**Dynamic Host Configuration Protocol (DHCP)**

|  |  |
| --- | --- |
| Prepared by | Ayushi Pradhan |
| Reviewed by | V.Mamatha |

DHCP runs at the application layer of the TCP/IP protocol stack.

It dynamically assigns IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol which uses UDP services. DHCP cannot use TCP as the transport protocol because TCP requires both endpoints to have unique IP addresses. At the time a host is required to use DHCP, it does not have an IP address it can source the packets from, nor does it have the IP address of the DHCP server. So, it uses 0.0.0.0 as the source IP address and 255.255.255.255 (broadcast) as the destination IP address (this is for DHCP - similar behavior is present for DHCPv6). These IP addresses are not valid host IP addresses and can be used by multiple clients at any time. So, a TCP connection would not be "unique" for lack of a better term.

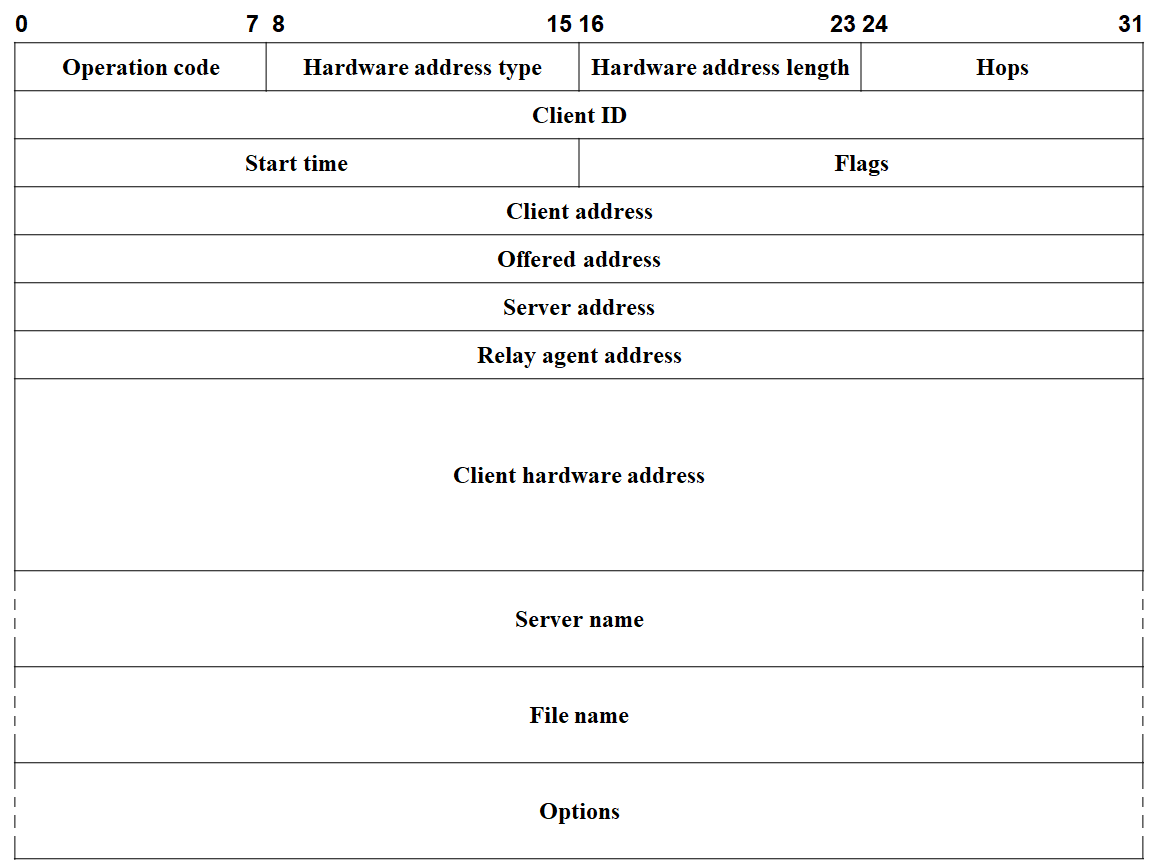
IP addresses are assigned from a pool of addresses. In DHCP, client and server exchanges 4 DHCP messages to make connection called DORA process.

There are 8 messages in DHCP.

