DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 16, 2013

M. Boucadair
X. Pougnard
France Telecom

May 15, 2013

Reconfigure Triggered by DHCPv6 Relay Agents
draft-ietf-dhc-triggered-reconfigure-07

Abstract

This document defines new DHCPv6 messages: Reconfigure-Request and Reconfigure-Reply. Reconfigure-Request message is sent by a DHCPv6 relay agent to notify a DHCPv6 server about a configuration information change, so that the DHCPv6 server can send a Reconfigure message accordingly. Reconfigure-Reply message is used by the server to acknowledge the receipt of Reconfigure-Request.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on November 16, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Requirements Language 3
3. Problem Statement 3
4. Solution Overview 4
5. Link Address Option 6
6. Detailed Specification 7
6.1. Messages Format 7
6.2. Messages Validation 7
6.2.1. RECONFIGURE-REQUEST 7
6.2.2. RECONFIGURE-REPLY 7
6.3. Creation and Transmission of RECONFIGURE-REQUEST 8
6.4. Intermediate Relay Agents Behavior 9
6.5. Server Behavior 9
6.6. Receipt of RECONFIGURE-REPLY 10
7. Rate Limiting Considerations 11
8. IANA Considerations 11
9. Security Considerations 11
10. Acknowledgements 12
11. References 12
11.1. Normative References 12
11.2. Informative References 12
Authors' Addresses 13

1. Introduction

This document specifies two new DHCPv6 messages [RFC3315]: Reconfigure-Request and Reconfigure-Reply.

Section 3 describes a typical problem encountered to trigger the DHCPv6 server to issue a Reconfigure message when the configuration data is supplied by the relay agent. This problem may be encountered in other contexts. It is out of scope of this document to list all these cases.

Section 4 describes the proposed solution which relies on the use of Reconfigure-Request and Reconfigure-Reply messages. Reconfigure-

Request message is sent by a DHCPv6 relay agent to notify a DHCPv6 server about a configuration information change, so that the DHCPv6 server can send a Reconfigure message accordingly. Reconfigure-Reply message is used by the server to acknowledge the receipt of Reconfigure-Request.

Section 6 provides the detailed specification of the procedure to trigger Reconfigure messages by DHCPv6 relay agents.

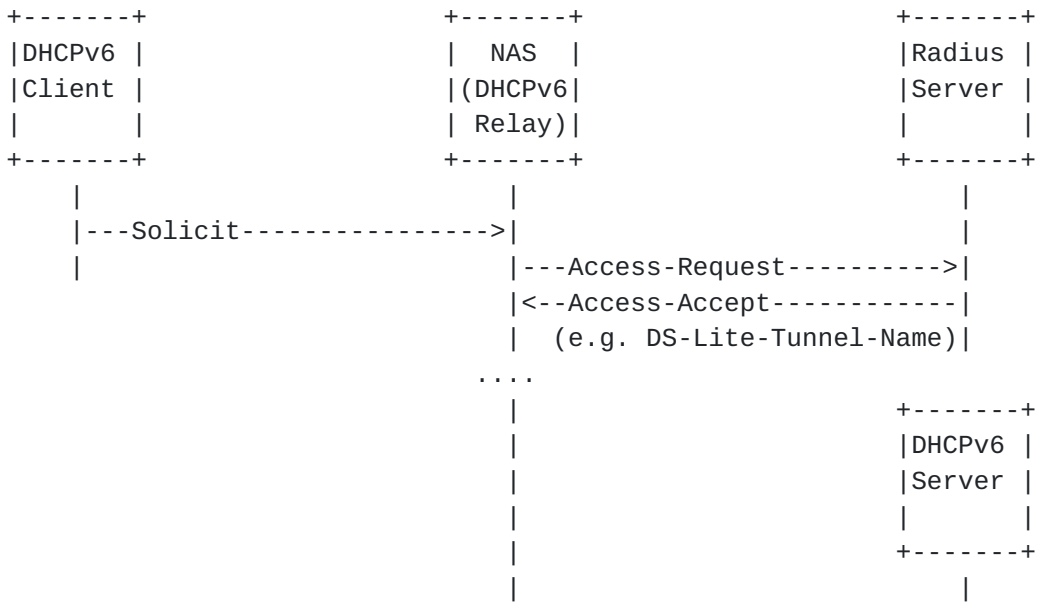
2. Requirements Language

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 [RFC2119].

