SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU-572103
(An Autonomous Institute under Visvesvaraya Technological University, Belagavi)

Department of Electronics and Communication Engineering
2022-23

DHCP Protocol analysis using Wireshark

CCNA Project

Submitted To :

Dr. SEEMA B HEGDE
Assistant Professor
Department of ECE

Submitted by :

1SI20EC117 Usama Ahamed

1SI20EC121 Preetham G M

1SI20EC131 Sachin Chimmalagi

1SI20EC101 Thatireddy Yaswanth Reddy

Dynamic Host Configuration Protocol

DHCP stands for Dynamic Host Configuration Protocol and it is an extension of BOOTP (the previous IP allocation specification) and it is an internal protocol in which computers dynamically get IP addresses from DHCP Servers. The basic functionality of the DHCP Server is to automatically assign the IP address to client machines and other network information such as the subnet mask, the default gateway, and the Domain Name system (DNS) address. DHCP also eliminates the involvement of network administrator and also it prevents from IP address conflicts among client machines connected to the same network. This can help us to manage the large networks easily.

DHCP is used extensively in corporate, University and home network to assign IP address dynamically to hosts and it is used both in wired and wireless LANs. In an IP network, when we connect our machine (host or client) connecting to the Internet it needs a unique IP address. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically assign a new IP address when a computer is plugged into a network. As DHCP server automatically assigns IP address to a host from a pool of address; there is an issue of IP address conflict. As we know DHCP client may receive multiple offers from DHCP Server and what happens here, the client accepts the first offer it receives.

To keep track of how IP address is assigned, a DHCP server uses the concept of leasing; it means that IP address is assigned for a fixed duration of time, called leasing. Just before the expiry of the lease, a computer should request the DHCP server for renewal. Otherwise, that IP address cannot be used further.

1.1 DHCP Process

Understanding the basics of a DHCP Process will help us to understand and remember the how to configure the IP Address for a host available in DHCP Pool. The DHCP Server can also issue otherconfigurations to the client that help to function on the network such as the addresses Domain Name System [DNS], Default Gateway Windows Internet Naming Service [WINS] servers. Wireshark has been used to investigate the DHCP packets in detail. This protocol helps reduce administrative overhead on an IP-based network. The DHCP request process breaks down into four steps:

1.1.1 DHCP Discover

The investigation of DHCP Discover packet has been carried out in a home network where a single PC was connected to that network. There has been an exchange of four different packets in which the PC broadcasts a message to the DHCP Server. The function of the DHCP Server is the reply to the DHCP client and assign an IP address that is unicast. From Fig. 1 it is clear that a unique transaction ID is assigned to these packets.