**COMPONENTS OF DHCP**

* **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router.
* **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server.
* **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients.
* **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
* **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
* **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

**DHCP HEADER**



**Operation Code (1)**

* It specifies type of DHCP message.
* If the bit is 1, the client(request) sends messages.
* If the bit is 0, messages are sent by the server(reply).

**Hardware type (8)**

* It specifies the network LAN architecture.
* The value is assigned based on the value used in ARP header.

|  |  |
| --- | --- |
| **Hardware Type (HTYPE)** | **Value** |
| Ethernet | 1 |
| IEEE 102 Networks | 6 |
| ARCNET | 7 |
| Frame Relay | 15 |
| Asynchronous Transfer Mode (ATM) | 2 |
| HDLC | 17 |
| Fiber Channel | 18 |
| Asynchronous Transfer Mode (ATM) | 19 |
| Serial Line | 20 |

**Hardware address length (1)**

* It specifies number of bytes used to hold the MAC address.
* It is usually 6.

**Transaction identifier (4)**

* It is used by the clients to match the responses from the servers with previously transmitted requests.
* Random number generated by the client.

**Seconds (2)**

* It tells the elapsed time since the client has begun DHCP process.

**Flags (2)**

* *Broadcast* (1 bit)

A client that does not know its own IP address at that time it sends its request sets this flag as 1. This flag serves as an immediate indicator to the DHCP server or relay agent that receives the request that it should send its reply to broadcast.

* *Reserved* (15 bits)

It is set to zero and not used.

**Client IP address (4)**

* It is set by the client when the client has confirmed that IP address is valid.
* The client puts its own current IP address in this field if and only if it has a valid IP address while in the BOUND, RENEWING or REBINDING states.
* It is set ‘0.0.0.0’ at initial IP configuration.

**Your IP address (4)**

* It is set by the server.
* It is to inform the client about its IP address.

**Server IP address (4)**

* It is the address of the server, from which the client obtained configuration parameters.

**Gateway IP address (4)**

* It specifies the IP address of the first relay agent a request message traveled.
* This field is filled by DHCP relay agent.
* It is set to ‘0.0.0.0’ if the server and client are in the same network.

**Client hardware address (16)**

* It specifies the hardware address of the client, and this can be used by DHCP server to provide same IP address each time client requests.

**Server name (64)**

* It specifies the server host name, from which the client obtained configuration parameters.

**Boot file name (128)**

* It specifies boot file name and path information, defined by the server to the client.

**Options**

* + - *Message type* (1)
      * It indicates the message type.

|  |  |
| --- | --- |
| **Message type** | **Type** |
| Discover | 1 |
| Offer | 2 |
| Request | 3 |
| Decline | 4 |
| Acknowledgement | 5 |
| Negative acknowledgement | 6 |
| Release | 7 |
| Inform | 8 |

* + - *Client identifier*
      * It contains the MAC address of client.
    - *Server identifier* (4)
      * It contains the IP address of server.
    - *Requested IP address* (4)
      * It contains the IP address offered to client.
    - *IP address lease time* (4)
      * It contains the time till the IP address can be used by the client.
    - *Renewal time* (4)
      * Tells the client the value to use for its renewal timer.
    - *Rebinding timer* (4)
      * Tells the client the value to use for its renewal timer.

**TYPES OF MESSAGES**

**DHCP DISCOVER**

This is a first message generated in the communication process between server and client. This message is generated by Client host to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.

**DHCP OFFER**

The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network, then client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet to identify the server.

**DHCP REQUEST**

When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address. A Client ID is also added in this message.

**DHCP ACK**

In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

**DHCP NEGATIVE ACKNOWLEDGEMENT (NAK)**

Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it sends DHCP NAK message to client.