3. Problem Statement

For cases where the DHCPv6 relay agent possesses some information that would be useful to the DHCPv6 client, [RFC6422] specifies a mechanism whereby the DHCPv6 relay agent can provide such information to the DHCPv6 server, which can, in turn, pass this information on to the DHCP client. This is achieved owing to the use of RSOO (Relay-Supplied Options option) which carries configuration data to the DHCPv6 server. The data conveyed in an RSOO is then sent back by the DHCPv6 server to the requesting DHCPv6 client.

An example of a RSOO context is shown in Figure 1; only a subset of exchanged DHCPv6 and RADIUS messages is represented. Figure 1 shows a broadband network scenario in which the Network Access Server (NAS) embeds a DHCPv6 relay agent.



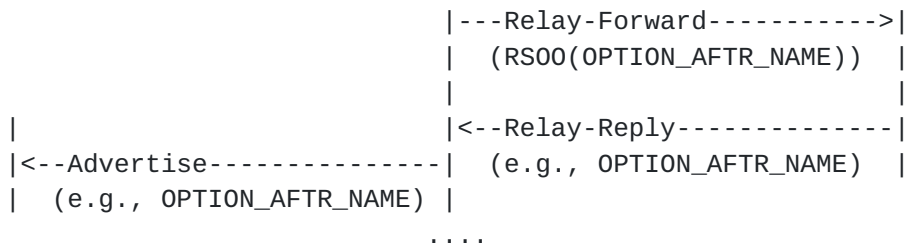


Figure 1: An Example of the RSOO Option Usage

A configuration change may result in an exchange of CoA (Change-of-Authorization, [RFC5176]) messages between the NAS/DHCPv6 relay agent and Dynamic Authorization Client (DAC) server as shown in Figure 2. In this example, the NAS answers with a CoA-Ack message to notify the DAC the CoA-Request is successfully handled.

Note the change of the configuration in the DHCPv6 relay agent can be triggered by any other out-of-band mechanism.

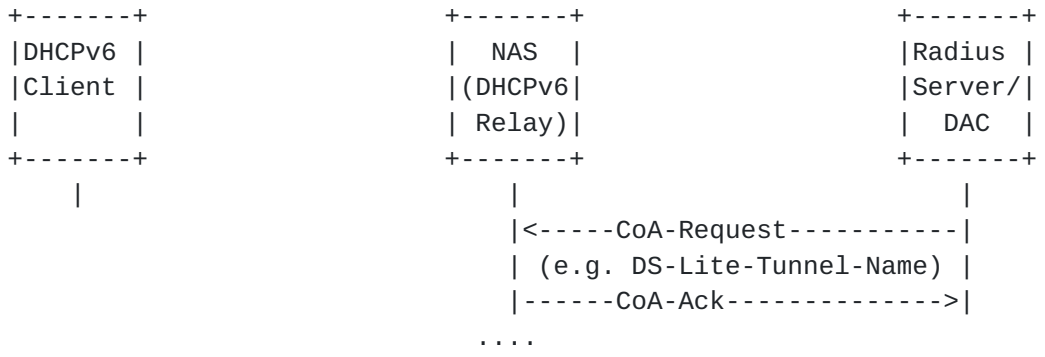


Figure 2: Change of configuration

Whenever the configuration information sent by the DHCPv6 relay agent to the DHCPv6 server change, the DHCPv6 server has no means to detect the change so that it can send a Reconfigure message accordingly. A solution is sketched in Section 4.

4. Solution Overview

To solve the problem described in Section 3, this document proposes a new DHCP message called Reconfigure-Request. In the example depicted in Figure 3, a Reconfigure-Request message is sent by the DHCPv6 relay agent to a DHCPv6 server as soon as the configuration data conveyed in an RSOO option have changed. Upon receipt of this message, and if it is configured to support such mode, the DHCPv6 server must build Reconfigure-Reply and Reconfigure messages. Reconfigure-Reply is used to acknowledge the receipt of Reconfigure-

Request. Reconfigure message encapsulated in Relay-Reply is sent to the DHCPv6 relay, which in turn will forward the message to the appropriate DHCPv6 client.

