

Submitted to DHC Working Group  
INTERNET DRAFT  
<[draft-ietf-dhc-pv4-reconfigure-00.txt](#)>

Peter De Schrijver  
Yves T'Joens  
Christian Hublet  
Alcatel

March 2000  
Expires September 2000

## **Dynamic host configuration : DHCP reconfigure extension**

### Status of this memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``work in progress.''

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

### Abstract

This draft defines extensions to DHCP [[DHCP](#)] to allow dynamic reconfiguration of a single host triggered by the DHCP server (eg. a new IP address). This is achieved by introducing a unicast DHCP FORCERENEW message which forces the client to the RENEW state.

## **1. Introduction**

The procedures as described within this draft allow the dynamic reconfiguration of individual hosts.

## **1.1 Conventions**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

## **2. DHCP force renew**

This section describes the DHCP force renew extension.

### **2.1 Terminology**

DHCP client : host to be reconfigured using DHCP.

DHCP server : server which configured the DHCP client.

### **2.2 Force renew procedures**

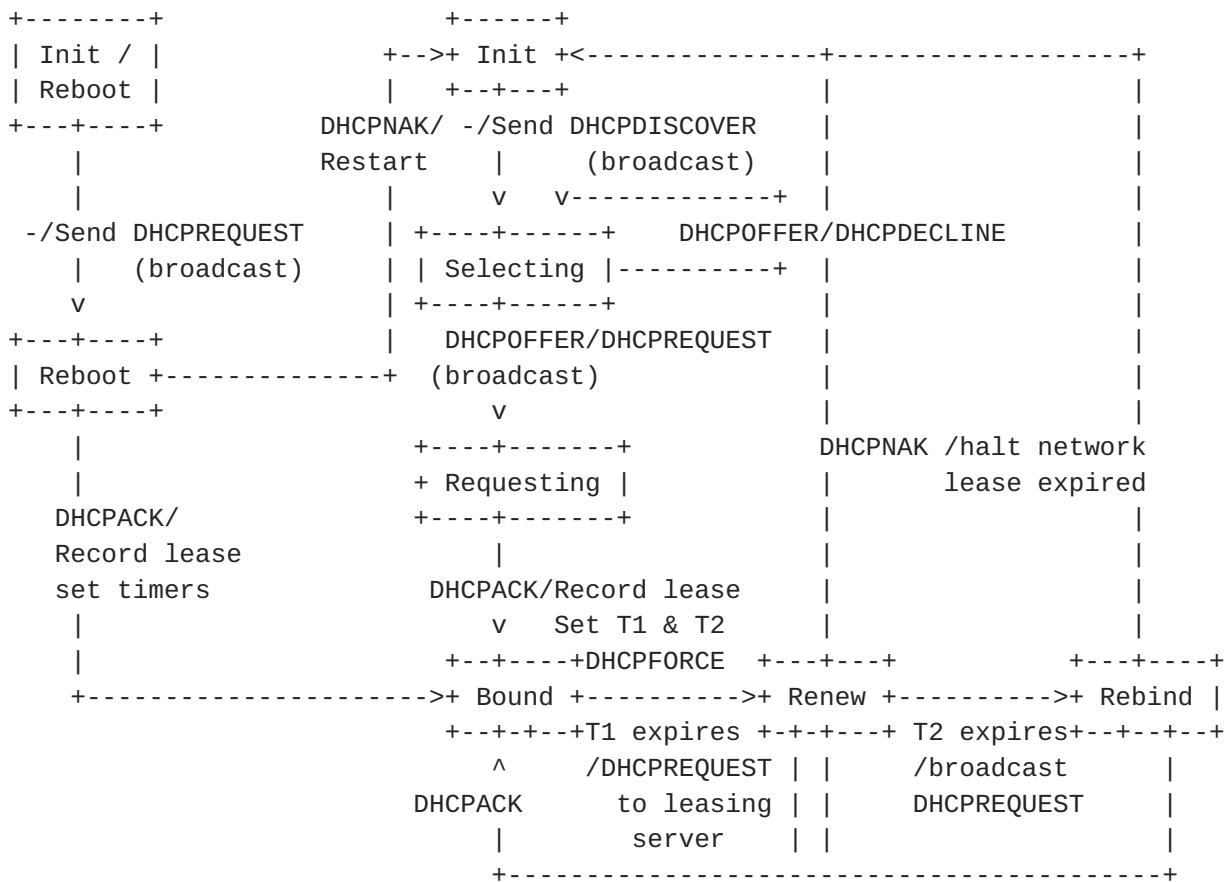
The DHCP server sends a force renew message to the client. The client will change its state to the RENEW state. The client will then try to renew its lease according to normal DHCP procedures. If the server wants to assign a new IP address to the client, it will reply to the DHCP REQUEST with a DHCP NAK. The client will then go back to the init state and broadcast a DHCP DISCOVER message. The server can now assign a new IP address to the client by replying with a DHCP OFFER. If the force renew message is lost, the DHCP server will not receive a DHCP REQUEST from the client and it should retransmit the DHCP FORCERENEW message using an exponential backoff algorithm. Depending on the bandwidth of the network between server and client, the server should choose a delay. This delay grows exponentially as retransmissions fail. The amount of retransmissions should be limited.