For example, when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

**DHCP DECLINE**

If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

**DHCP RELEASE**

A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

**DHCP INFORM**

If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

**WORKING OF DHCP**

**DORA PROCESS**



**DISCOVER MESSAGE**

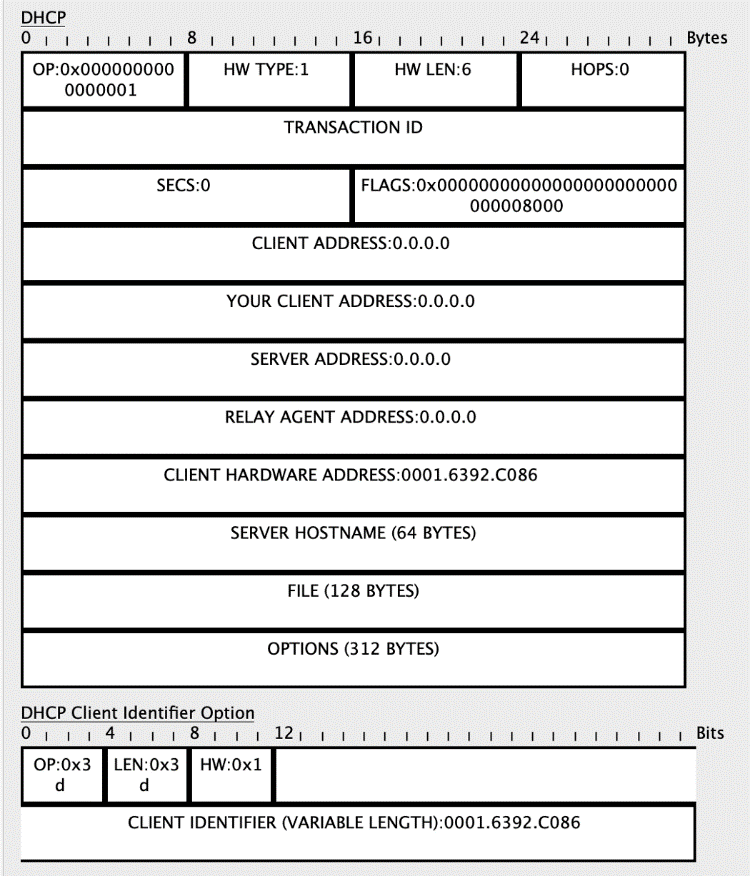
This is the first message in the DORA process which helps in finding the DHCP server of the network. DHCP client will find the server by sending DHCP discover message. The broadcast message is sent to the network. As the DHCP client does not know the IP address of the server so the message is broadcast with a destination IP is 255.255.255.255. And the source IP will be 0.0.0.0 as the client does not have any IP address. Here the DHCP discover message in the data link layer and network layer is always broadcast.

Source IP address: 0.0.0.0

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP clients

Destination MAC address: FF: FF:FF:FF:FF:FF



**DHCP OFFER**

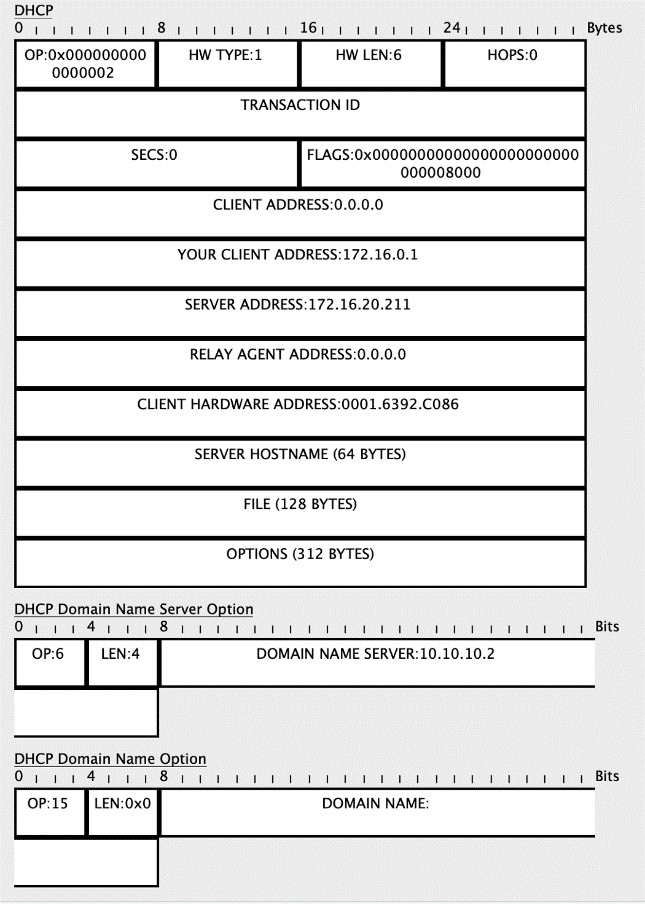
DHCP server receives the discover message and it replays the DHCP client with the DHCP offer request. The server sends a DHCP offer message with filled information. It has information about the IP address and duration of time that a host can use. Here destination IP address will be 255.255.255.255 as the DHCP client still does not have its IP address. But this DHCP offer message is broadcast in the network layer and unicast in the data link layer.

