INTERNET-DRAFT
Intended Status: Standards Track
Expires: June 7, 2017

Luyuan Fang
eBay
Deepak Bansal
Microsoft
Fabio Chiussi
Luiginius

December 4, 2016

Forcerenew Reconfiguration Extensions for DHCPv4 draft-ietf-dhc-dhcpv4-forcerenew-extensions-01

Abstract

This document extends the definition of the DHCPFORCERENEW message for parameter reconfiguration in DHCPv4. This extension makes the DHCPFORCERENEW message more suitable to reconfigure configuration parameters other than IP addresses, and aligns the behavior of the reconfiguration procedure in DHCPv4 to the corresponding behavior in DHCPv6.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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 and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

Table of Contents

1. Introduction

Network and cloud operators increasingly use DHCP to distribute not just IP addresses, but also a variety of other configuration parameters to the clients. The DHCP servers may need to reconfigure such other configuration parameters in the clients in isolation, i.e., without reconfiguring IP addresses. In the case of reconfiguration of only configuration parameters other than IP addresses, it is especially important that service interruptions be avoided. Towards this goal, it is desirable for a DHCP client, when receiving a reconfiguration request from the DHCP server, to be made aware of whether such a request includes reconfiguration of IP addresses or only pertains to other configuration parameters, and have the client adapt its behavior to each situation. Currently, this is achieved in DHCPv6, but not in DHCPv4. This draft proposes an extension of the FORCERENEW message in DHCPv4 to provide this additional desired client behavior.

For historical reasons, the procedure for server-initiated reconfiguration of configuration parameters uses a different mechanism and produces a different behavior in DHCPv4 and in DHCPv6. This is especially noticeable in the case of reconfiguration of parameters other than IP addresses.

In DHCPv6 [RFC3315] [I-D. draft-ietf-dhc-rfc3315bis], the DHCP server sends a Reconfigure message to a client to inform the client that the server has new or updated configuration parameters. The Reconfigure message allows the client to distinguish whether the reconfiguration pertains to the IP addresses, in which case the client initiates a Renew/Reply, or it pertains to other parameters, in which case the client initiates an Information-request/Reply. In addition, the DHCPv6 reconfiguration procedure includes a way for the client to decline the reconfiguration attempt.

In DHCPv4 [RFC2131], the server-initiated reconfiguration procedure relies on the use of the DHCPFORCERENEW message [RFC3203] and is less granular than its IPv6 counterpart, which can result in service interruptions that could be otherwise avoided when the reconfiguration only involves parameters other than IP addresses.

This is the consequence of two differences with respect to the reconfiguration procedure in DHCPv6.

1. The DHCPFORCERENEW message does not contain any indication for the client to distinguish a reconfiguration of IP addresses from a reconfiguration of some other configuration information. As a result, the client always initiates a Renew/Reply transaction with the server, which typically lead to service interruptions.

2. In DHCPv4, there is no easy way for the client to decline a server-initiated reconfiguration request. The ability for a client to decline server-initiated reconfiguration may turn useful in the case of configuration information reconfiguration.

It should be noted that [RFC7341] specifies DHCPv4 over DHCPv6, thus making it possible to use the DHCPv6 reconfigure function to reconfigure parameters in DHCPv4. However, [RFC7341] is only applicable to a IPv6 core network. Thus, achieving similar reconfiguration behavior as DHCPv6 on a IPv4 network requires an extension to the DHCPFORCERENEW message.

In this document, we extend the DHCPFORCERENEW message used in DHCPv4 by introducing a new Message Type DHCPFORCEINFORENEW to distinguish reconfiguration of IP addresses from reconfiguration of other information. In the latter case, we use the usual option mechanism to distribute new or updated parameters to the client.

We also introduce a way for the client to decline the reconfiguration request.

Any server-initiated reconfiguration requires authentication. The extended DHCPFORCERENEW message must be used with the security mechanisms described in [RFC6704], which aligns DHCPv4 authentication with DHCPv6 authentication described in [I-D. draft-ietf-dhc-rfc3315bis].

The extended DHCPFORCENEW message described in this document aligns the behavior of server-initiated reconfiguration in DHCPv4 with the corresponding behavior in DHCPv6.

1.1. Terminology

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].

In this document, we use the terminology defined in [RFC3203] and in [I-D. draft-ietf-dhc-rfc3315bis].

2. Extended DHCPFORCERENEW Message for DHCPv4

2.1 DHCPFORCERENEW Procedure

This is the DHCPFORCERENEW procedure defined in [RFC3203].