### **2.3 Rationale**

This approach has a number of advantages. It does not require new states to be added to the DHCP client implementation. This minimizes the amount of code to be changed. It also allows lease RENEWAL to be driven by the server, which can be used to optimize network usage or DHCP server load.

## **3. Extended DHCP state diagram**





#### 4. Message layout

Field	DHCPFORCERENEW
-----	-----
'op'	BOOTREPLY
'htype'	(From "Assigned Numbers" RFC)
'hlen'	(Hardware address length in octets)
'hops'	0
'xid'	selected by server
'secs'	0
'ciaddr'	0
'yiaddr'	0
'siaddr'	0
'flags'	0
'giaddr'	0
'chaddr'	client's hardware address
'sname'	0
'file'	0
'options'	options

DHCP option 53 (DHCP message type) is extended with a new value :



DHCPFORCERENEW

## **5. Failover Considerations**

A DHCP server should only send a DHCPFORCERENEW when it's fully aware of the current state of the DHCP client. In practice this means it should only send a DHCPFORCERENEW when in "PARTNER DOWN", "COMMUNICATIONS INTERRUPTED" or "NORMAL" state, and only for DHCP clients of which the state is synchronised.

## **6. IANA Considerations**

A new value for DHCP option 53 (DHCP message type) should be added to indicate a DHCPFORCERENEW message.

## **7. Security Considerations**

Depending on layer 2 characteristics, DHCP force renew can be used to snoop and spoof traffic. To prevent this, the DHCPFORCERENEW message should be authenticated using a shared secret based mechanism as described in [[DHCP-AUTH](#)].

## **8. References**

[DHCP] R.Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[DHCP-AUTH] R. Droms, "Authentication for DHCP Messages", [draft-ietf-dhc-euthentication-12](#), October 1999.

## **9. Contacts**

Peter De Schrijver  
Alcatel Corporate Research Center  
Francis Wellesplein 1, 2018 Antwerp, Belgium  
Phone : +32 3 240 8569  
E-mail : peter.de\_schrijver@alcatel.be

Yves T'joens  
Alcatel Corporate Research Center  
Francis Wellesplein 1, 2018 Antwerp, Belgium  
Phone : +32 3 240 7890  
E-mail : yves.tjoens@alcatel.be

Christian Hublet  
Alcatel Carrier Internetworking Division  
De Villermontstraat 28, 2550 Kontich, Belgium



Phone : +32 3 450 3322

E-mail : Christian.Hublet@alcatel.be