Source IP address: IP Address of DHCP Server

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP Server

Destination MAC address: FF:FF:FF:FF:FF:FF



**DHCP REQUEST**

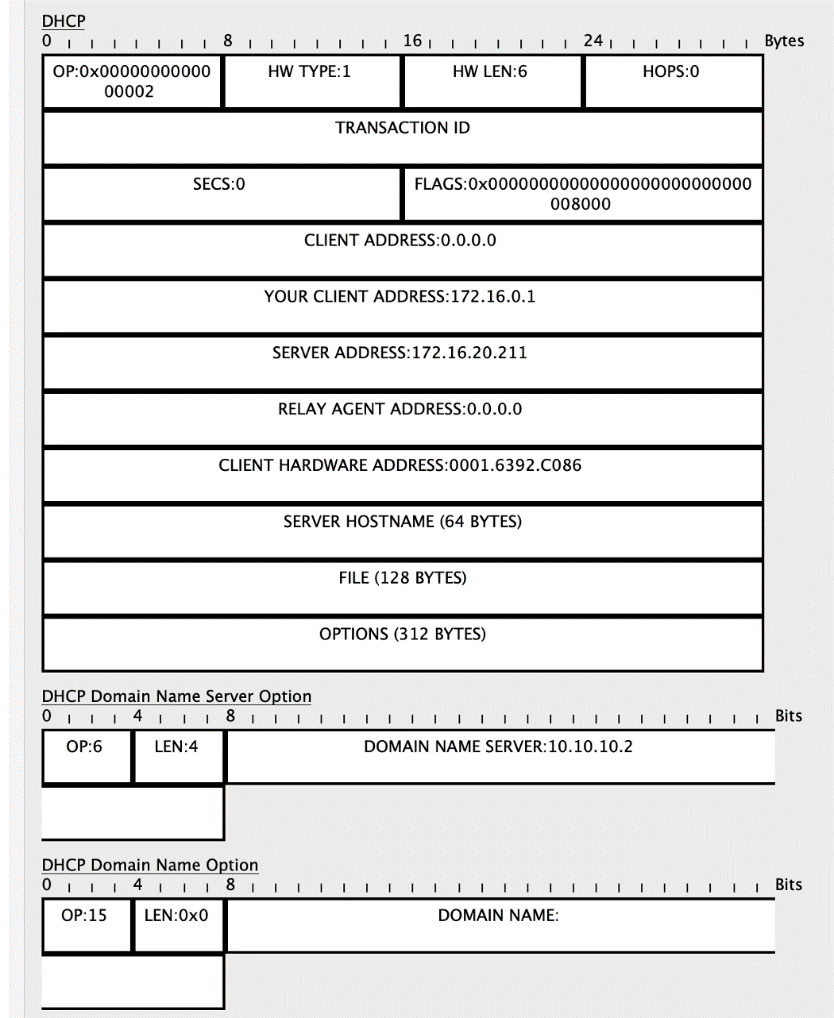
DHCP clients send the request message to the server when it receives a DHCP offer message from the server. This message tells the server that it accepts the IP address given by the server. Here destination address will be 255.255.255.255 means its again broadcast. The reason for this is there might be many DHCP servers in the network so the client may receive multiple offer messages and it will accept the request that reaches him first and send a broadcast message to eliminate other DHCP servers. Here source IP address will be 0.0.0.0 as the DHCP server has not yet assigned an IP address to the client. DHCP Request Message is also a broadcast message.

Source IP address: 0.0.0.0

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP clients

Destination MAC address: FF:FF:FF:FF:FF:FF



The fields found in DHCP Request are like DHCP Discover. The Options is set to 0x 35 01 03.