The DHCP server sends a unicast DHCPFORCERENEW message to the client. Upon receipt of the unicast DHCPFORCERENEW message, the client enters

a Renew/Reply transaction with the server to try to renew its lease according to normal DHCP procedures. If the server wants to assign a new IP address to the client, it replies to the DHCPREQUEST with a DHCPNAK. The client then goes back to the init state and broadcasts a DHCPDISCOVER message. The server can now assign a new IP address to the client by replying with a DHCPOFFER. If the DHCPFORCERENEW message is lost, the DHCP server does not receive a DHCPREQUEST from the client and retransmits the DHCPFORCERENEW message using an exponential backoff algorithm.

The DHCPFORCERENEW message makes use of the normal DHCP message format with DHCP option 53 (DHCP message type) value equal to DHCPFORCERENEW (9).

As recognized in [RFC3203], usage of the DHCPFORCERENEW message to reconfigure local configuration parameters other than IP addresses can lead to the unnecessary interruption of active sessions. Thus, a modification of the DHCPFORCERENEW message is desirable to avoid service interruptions in such increasingly common situations.

2.2 DHCPFORCEINFORENEW: Extended DHCPFORCERENEW Message

The extended FORCERENEW message makes use of the normal DHCP message format with DHCP option 53 (message type) value equal to DHCPFORCEINFORENEW (TBD, see IANA considerations below).

Upon receipt of a DHCPFORCEINFORENEW, the client sends a DHCPINFORM message to the server to request and obtain new configuration information.

If the DHCPFORCEINFORENEW message is lost, the DHCP server does not receive a DHCPINFORM from the client and retransmits the DHCPFORCEINFORENEW message using an exponential backoff algorithm.

In order to assure backward compatibility with DHCP clients not supporting the extended DHCPFORCERENEW message, if no DHCPINFORM is received once the backoff expires, the DHCP server SHOULD send a DHCPFORCERENEW message to brute force the reconfiguration by reverting to the conventional DHCPv4 reconfiguration mechanism.

The fact that the DHCP server ultimately reverts to the DHCPFORCERENEW message, however, complicates the ability of the client to decline the FORCEINFORENEW message, as discussed in the next section.

2.3 DHCPFORCEINFORENEW Client Decline

It is desirable to introduce a way to allow the client to decline the

DHCPFORCEINFORENEW request from the server. This further aligns the client behavior in DHCPv4 server-initiated reconfiguration with the corresponding behavior in DHCPv6.

Because of the server behavior defined in the previous section, motivated by the objective of achieving backward compatibility with clients not supporting the extended DHCPFORCERENEW message, the DHCP client can't simply ignore the request, since that would eventually result in a DHCPFORCERENEW message to be sent by the server.

One obvious solution is to forego backward compatibility and have the DHCP server simply abandon the reconfiguration procedure at the end of the DHCPINFOFORCERENEW reconfiguration procedure.

Alternatively, a mechanism for the client to explicit inform the server that it is declining the server-initiated DHCPINFOFORCERENEW reconfiguration procedure needs to be devised.

3. Security Considerations

The reconfiguration procedure using extended DHCPFORCERENEW message described in this draft MUST be authenticated with the procedures described in [RFC3118] or [RFC6704].

The security considerations relating to the DHCPFORCEINFORENEW message are the same as for DHCPFORCERENEW message discussed in [RFC3203] and [RFC6704].

4. IANA Considerations

IANA is requested to assign a new value for DHCP option 53 (DHCP message type) [RFC2939] for the DHCPFORCEINFORENEW message from the registry "DHCP Message Type 53 Values" maintained at http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml

5. Acknowledgments

We would like to acknowledge Tomek Mrugalski, Christian Huitema and Bernie Volz for their comments and reviews.

6. References

6.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2939] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", BCP 43, RFC 2939, September 2000.

[RFC3203] T'Joens, Y., Hublet, C., and P. De Schrijver, "DHCP reconfigure extension", RFC 3203, December 2001.

[RFC3118] Droms, R., Ed., and W. Arbaugh, Ed., "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC6704] D. Miles et al., "Forcerenew Nonce Authentication", RFC 6704, August 2012.

[RFC7341] Q. Sun et al., "DHCPv4-over-DHCPv6 (DHCP 4o6) Transport", RFC 7341, August 2012.

6.2 Informative References

[I-D. draft-ietf-dhc-rfc3315bis] T. Mrugalski et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) bis", draft-ietf-dhc-rfc3315bis-06 (work in progress), October 201.

Authors' Addresses

Luyuan Fang
eBay
411 108th Ave NE
Bellevue, WA 98004
Email: lufang@ebay.com

Deepak Bansal
Microsoft
15590 NE 31st St.
Redmond, WA 98052
Email: dbansal@microsoft.com

Fabio Chiussi
Seattle, WA 98116
Email: fabiochiussi@gmail.com