This setup assumes the relay has a record of the client, so that it has enough information to send the Reconfigure-Request message to the server. How the state is recorded in the relay is out of scope. For better resilience of the proposed solution, means to recover state in failure events (e.g., use of stable storage, DHCPv6 Bulk Leasequery [RFC5460]) need to be supported. These state recovery solutions are not discussed in this document.

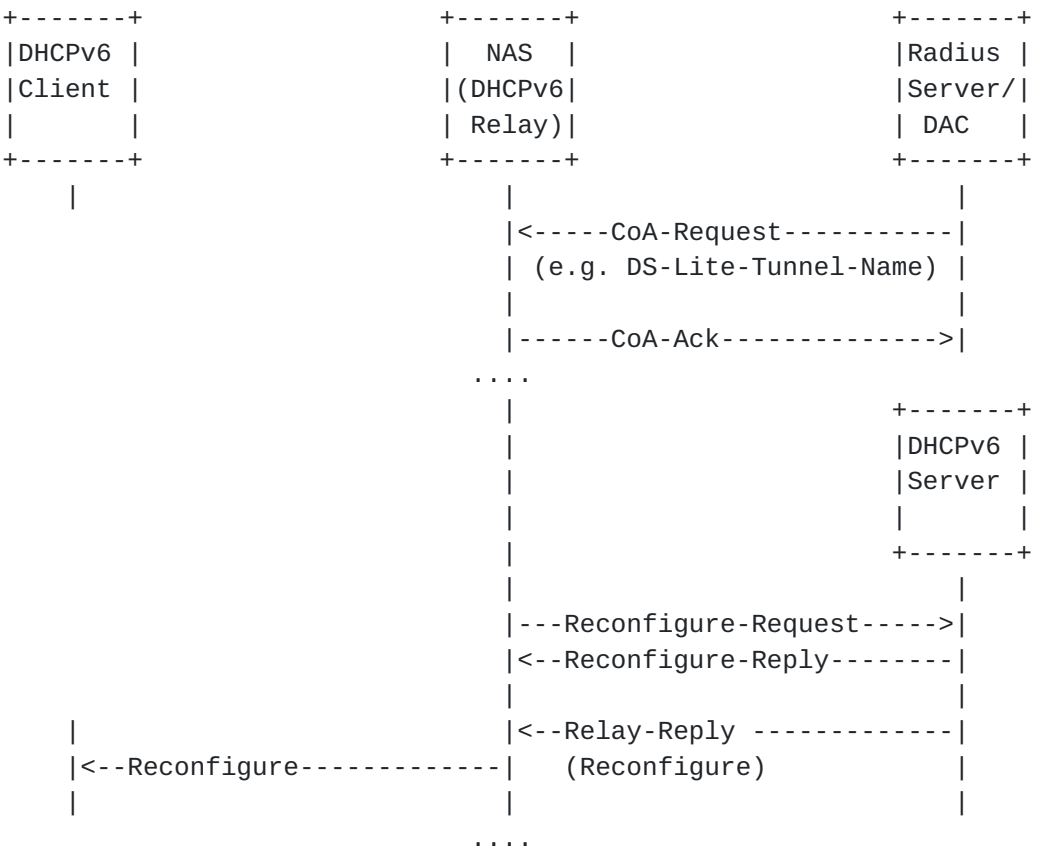


Figure 3: Flow Example with Reconfigure-Request

The support of Reconfigure-Reply simplifies the retransmission procedure of the relay as it provides an explicit indication from the server (see Section 6.3 for more details). An alternative approach is the relay monitors Reconfigure messages received from the server to conclude whether Reconfigure-Request was successfully handled or not. Nevertheless, this implicit approach may fail to achieve its goals in some cases: e.g., the server accepts the request but it delays to generate the corresponding Reconfigure messages due to its rate-limiting policies, the request was partially failed for some

clients, etc. To avoid useless reconfigure cycles (e.g., due to the loss of Reconfigure-Reply), the approach adopted in this document allows the relay to correct the content of a re-transmitted Reconfigure-Request based on some observed events (e.g., the client has retrieved the updated configuration). If the relay has no client to be reconfigured, it stops sending Reconfigure-Request messages.