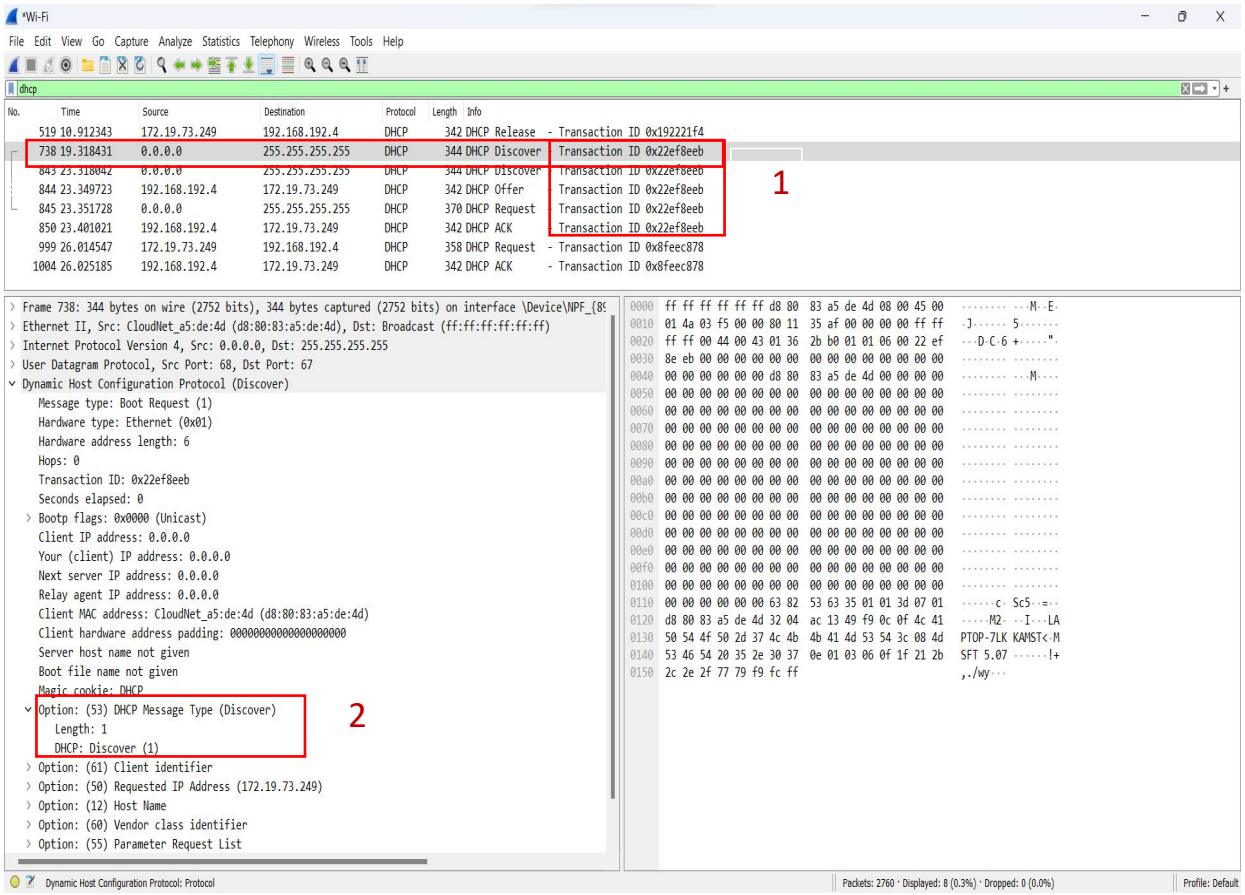

Figure 1: Analysis of DHCP Discover packets in Wireshark

1.1.2 DHCP Offer

The Server responds with a DHCP Offer (unicast), however if there are many offers from a different DHCP Servers the client accepts the first offer. Additionally, the offer from the DHCP Server is not an assurance that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. From Fig. 2 it is clear that there is an offer for DHCP Server to DHCP Client.

1. The offered IP address to the DHCP Client is based on lease. Here on this home network the lease that is offered to DHCP Client is 8 days. After the expiration of this lease, it will not be renewed. The default time of the lease is one day. DHCP Server will block this IP address and it will be unavailable for other DHCP Clients.

2.The DHCP offer has also mentioned the renewal time that is 4 days.

3.The rebinding time value is 7 days.