**DHCP ACKNOWLEDGEMENT**

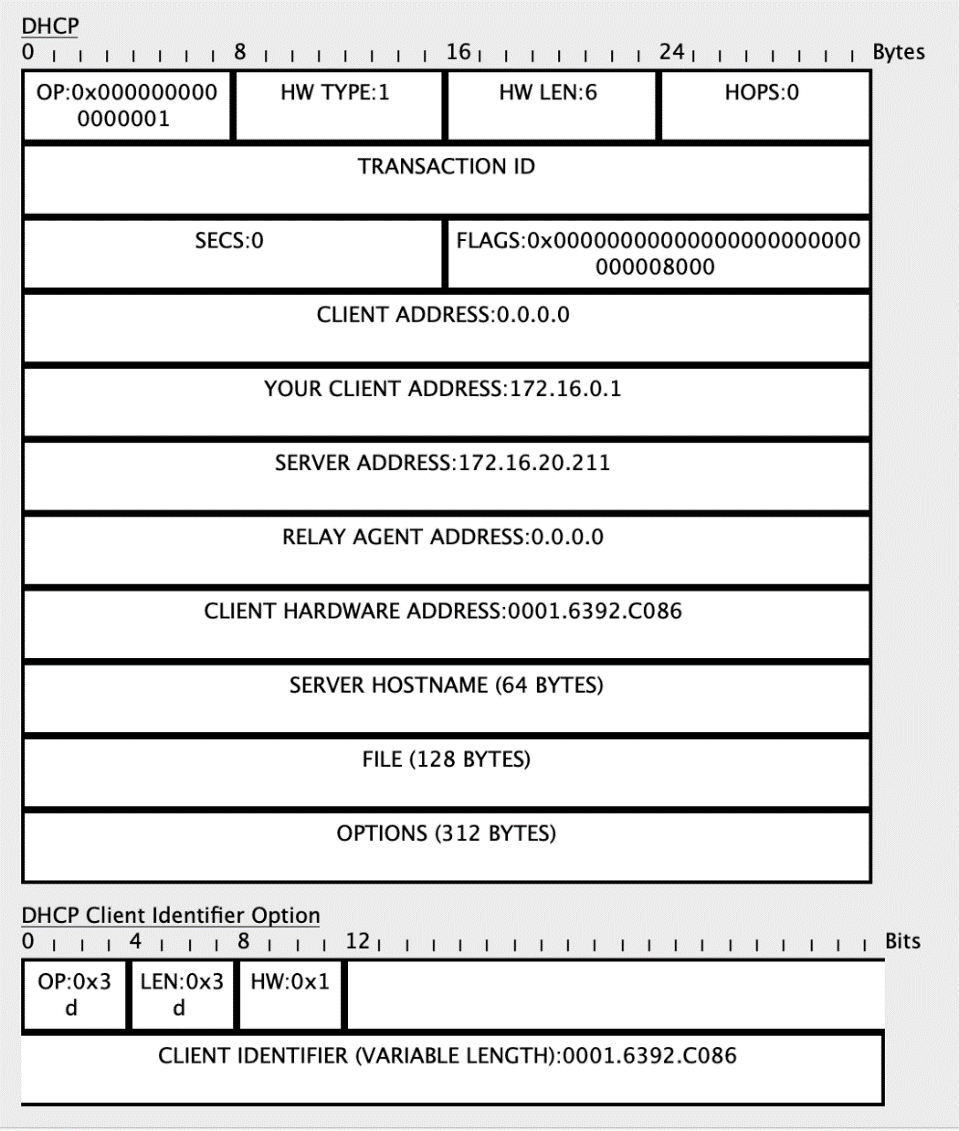
This is the last step or message in the DORA process. The DHCP server sends Acknowledge Message to the client when it receives the request message from the DHCP client. This message will contain the IP address and subnet mask that the server assigns to the client. Source IP address will be the IP address of the server. This will again broadcast message as the destination IP address is 255.255.255.255. But it is unicast in the case of the data link layer.

