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 with 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 between subnets. This allows a VPN like service to be offered to customers.
The following describes an example configuration and operation to allow the reader both to understand the need and applicability of the DHCP extension.

Assume a dial in host that establishes a connection with its network access provider. Upon network layer configuration, the host gets configured by DHCP with an IP address local to the network access provider. This local IP address allows the host to communicate within the boundary of the (private) IP network operated by the network access provider. The network access provider provides, besides offering local content, VPN services by means of service selection through e.g., a web browser (personalized web page). Upon selecting (clicking) a specific VPN service, the host IP stack needs to be reconfigured with an IP address local to a subnet of the selected VPN.

To that end, some entity within the network access will trigger the host to reconfigure its IP layer, after which, the host is virtually connected to the VPN of choice. The procedures by which the entity obtains the VPN IP address is outside the scope of this document.

Note that these procedures are not limited to dial-in like (point to point) access, but can equally well apply within shared LAN media. The extensions defined within this draft should be clearly distinguished from subnet reconfiguration as it applies to single hosts.

The same host behaviour may be obtained in the following ways, however with some clear drawbacks.

The first alternative is to use a short lease time for the original DHCP request. Depending on the specified lease time, this either introduces unnecessary traffic and DHCP server load due to frequent DHCP REQUEST messages to extend the lease, or lacking interactivity due to the long delays between service selection and service establishment. These problems render this alternative useless in practice.

The second alternative is to specify a different protocol which allows the client to be triggered to release its IP address. Regardless of the installation and maintenance headaches at the client end this would introduce, this would be including DHCP related functionality in another protocol, and goes against the spirit of reusing existing protocols whenever applicable.

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.
"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 should do message retransmission based on the strategy as described in RFC 2131 [DHCP] page 24.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>DHCPFORCERENEW</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>op</code></td>
<td>BOOTREPLY</td>
</tr>
<tr>
<td><code>htype</code></td>
<td>(From &quot;Assigned Numbers&quot; RFC)</td>
</tr>
<tr>
<td><code>hlen</code></td>
<td>(Hardware address length in octets)</td>
</tr>
<tr>
<td><code>hops</code></td>
<td>0</td>
</tr>
<tr>
<td><code>xid</code></td>
<td>selected by server</td>
</tr>
<tr>
<td><code>secs</code></td>
<td>0</td>
</tr>
<tr>
<td><code>ciaddr</code></td>
<td>0</td>
</tr>
<tr>
<td><code>yiaddr</code></td>
<td>0</td>
</tr>
<tr>
<td><code>siaddr</code></td>
<td>0</td>
</tr>
<tr>
<td><code>flags</code></td>
<td>0</td>
</tr>
<tr>
<td><code>giaddr</code></td>
<td>0</td>
</tr>
<tr>
<td><code>chaddr</code></td>
<td>client’s hardware address</td>
</tr>
<tr>
<td><code>sname</code></td>
<td>0</td>
</tr>
<tr>
<td><code>file</code></td>
<td>0</td>
</tr>
<tr>
<td><code>options</code></td>
<td>options</td>
</tr>
</tbody>
</table>

DHCP option 53 (DHCP message type) is extended with a new value:
5. IANA Considerations

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

6. Security Considerations

Depending on layer 2 characteristics, DHCP reconfigure can be a security problem. Use of DHCP authentication is recommended in such cases.

7. References


8. 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