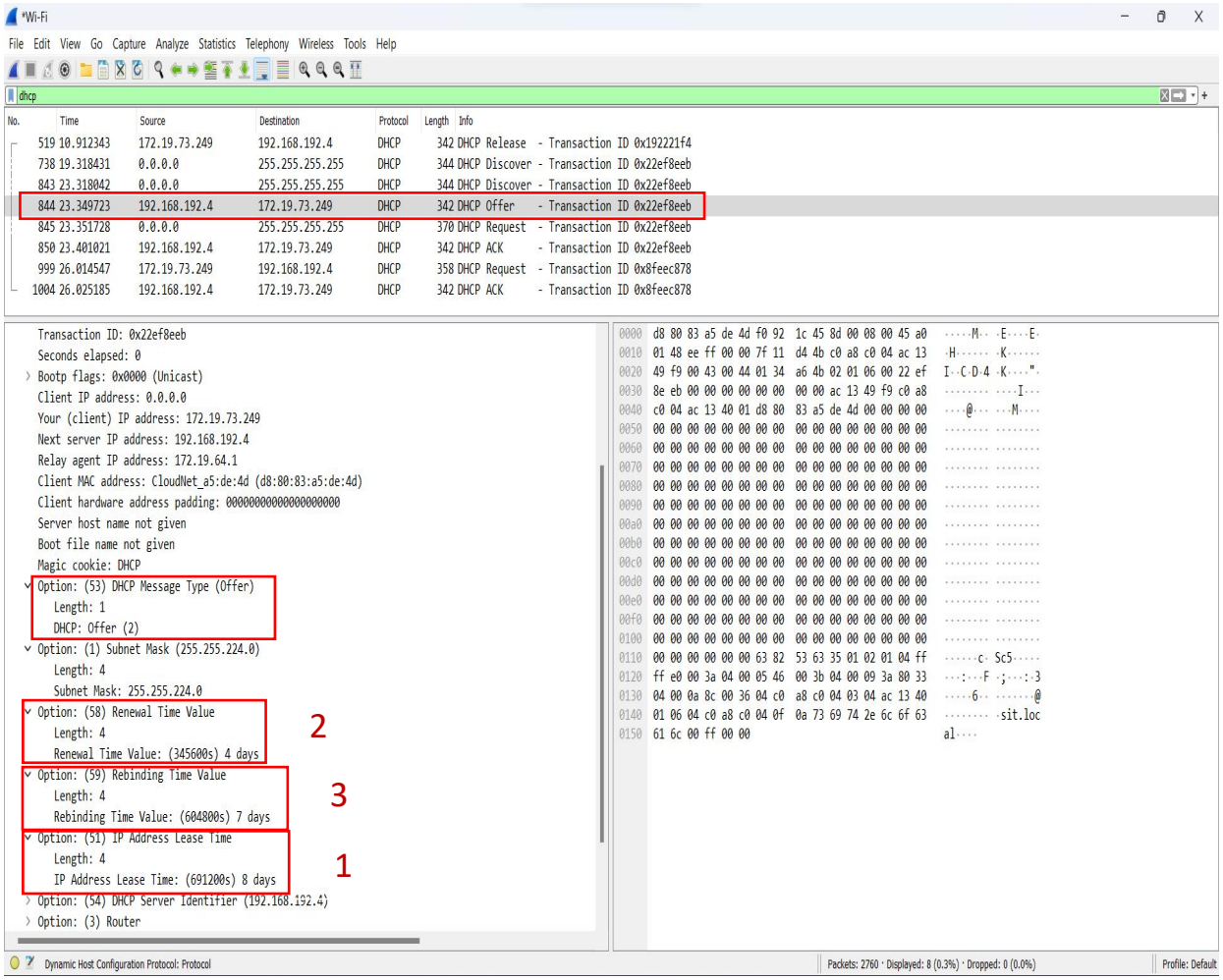

Figure 2: Analysis of DHCP Offer packets in Wireshark

1.1.3 DHCP Request

The client sends DHCP Request (Broadcast) that it has accepted the offered IP and it implicitly declines other offers from other servers if any. From Fig 3 the following contents were found while analysing the DHCP Request packets:

1. The Client IP address is still 0.0.0.0. This means that IP address has not been assigned to the DHCP Client. The destination IP address is 255.255.255.255 which means DHCP request is also broadcasted.