Source IP address: IP Address of DHCP Server

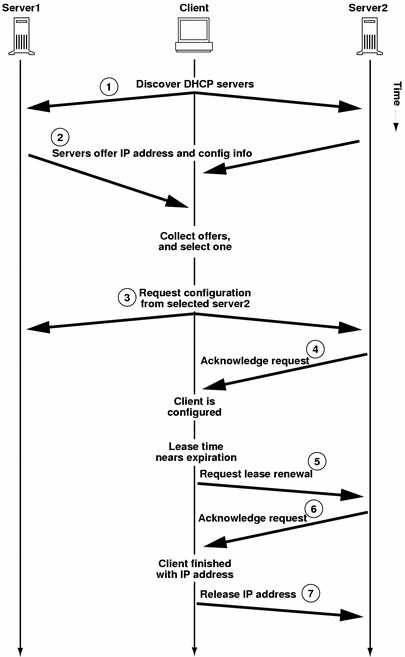
Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP server

Destination MAC address: FF:FF:FF:FF:FF:FF

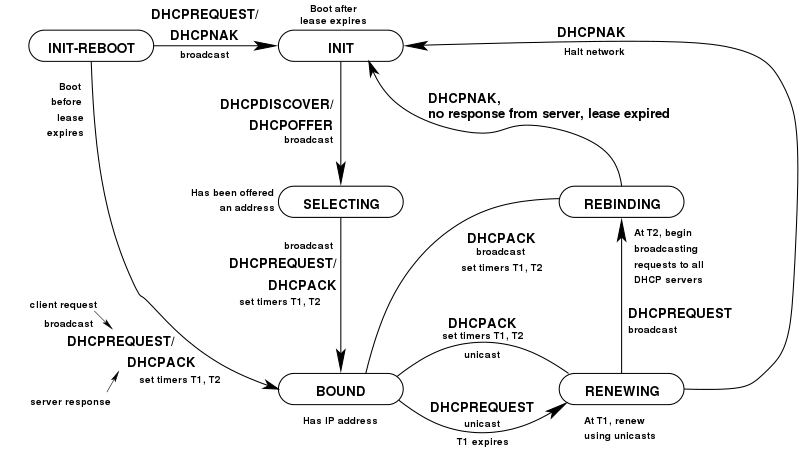


The fields in DHCP ACK are like DHCP Offer; except the Options is set to 0x35 01 05.



Timeline of messages between DHCP server and client when allocating a new IP address

**DHCP STATE DIAGRAM**



**INIT** State: When the DHCP client first starts, it is in the INIT state (initializing state). The client broadcasts a DHCPDISCOVER message (a request message with the DHCPDISCOVER option), using port 67.

**SELECTING** State: After sending the DHCPDISCOVER message, the client goes to the selecting state. Those servers that can provide this type of service respond with a DHCPOFFER message. In these messages, the servers offer an IP address. They can also offer the lease duration. The default is 1 hour. The server that sends a DHCPOFFER locks the offered IP address so that it is not available to any other clients. The client chooses one of the offers and sends a DHCPREQUEST message to the selected server. It then goes to the requesting state. However, if the client receives no DHCPOFFER message, it tries four more times, each with a span of 2 seconds. If there is no reply to any of these DHCPDISCOVERs, the client sleeps for 5 minutes before trying again.

**REQUESTING** State: The client remains in the requesting state until it receives a DHCPACK message from the server that creates the binding between the client physical address and its IP address. After receipt of the DHCPACK, the client goes to the bound state.

**BOUND** State: In this state, the client can use the IP address until the lease expires. When 50 percent of the lease period is reached, the client sends another DHCPREQUEST to ask for renewal. It then goes to the renewing state. When in the bound state, the client can also cancel the lease and go to the initializing state.

**RENEWING** State: The client remains in the renewing state until one of two events happens. It can receive a DHCPACK, which renews the lease agreement. In this case, the client resets its timer and goes back to the bound state. Or, if a DHCPACK is not received, and 87.5 percent of the lease time expires, the client goes to the rebinding state.

**REBINDING** State: The client remains in the rebinding state until one of three events happens. If the client receives a DHCPNACK or the lease expires, it goes back to the initializing state and tries to get another IP address. If the client receives a DHCPACK, it goes to the bound state and resets the timer.

**DHCP LEASE RENEWAL / REBINDING PROCESS**

Once a DHCP client completes the allocation or reallocation process, it enters the BOUND state. The client is now in its regular operating mode, with a valid IP address and other configuration parameters it received from the DHCP server and can be used like any regular TCP/IP host.

While the client is in the BOUND state, DHCP lies dormant. If the client stays on and functioning normally, no real DHCP activity will occur while in this state. The most common occurrence that causes DHCP to “wake up” and come active again is arrival of the time when the lease is to be renewed. Renewal ensures that a lease is perpetuated so it can be used for a prolonged period and involves its own message exchange procedure. (The other way that a client can leave the BOUND state is when it terminates the lease early.)

