Dynamic Host Configuration Protocol

Classical Internet Applications - Midterm Research

Ahmed Nouralla
Security and Network Engineering Lab
Innopolis University

November 26, 2024

Overview

1. Introduction

- Dynamic Host Configuration Protocol (DHCP) provides a framework for hosts joining a network to automatically obtain configuration information essential for further communications.

- Such information includes: 1. The host's identity (e.g., IP address with subnet mask) and 2. Addresses of other key nodes (e.g., network gateway, name server, time server, etc.).

2. History

- **RFC 951 (1985)** defined the bootstrap protocol (BOOTP) for static IP assignment to clients based on their MAC address.
- **RFC 1531 (1993)** introduced DHCP as an extension to BOOTP for automatic IP address assignment. RFC 1541 (1993) replaced it with clearer specifications.
- **RFC 2131 (1997)** standardized DHCPv4, defining the DHCP message format and operation procedures. **It remains the primary DHCPv4 standard**.

Note

Multiple RFCs were published later introducing extensions, enhancements, security patches, and support for IPv6.

3. Terminology

Essential terminology as defined in RFC 2131

- **DHCP client**: host using DHCP to obtain configuration parameters
- **DHCP server**: host providing the configuration parameters to clients
- **Relay agent**: host/router forwarding DHCP messages between server and client
- **Binding**: the configuration parameters (i.e., at least the IP address to be bound to the client).

4. Use case

The most common use-case of DHCP (also known as the DORA process) involves four message exchanges.

- **Discover**: client probing DHCP servers
- **Offer**: server proposing an address
- **Request**: client asking to get a certain address
- **ACK**: server acknowledging the assignment

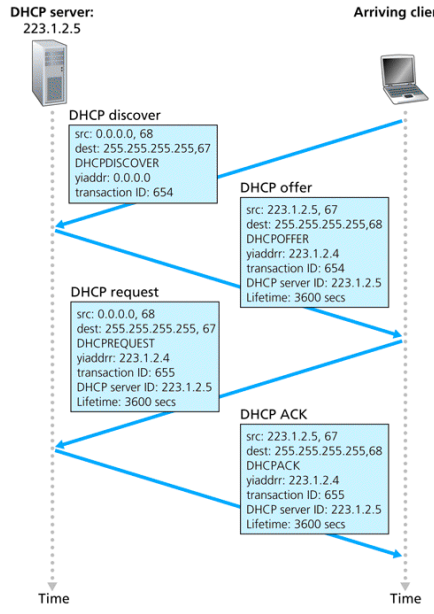
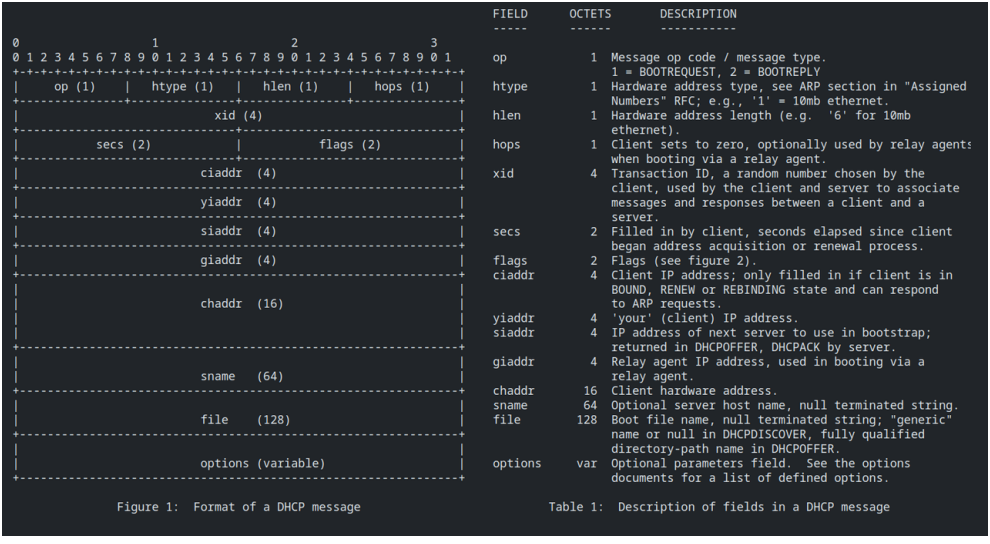