2. The IP address that is offered from DHCP Server to DHCP Client is 172.19.73.249

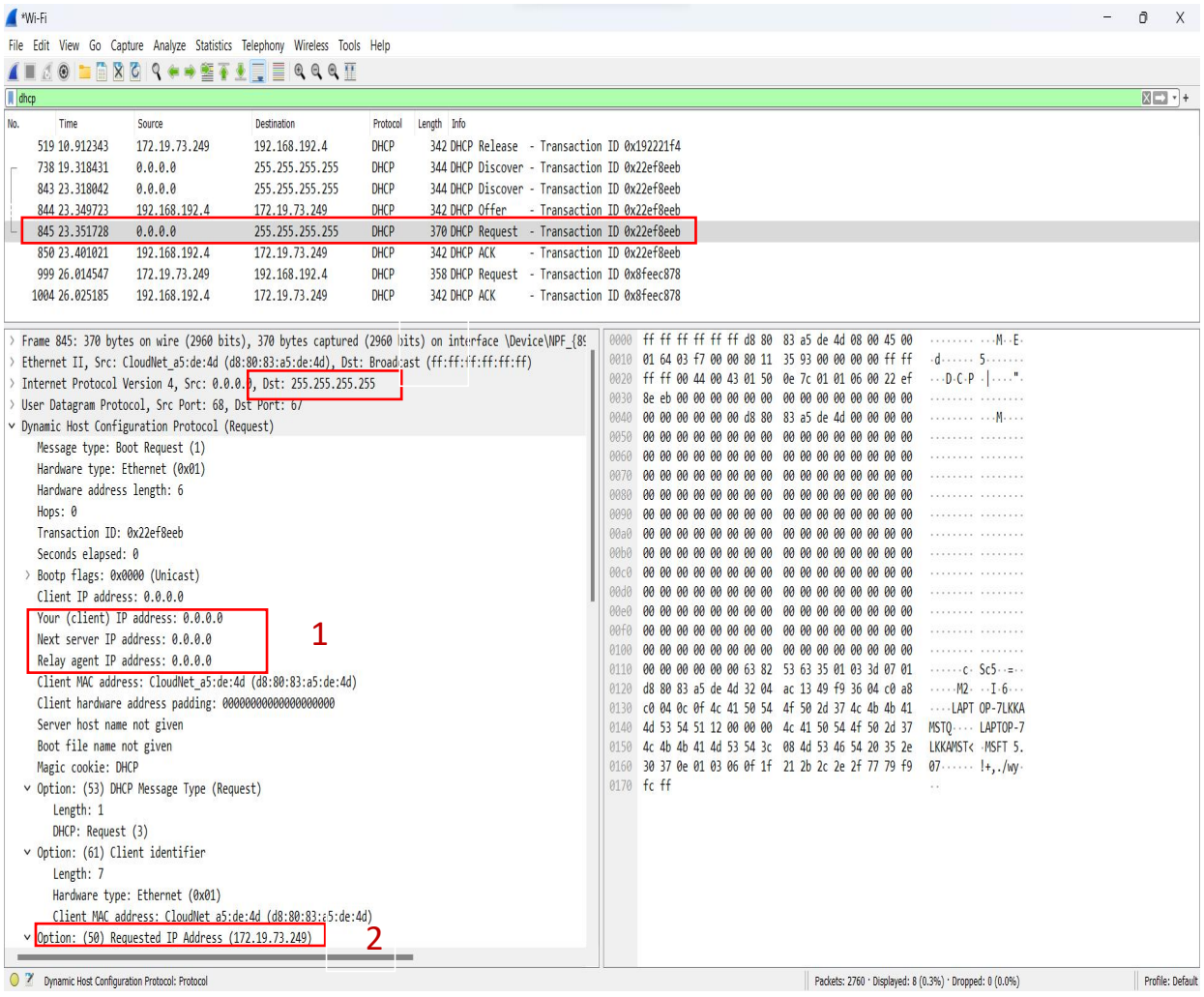

Figure 3: Analysis of DHCP Request packets in Wireshark

1.1.4 DHCP ACK

The DHCP server sends back DHCP ACK (unicast) which includes additional network parameters (gateway and DNS server addresses). Fig. 4 gives the contents found while analysing the DHCP ACK packets:

1. The DHCP Server will now assign the IP address to the Client i.e.; 172.19.73.249 and blocks this IP address for further use till lease time expires.

2. The IP address that is assigned to DHCP Client has a lease time. After the expiration of the lease it will be taken away from the DHCP Client and will become available in the DHCP Pool.

3. The renewal time value of an IP address is 4 days. This means the end of the renewal time the IP address of the DHCP Client is changed.

