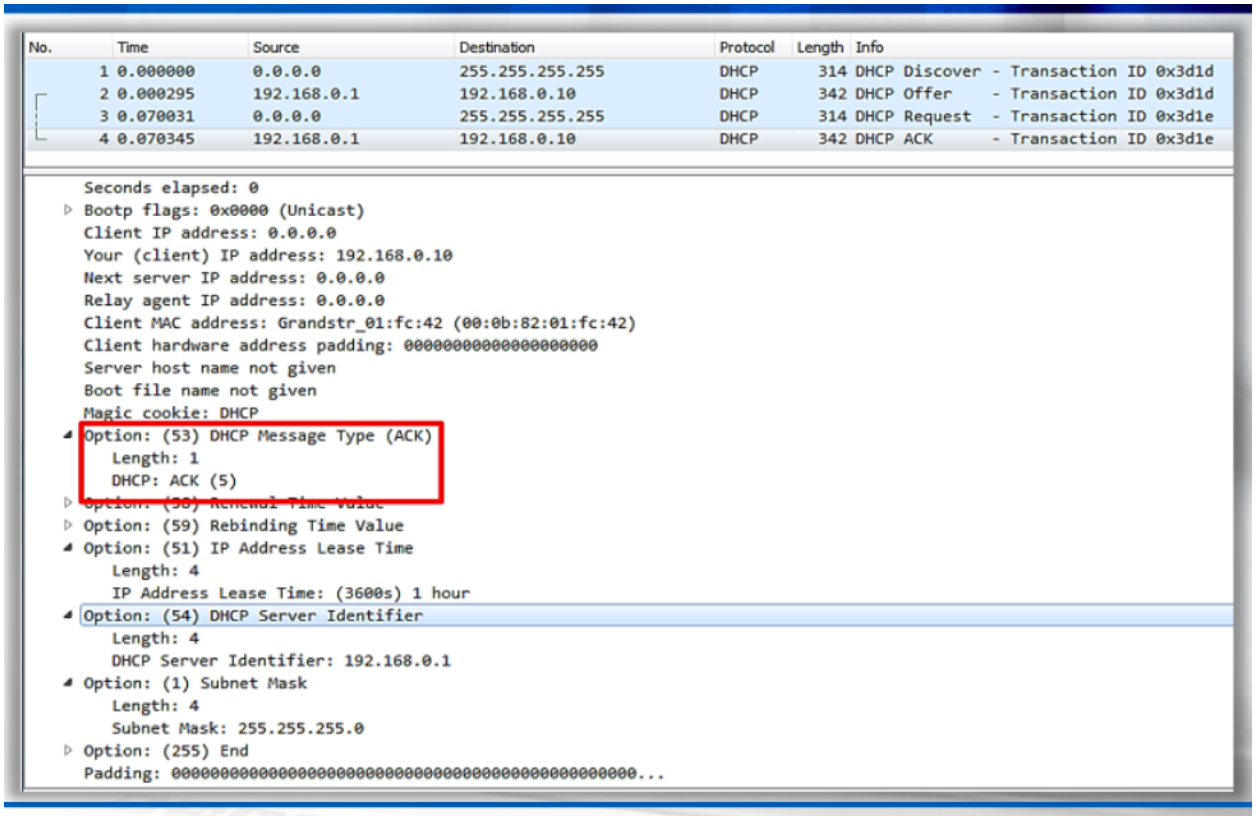
As we said about the DHCP server IP, it's the same as the router IP here which means the DHCP server is In the router.

The request:



Here the request is made by the node to accept the offer:

The Acknowledgement:



The DHCP here acknowledge that the user got the IP, or acknowledged the user accepted the offer.

We should carefully look at the DHCP request and responding to the DHCP requests, as we saw there is Discover request sent by the node when it connects to the network, in here the attacker can act as DHCP server and this can lead to MITIM attack and what if the attacker change its mac address and then send another DHCP request for a new IP? Yes this is possible and this can lead to DHCP running out of IP and cant assign IPs to the new devices so these new devices cant connect to the network as they are given out. Mean when a device connect to the network, they will get an IP and they can keep it for like 2 days, so that mean this IP will not be given to a new device until the 2 days pass by.