The Reconfigure-Request message can also be used in other scenarios than those that assume the use of RSOO. It is out of scope of this document to describe all these scenarios.

5. Link Address Option

Figure 4 shows the format of the Link Address Option.

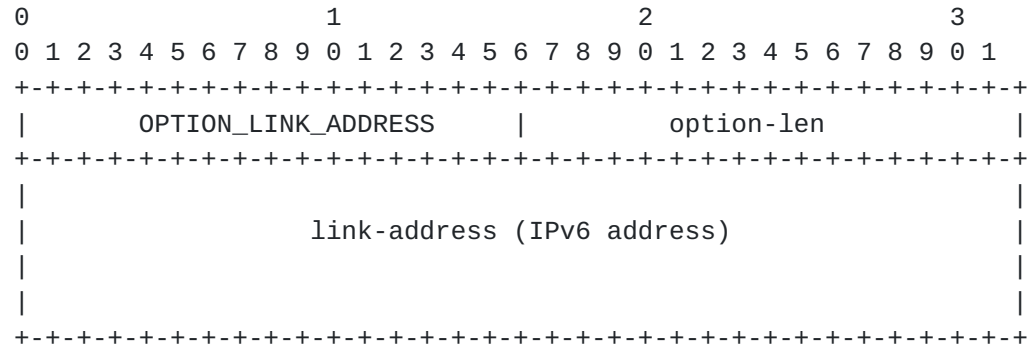


Figure 4: Message Format of Link Address Option

The description of the fields are as follows:

option-code: OPTION_LINK_ADDRESS (To be assigned by IANA, see Section 8).

option-len: 16 (octets).

link-address: An IPv6 address used by the server to identify the link on which the client is located.

The Link Address Option is used by the relay agent to indicate to the server the link on which the client is located. The relay agent MUST use a link-address value that is equivalent to the value used when relaying messages from the client to the server. Two link-address values are said to be equivalent if both values are IPv6 addresses that are on-link for the network link to which the client is connected.

To defend against poor implementations that do not correctly evaluate equivalence, the relay agent SHOULD use the same value that was sent

to the DHCPv6 server when relaying messages from the client to the server, as in Section 20.1.1 of [RFC3315].

6. Detailed Specification

6.1. Messages Format

Two new message type codes are defined:

- RECONFIGURE-REQUEST (To be assigned by IANA, see Section 8).
- RECONFIGURE-REPLY (To be assigned by IANA, see Section 8).

RECONFIGURE-REQUEST and RECONFIGURE-REPLY use the same format as defined in Section 6 of [RFC3315].

6.2. Messages Validation

6.2.1. RECONFIGURE-REQUEST

Clients MUST silently discard any received RECONFIGURE-REQUEST messages.

Servers MUST discard any received RECONFIGURE-REQUEST messages that meet any of the following conditions:

- the message does not include a Client Identifier Option [RFC3315].
- the message does not include a Link Address Option (Section 5).
- the message includes a Server Identifier Option [RFC3315] but the contents of the Server Identifier Option does not match the server's identifier.

6.2.2. RECONFIGURE-REPLY

Clients and Servers MUST silently discard any received RECONFIGURE-REPLY messages.

The relay MUST silently discard any received RECONFIGURE-REPLY messages that meet any of the following conditions:

- the "transaction-id" field in the message does not match the value used in the original message.
- the message does not include a Server Identifier Option.
- the message does not include a Status Code Option [RFC3315].

6.3. Creation and Transmission of RECONFIGURE-REQUEST

For any event (e.g., modification of the configuration information) that requires the server to issue a Reconfigure message, the relay agent determines the client(s) affected by the change and then builds a Reconfigure-Request message: the relay agent sets the "msg-type" field to RECONFIGURE-REQUEST, generates a transaction ID and inserts it in the "transaction-id" field.

The relay agent MUST include one or more Client Identifier Options [RFC3315] and a Link Address Option (Section 5) so that the DHCPv6 server can identify the corresponding client and the link on which the client is located.

The relay agent MAY include a Relay Identifier Option [RFC5460].

