

DHCP Header (RFC 2131)



Notes:

Op – the message type (see DHCP message types table below)

Htype – Hardware address type (see HTYPE codes table below)

Hlen – Hardware address length

Hops – set to zero by a client – but can optionally be used when booting via a relay agent

Xid – Transaction ID, a random number chosen by the client, used by the client and server so that no-one get confused between messages.

Secs – The number in seconds since the address was allocated, the client fills this part

Flags – Exactly what it says on the tin

Ciaddr – The clients IP address, but only if they have one, basically if the client is BOUND, RENEW or REBINDING.

Yiaddr – Your (client) IP address.

Siaddr – IP address of the next server to use in bootstrap. Is returned in DHCP OFFER and DHCP ACK messages by the DHCP server.

Giaddr – VPN server IP address used in booting via relay agents

Chaddr – Client Hardware address (should be unique – LOL)

Sname – Optional server host name, should be a null terminated string

File – Boot file name, it should be a null terminated string. For DHCP DISCOVER messages it should be a fully generic name or null, for DHCP OFFER messages it should be a fully qualified directory path name.

Options – For optional parameters.

DHCP Message Type (OP codes)

Message	Description	Code??
Discover	A broadcast from a client to recognise server.	
Offer	A response from a server with a proposal of parameters.	Op code 2 - BOOTREPLY
Request	A client broadcasts to a preferred server, declining all others.	Op code 1 - BOOTREQUEST
Ack	The server assigns an IP address.	
Nak	The server rejects the clients request.	
Decline	The client found a problem with the assigned address.	
Release	The client returns the assigned IP address before the lease expires.	

Format of the Flags field

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
B	Must Be Zero'd														

B = Broadcast

The rest of the byte must be zero'd this is for future use.

Hardware Address type codes HTYPE codes

Code	Definition
1	Ethernet (10Mb)
2	Experimental Ethernet (3Mb)
3	Amateur Radio AX.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)