Figure: The DORA process in DHCP

5. Architecture

- DHCP uses a client server architecture as illustrated.
- A DHCP server is always listening on port 67/UDP for client messages.
- Currently, 18 OP codes (1-18) are in use to specify different types of DHCP messages, with over 80 options and extensions for communicating different types of information.



```
                                                    FIELD      OCTETS       DESCRIPTION
                                                    -----      ------       -----------
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1     op           1  Message op code / message type.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                  1 = BOOTREQUEST, 2 = BOOTREPLY
|     op (1)    |   htype (1)   |   hlen (1)    |   hops (1)    |     htype        1  Hardware address type, see ARP section in "Assigned
+---------------+---------------+---------------+---------------+                  Numbers" RFC; e.g., '1' = 10mb ethernet.
|                            xid (4)                            |     hlen         1  Hardware address length (e.g.  '6' for 10mb
+-------------------------------+-------------------------------+                  ethernet).
|           secs (2)            |           flags (2)           |     hops         1  Client sets to zero, optionally used by relay agents
+-------------------------------+-------------------------------+                  when booting via a relay agent.
|                          ciaddr  (4)                          |     xid          4  Transaction ID, a random number chosen by the
+---------------------------------------------------------------+                  client, used by the client and server to associate
|                          yiaddr  (4)                          |                  messages and responses between a client and a
+---------------------------------------------------------------+                  server.
|                          siaddr  (4)                          |     secs         2  Filled in by client, seconds elapsed since client
+---------------------------------------------------------------+                  began address acquisition or renewal process.
|                          giaddr  (4)                          |     flags        2  Flags (see figure 2).
+---------------------------------------------------------------+     ciaddr      4  Client IP address; only filled in if client is in
|                                                               |                  BOUND, RENEW or REBINDING state and can respond
|                          chaddr  (16)                         |                  to ARP requests.
|                                                               |     yiaddr       4  'your' (client) IP address.
|                                                               |     siaddr       4  IP address of next server to use in bootstrap;
+---------------------------------------------------------------+                  returned in DHCPOFFER, DHCPACK by server.
|                                                               |     giaddr       4  Relay agent IP address, used in booting via a
|                          sname   (64)                         |                  relay agent.
+---------------------------------------------------------------+     chaddr      16  Client hardware address.
|                                                               |     sname        64  Optional server host name, null terminated string.
|                          file    (128)                        |     file        128  Boot file name, null terminated string; "generic"
+---------------------------------------------------------------+                  name or null in DHCPDISCOVER, fully qualified
|                                                               |                  directory-path name in DHCPOFFER.
|                          options (variable)                   |     options     var  Optional parameters field.  See the options
+---------------------------------------------------------------+                  documents for a list of defined options.

            Figure 1:  Format of a DHCP message                             Table 1:  Description of fields in a DHCP message
```

Figure: DHCP message format as defined in RFC2131

DHCP message types

Code	Name	Length	RFC
1	DHCPDISCOVER	1 octet	rfc2132[14]: Section 9.6
2	DHCPOFFER	1 octet	rfc2132[14]: Section 9.6
3	DHCPREQUEST	1 octet	rfc2132[14]: Section 9.6
4	DHCPDECLINE	1 octet	rfc2132[14]: Section 9.6
5	DHCPACK	1 octet	rfc2132[14]: Section 9.6
6	DHCPNAK	1 octet	rfc2132[14]: Section 9.6
7	DHCPRELEASE	1 octet	rfc2132[14]: Section 9.6
8	DHCPINFORM	1 octet	rfc2132[14]: Section 9.6
9	DHCPFORCERENEW	1 octet	rfc3203[15]: Section 4
10	DHCPLEASEQUERY	1 octet	rfc4388[16]: Section 6.1
11	DHCPLEASEUNASSIGNED	1 octet	rfc4388[16]: Section 6.1
12	DHCPLEASEUNKNOWN	1 octet	rfc4388[16]: Section 6.1
13	DHCPLEASEACTIVE	1 octet	rfc4388[16]: Section 6.1
14	DHCPBULKLEASEQUERY	1 octet	rfc6926[17]: Section 6.2.1
15	DHCPLEASEQUERYDONE	1 octet	rfc6926[17]: Section 6.2.1
16	DHCPACTIVELEASEQUERY	1 octet	rfc7724[18]: Section 5.2.1
17	DHCPLEASEQUERYSTATUS	1 octet	rfc7724[18]: Section 5.2.1
18	DHCPTLS	1 octet	rfc7724[18]: Section 5.2.1

RFC 1497 (BOOTP Vendor Information Extensions) vendor extensions[14]:Section 3

Code	Name	Length	Notes
0	Pad	0 octets	Can be used to pad other options so that they are aligned to the word boundary; is not followed by length byte
1	Subnet mask	4 octets	Client's subnet mask as per RFC 950. If both the subnet mask and the router option (option 3) are included, the subnet mask option must be first.
2	Time offset	4 octets	Offset of the client's subnet in seconds from Coordinated Universal Time (UTC). The offset is expressed as a two's complement 32-bit integer. A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian.
3	Router	Multiples of 4 octets	Available routers, should be listed in order of preference
4	Time server	Multiples of 4 octets	Available Time Protocol servers to synchronise with, should be listed in order of preference
5	Name server	Multiples of 4 octets	Available IEN 116 name servers, should be listed in order of preference
6	Domain name server	Multiples of 4 octets	Available DNS servers, should be listed in order of preference
7	Log server	Multiples of 4 octets	Available log servers, should be listed in order of preference