The relay agent MAY supply the updated configuration in the RSOO [RFC6422]. The relay agent MAY supply a Reconfigure Message Option to indicate which form of Reconfigure to use. The relay agent MAY include any option (e.g., Interface Identifier [RFC3315]) which it might insert when relaying a message received from a client.

When several clients on the same link are affected by a configuration change, the relay MUST include several Client Identifier Options, each of them identifies a specific client. If including Client Identifier Options of all impacted clients exceeds the maximum message size (see Section 7), the relay MUST generate several RECONFIGURE-REQUEST messages required to carry all Client Identifier Options. Rate-limit considerations are discussed in Section 7.

The relay sets the destination address of the RECONFIGURE-REQUEST message to the IP address it would have sent a Relay-Forw message (see Section 20 of [RFC3315]).

In case multiple servers are configured to the relay agent, several RECONFIGURE-REQUEST messages are to be built. The behavior of the relay agent to disambiguate responses when multiple servers are configured is implementation-specific. For example, an implementation may generate distinct "transaction-id"s per server while another implementation may use the content of the "transaction-id" field and the Server Identifier Option to disambiguate the responses.

The relay transmits RECONFIGURE-REQUEST messages according to Section 14 of [RFC3315], using the following parameters:

IRT 1 sec
MRT 10 secs

MRC 5
MRD 0

The relay MAY remove clients from the client identifier list in subsequent retransmissions, but MUST NOT add clients to the client identifier list. This decision is local to the relay (e.g., it may be based on observed events such as one or more clients were reconfigured on their own).

The relay may receive Reconfigure encapsulated in Relay-Reply before Reconfigure-Reply. The relay SHOULD NOT interpret it as if the Reconfigure-Request was successfully handled by the Server. The relay SHOULD use Reconfigure-Reply, not the Reconfigure message, to determine if the request was successful (see the discussion in Section 4) .

6.4. Intermediate Relay Agents Behavior

The relay agent MUST be configurable to accept or reject RECONFIGURE-REQUEST messages received from other relay agents. If no indication is explicitly configured to the relay, the default behavior is to accept RECONFIGURE-REQUEST messages.

If the relay is configured not to allow RECONFIGURE-REQUEST messages, the relay MUST silently discard any RECONFIGURE-REQUEST message it receives. If the relay is configured to accept RECONFIGURE-REQUEST messages, these messages are relayed as specified in Section 20.1.1 of [RFC3315].

6.5. Server Behavior

The server MUST be configurable to accept or reject RECONFIGURE-REQUEST messages. If no indication is explicitly configured to the server, the default behavior is to reject RECONFIGURE-REQUEST messages.

Upon receipt of a valid RECONFIGURE-REQUEST message from a DHCPv6 relay agent (see Section 6.2), the server determines the client(s) for which a Reconfigure message is to be sent.

The server constructs a Reconfigure-Reply message by setting the "msg-type" field to RECONFIGURE-REPLY, and copying the transaction ID from the RECONFIGURE-REQUEST message into the "transaction-id" field. The server includes its server identifier in a Server Identifier Option. The server MUST include a Status Code Option [RFC3315] indicating whether the request is successfully processed, failed or partially failed.

- If the server fails to process the request, the server MUST set the Status Code Option to the appropriate status code (e.g., UnspecFail, NotAllowed, etc.). In particular,
  - UnspecFail MUST be returned if Reconfigure-Request message is malformed.
  - NotAllowed MUST be returned if the server is not configured to allow Reconfigure-Request.
  - NotConfigured MUST be returned if the server has no record of the link [RFC5007].
- If the RECONFIGURE-REQUEST is successfully validated, the server MUST return a Status Code Option indicating "Success". In addition, the server MUST include a list of all the Client Identifier Options of the clients to which Reconfigure messages will not be sent (e.g., the server has no record of the client or the client did not negotiate for Reconfigure support). Note that this means that "Success" will be returned even if Reconfigure messages will not be sent to any of the clients.

If RSOO is supplied, the server might use its content to double check whether a Reconfigure is required to be sent to the client. This assumes the server stored the content of RSOO it used to generate configuration data sent to requesting clients.

The server might use the content of the Reconfigure Message Option supplied by the relay agent to determine which form of Reconfigure to use.