If DHCP's automatic allocation is used, or if dynamic allocation is used with an infinite lease period, the client's lease will never expire, so it never needs to be renewed. Short of early termination, the device will remain in the BOUND state forever, or at least until it is rebooted. However, as we have already discussed, most leases are finite in nature. A client must take action to ensure that its lease is extended, and normal operation continues.

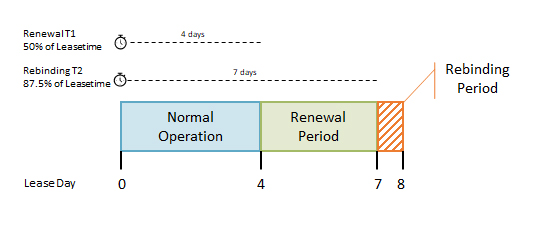
To manage the lease extension process, two timers are set at the time that a lease is allocated. The renewal timer (T1) goes off to tell the client it is time to try to renew the lease with the server that initially granted it. The rebinding timer (T2) goes off if the client is not successful in renewing with that server and tells it to try any server to have the lease extended. If the lease is renewed or rebound, the client goes back to normal operation. If it cannot be rebound, it will expire, and the client will need to seek a new lease.

**TYPES OF TIMERS**

**Renewal timer (T1)**

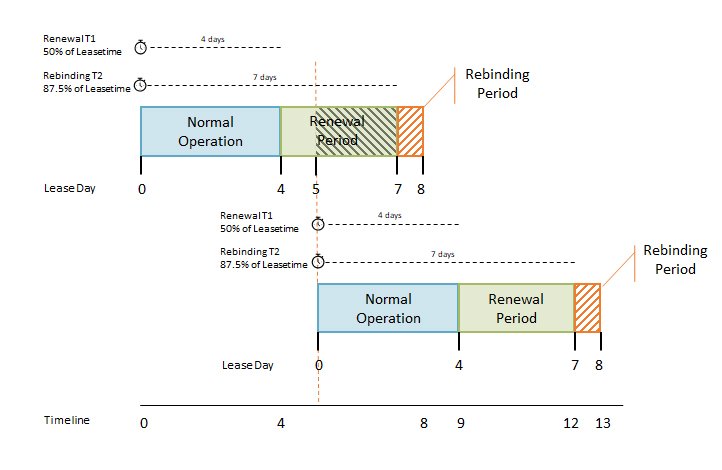
After certain portion of lease time has expired, you attempt to contact the server that initially granted the lease time to renew the lease, so its IP address still be in use.

It is the 50% of the lease time.

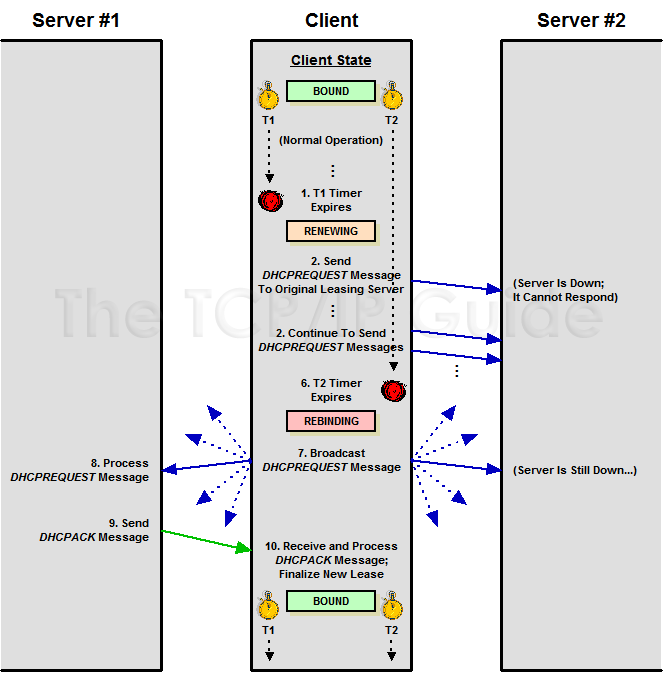


**Rebinding timer (T2)**

If the client is not successful in renewing with that server and tells it to try any server to have lease extended.