Figure: DHCP message types and common options

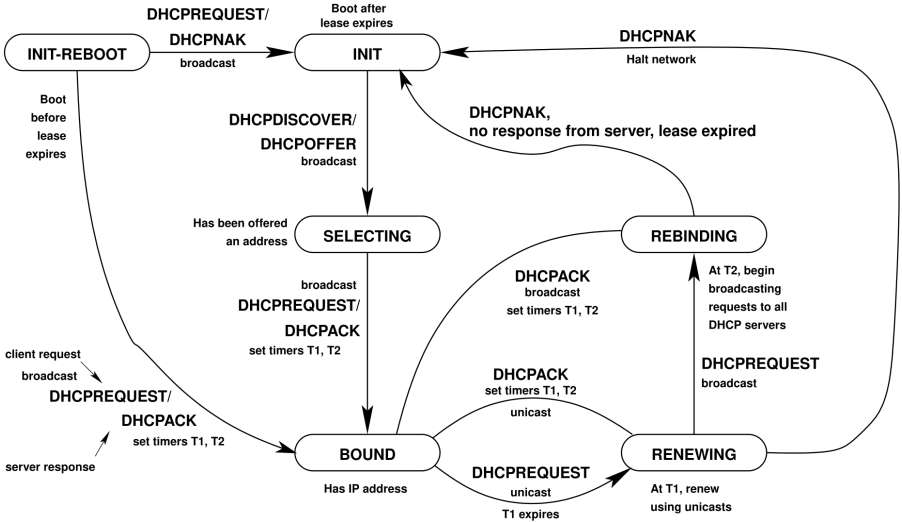


Figure: DHCP client state transition diagram. Adapted from RFC 2131 Fig 5.

6. Configuration Management

A DHCP server can be configured to allocate addresses using one of three allocation strategies:

- **Dynamic**: providing addresses from a pool with leases (expiration) time.
- **Automatic**: permanent address assignment, unless voluntarily released.
- **Manual**: static IP/MAC binding table maintained by the administrator.

7. Security issue

- Rogue DHCP is a Man-In-The-Middle attack where a malicious host on the same subnet as the DHCP client deceives them by acting as the DHCP server
- It does so by replying to DHCPDISCOVER, offering it's own IP address as the default gateway.
- Once carried out, it allows the attacker to intercept all requests sent by the victim.
- A common mitigation strategy (DHCP snooping) involves dropping DHCP messages that did not come from the trusted switchport (the one connected to the real DHCP server).

8. Tools and implementations

- DHCP server functionality can be implemented in routers, and in Linux hosts.
- Popular server implementations include dnsmasq and ISC DHCP server (superseded by Kea)
- A thin client (e.g., dhcpcd or dhclient) is needed for communication with the server.

9. Practical Demonstration

A quick demo showing the minimal set of commands to configure a working DHCP server on Cisco IOS. The scenario is simulated in GNS3 and the results are inspected in Wireshark.

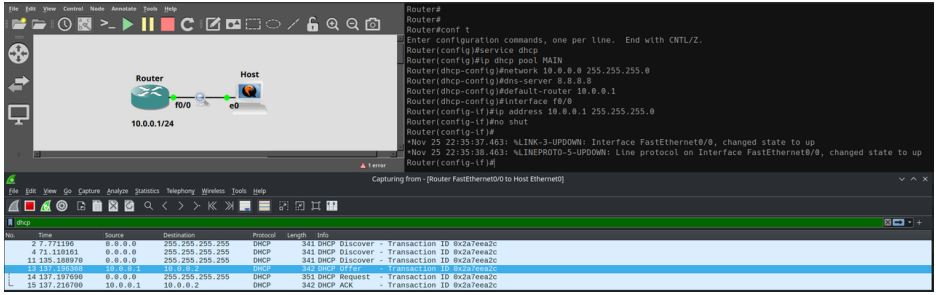


Figure: Demo with Cisco IOS, GNS3, and Wireshark

References

Ralph Droms (1997)
Dynamic Host Configuration Protocol
RFC 2131. Available: https://doi.org/10.17487/RFC2131

Kurose, James F. and Ross, Keith W. (2012)
Computer Networking: A Top-Down Approach (6th Edition)
Available: https://doi.org/10.5555/258450

Cisco Documentation
Configuring the Cisco IOS DHCP Server
Available:
https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html