DYNAMIC HOST CONTROL PROTOCOL :

1. It is an application layer (UDP) (port: 67) protocol that is used to automate the process of assigning IP address and other network related information like subnet mask, DNS server address, default gateway to devices when connected to internet instead of manually assigning these network details.
2. It is based on client-server model where DHCP client (end host which requires IP) requests DHCP server (which maintains pool of IP and other network related info) and server responds back with valid data. This communication happens with the help of DHCP relay (by default, routers wont broadcast packets. Thus , the client broadcasts will reach only within the subnet. If no dhcp servers present there, it leads to issues in connecting with internet. So , routers today are configured to act as relay that forwards as unicast the request from client to intended server )
3. DHCP client will be given IP address under lease. That is , there will be predefined expiry time for obtained details upon which client should possibly renew it to reuse it.
4. DHCP IP assignment is done by DORA process. It is explained as follows:
   1. Discover : It is the first communication between client and server in search of IP. Client sends a broadcast request packet with its MAC and destination IP as all “F” (since client doesn’t know particular server before hand) requesting for DHCP info (with and without IP- other infor alone) with client ID
   2. Nack : this message will be sent by server in case if the request is invalid or no IP is available in its pool.
   3. Offer : This message will be given by server in response to request sent. Since there will be many servers in network, server ID will be mentioned in this packet so that further communication from client will be targeted towards this server. DHCP server will analyze its pool for valid unused IP and allocates one if exists in this packet and sends as broadcast. (Default lease time : 72 hrs)
   4. Request : After getting offer, client broadcasts gratuitous ARP packet in its network to ensure no other device uses same IP to avoid conflict. In case, no reply for ARP found , it is considered safe and sends request packet to server stating that it is ready to use the allocated IP. In case, if offer found invalid, it sends Decline message to appropriate server.
   5. Acknowledgment : this is the final communication from server acknowledging the IP allocation and makes entry in its table with lease time.
   6. Release : This packet will be sent from client side in case if it is releasing IP allocation before its lease time

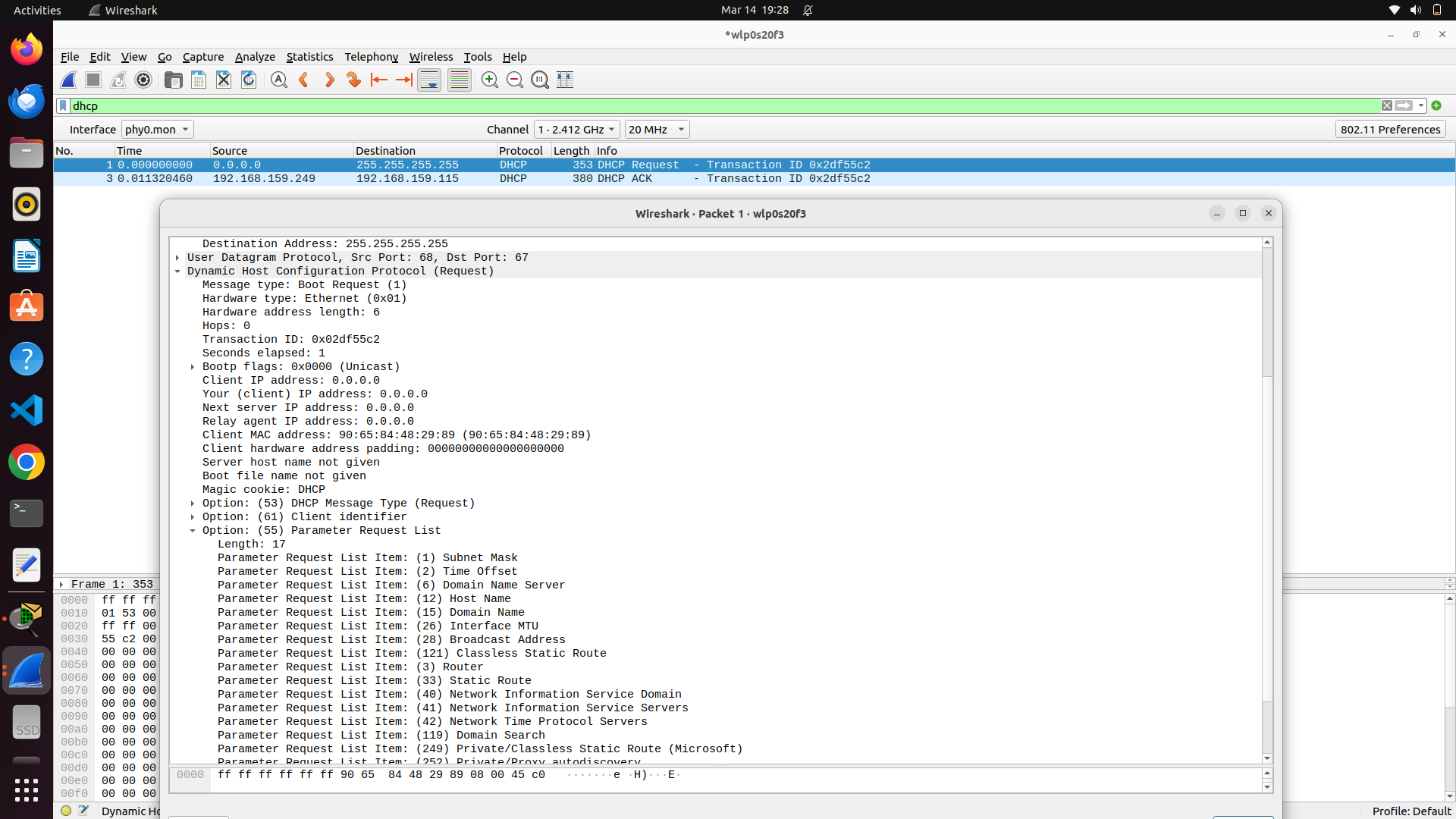
Advantages :

1. DHCP lets the users get IP addresses without hassle
2. Centralized maintenance
3. Supports IP reuse.

Disadvantages :

1. Absence of servers may reduce chance for client to get connected to internet.
2. DHCP fake servers may respond with malicious IP addresses.
3. DHCP flooding may reduce server’s performance for valid clients.

SAMPLE WIRESHARK CAPTURE SHOWING REQUEST AND ACKNOWLEDGMENT PACKETS



It is very common that if particular wifi ssid is already connected and used, it remembers the previously assigned IP and other details thus requesting the same IP again with request and expecting ACK back.

It is also possible in the case of using Relay since wireshark captures only the packets in the current subnet.