4. The rebinding time value is 7 days.

5. The subnet mask of the IP address is 255.255.255.0.This means there can be 254 available IP address in the DHCP pool.

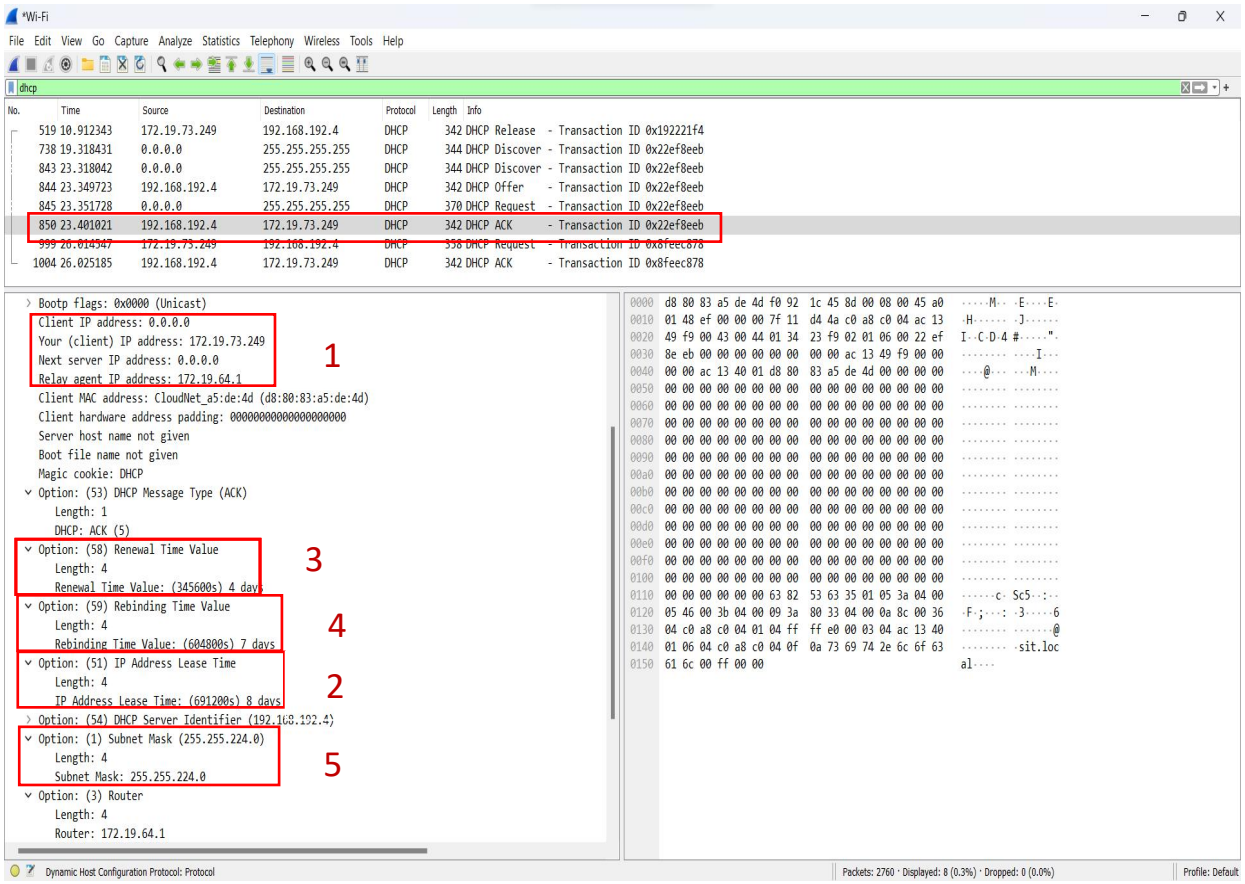

Figure 4: Analysis of DHCP ACK packets in Wireshark

1.1.5 DHCP WIRESHARK LADDER DIAGRAM

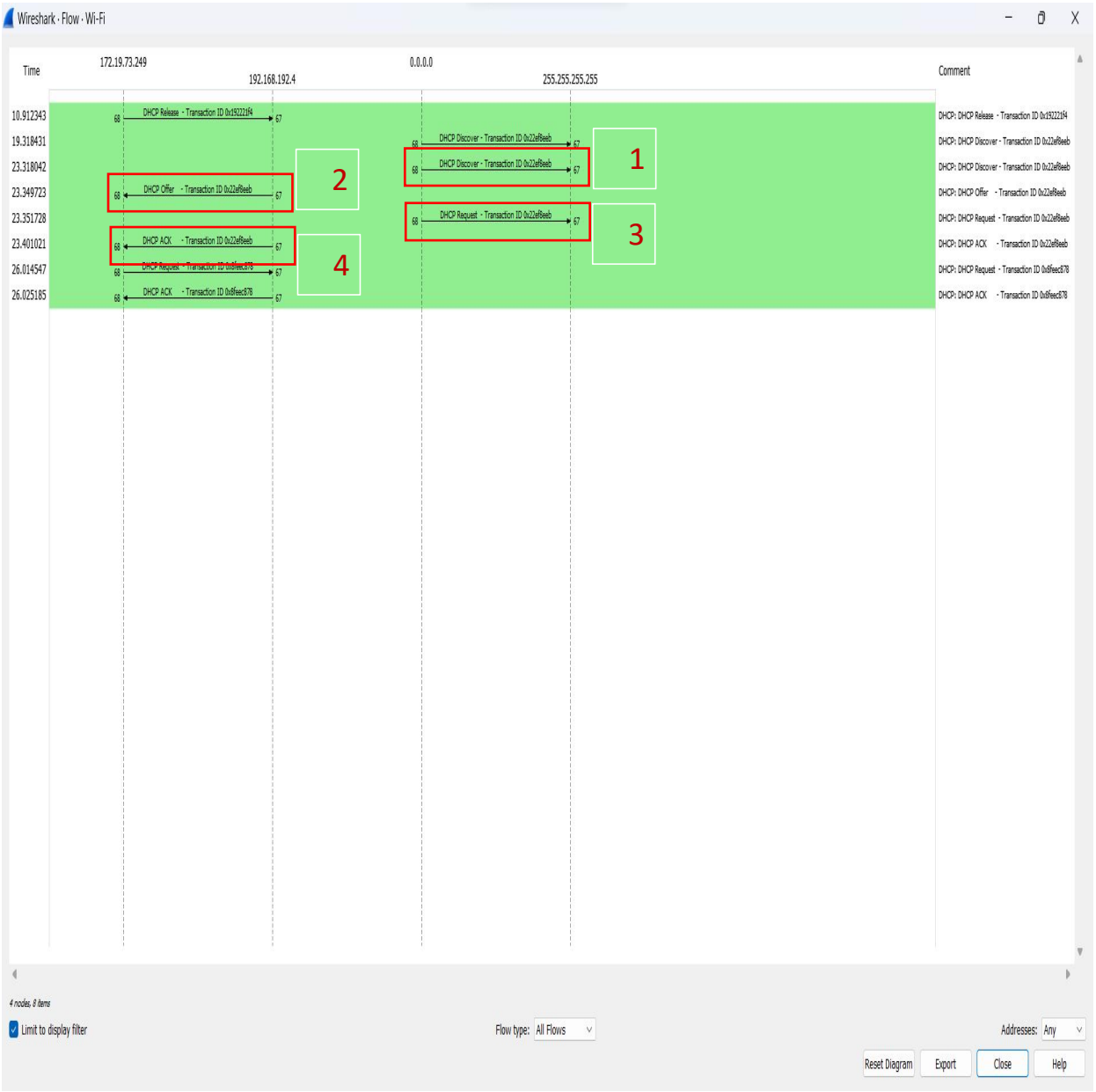

Figure 4: Analysis of DHCP ladder diagram in Wireshark

The ladder diagram analysis of the DHCP protocol using Wireshark provides valuable insights into the Dynamic Host Configuration Protocol's (DHCP) four-step process known as DORA (Discover(1), Offer(2), Request(3), Acknowledge(4)). By examining the sequence of DHCP messages exchanged between clients and servers, we can visualize the flow of communication and gain a comprehensive understanding of the DORA process.