**LEASE RENEWAL AND REBINDING PROCESS**



1. **Renewal Timer (T1) Expires**

* The renewal timer, T1, is set by default to 50% of the length of the lease. When the timer goes off, the client transitions from the BOUND state to the RENEWING state.
* Note that a client may initiate lease renewal prior to T1 timer expiration if it desires.

1. **Client Sends DHCPREQUEST Renewal Message**

The client creates a DHCPREQUEST message that identifies itself and its lease. It then transmits the message directly to the server that initially granted the lease, unicast. Note that this is different from the DHCPREQUEST messages used in the allocation/reallocation processes, where the DHCPREQUEST is broadcast. The client may request a particular new lease length, just as it may request a lease length in its requests during allocation, but as always, the server makes the final call on lease length.

1. **Server Receives and Processes DHCPREQUEST Message and Creates Reply**

* Assuming the server is reachable, it will receive and process the client's renewal request.
* There are two possible responses:
  + Server Agrees to Renew Client Lease: The server decides that the client's lease can be renewed. It prepares to send to the client a DHCPACK message to confirm the lease's renewal, indicating the new lease length and any parameters that may have changed since the lease was created or last renewed.
  + Server Refuses to Renew Client Lease: The server decides for whatever reason not to renew the client's lease. It will create a DHCPNAK message.

1. **Server Sends Reply**

* The server sends the DHCPACK or DHCPNAK message back to the client.

1. **Client Receives and Processes Server Reply**

* The client takes the appropriate action in response to the server's reply:
* Positive Acknowledgment:
  + The client receives a DHCPACK message, renewing the lease.
  + The client makes note of the new lease expiration time and any changed parameters sent by the server, resets the T1 and T2 timers, and transitions back to the BOUND state.
* Negative Acknowledgment:
  + The message is a DHCPNAK, which tells the client that its lease renewal request has been denied.
  + The client will immediately transition to the INIT state to get a new lease—step #1 in the allocation process.

1. **Rebinding Timer (T2) Expires**

* If the client receives no reply from the server, it will remain in the RENEWING state, and will regularly retransmit the unicast DHCPREQUEST to the server.
* During this period, the client is still operating normally, from the perspective of its user.
* If no response from the server is received, eventually the rebinding timer (T2) expires.
* This will cause the client to transition to the REBINDING state. Recall that by default, the T2 timer is set to 87.5% (7/8ths) of the length of the lease.

1. **Client Sends DHCPREQUEST Rebinding Message**

* Having received no response from the server that initially granted the lease, the client “gives up” on that server and tries to contact any server that may be able to extend its existing lease.
* It creates a DHCPREQUEST message and puts its IP address in the CIAddr field, indicating clearly that it presently owns that address. It then broadcasts the request on the local network.

1. **Servers Receives and Processes DHCPREQUEST Message and Send Reply**

* Each server receives the request, and responds according to the information it has for the client (a server that has no information about the lease or may have outdated information does not respond):
* Server Agrees to Rebind Client Lease:

A server has information about the client's lease and agrees to extend it. It prepares for the client a DHCPACK message to confirm the lease's renewal, indicating any parameters that may have changed since the lease was created or last renewed.

* Server Decides Client Cannot Extend Its Current Lease:

A server determines that for whatever reason, this client's lease should not be extended. It gets ready to send back to the client a DHCPNAK message.

1. **Server Sends Reply**

* Each server that is responding to the client sends its DHCPACK or DHCPNAK message.

1. **Client Receives Server Reply**

* The client takes the appropriate action in response to the two possibilities in the preceding step:
  + Positive Acknowledgment:

The client receives a DHCPACK message, rebinding the lease. The client makes note of the server that is now in charge of this lease, the new lease expiration time, and any changed parameters sent by the server. It resets the T1 and T2 timers, and transitions back to the BOUND state

* + Negative Acknowledgment:

The message is a DHCPNAK, which tells the client that some server has determined that the lease should not be extended. The client immediately transitions to the INIT state to get a new lease—step #1 in the allocation process.

1. **Lease Expires**

If the client receives no response to its broadcast rebinding request, it will, as in the RENEWING state, retransmit the request regularly. If no response is received by the time the lease expires, it transitions to the INIT state to get a new lease.