Then, the server MUST follow the procedure defined in Section 19.1 of [RFC3315] to construct a Reconfigure message.

Rate-limit considerations are discussed in Section 7.

6.6. Receipt of RECONFIGURE-REPLY

Depending on the status code enclosed in a received RECONFIGURE-REPLY message, the relay may decide to terminate the request (e.g., NotAllowed, NotConfigured, and Success) or try a different corrected RECONFIGURE-REQUEST (e.g., UnspecFail).

When multiple servers are configured, the relay should expect to receive several RECONFIGURE-REPLY messages. As mentioned in Section 6.3, the relay should be able to disambiguate these responses and associate them with a given server. The relay agent assumes the request is successfully handled for a client if there is at least one

Reconfigure-Reply message in which the corresponding Client Identifier Option does not appear.

7. Rate Limiting Considerations

The relay MUST rate-limit RECONFIGURE-REQUEST messages to be sent to the server. The relay MUST be configured with required rate-limit parameters. The maximum RECONFIGURE-REQUEST packet size SHOULD be configurable and the default value MUST be 1280 octets.

The server MUST rate-limit Reconfigure messages triggered by RECONFIGURE-REQUEST messages. The server MUST be configured with required rate-limit parameters.

8. IANA Considerations

IANA is requested to assign the following new DHCPv6 Message type in the registry maintained in http://www.iana.org/assignments/ dhcpv6-parameters:

RECONFIGURE-REQUEST

RECONFIGURE-REPLY

IANA is requested to assign the following new DHCPv6 Option Codes in the registry maintained in http://www.iana.org/assignments/ dhcpv6-parameters:

OPTION_LINK_ADDRESS

9. Security Considerations

Security considerations elaborated in [RFC3315] (in particular Section 21.1) and [RFC6422] must be taken into account. In addition, DHCPv6 servers MAY be configured to reject relayed RECONFIGURE-REQUEST messages or restrict relay chaining (see [RFC5007] for more discussion about the rationale of this recommended behavior). Section 6.5 specifies the error code to return when the server is configured to reject RECONFIGURE-REQUEST messages.

Relay agents SHOULD implement appropriate means to prevent using RECONFIGURE-REQUEST messages as a denial-of-service attack on the DHCPv6 servers.

Because RECONFIGURE-REQUEST message provides a mechanism for triggering the DHCPv6 Reconfigure message, and the DHCPv6 Reconfigure message can raise security threats (e.g., to control the timing of a DHCPv6 renewal), the DHCPv6 server MUST have some mechanism for

determining that the relay agent is a trusted entity. DHCPv6 servers and relay agents MUST implement relay message authentication as described in Section 21.1 of [RFC3315]. DHCPv6 servers MAY also implement a control policy based on the content of received Relay Identifier Option [RFC5460]. Administrators are strongly advised to configure one of these security mechanisms.

In an environment where the network connecting the relay agent to the DHCPv6 server is physically secure and does not contain devices not controlled by the server administrator, it may be sufficient to trust the Relay Agent Identifier provided by the relay agent. In networks where the security of the machines with access to the data path is not under the control of the server administrator, IPsec [RFC4301] is necessary to prevent spoofing of RECONFIGURE-REQUEST messages. DHCPv6 servers MUST silently discard RECONFIGURE-REQUEST messages originating from unknown relay agents.

10. Acknowledgements

Many thanks to R. Maglione, A. Kostur, G. Halwasia, C. Jacquenet, B. Leiba, R. Sparks, A. Farrel, B. Claise, J. Jaeggli, and P. Resnick for the comments and review.

Special thanks to T. Lemon, B. Volz and T. Mrugalski who provided a detailed review.

11. References

11.1. Normative References

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

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

[RFC6422] Lemon, T. and Q. Wu, "Relay-Supplied DHCP Options", RFC 6422, December 2011.

11.2. Informative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5007] Brzozowski, J., Kinnear, K., Volz, B., and S. Zeng, "DHCPv6 Leasequery", RFC 5007, September 2007.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

[RFC5460] Stapp, M., "DHCPv6 Bulk Leasequery", RFC 5460, February 2009.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Xavier Pougnard
France Telecom
Lannion
France

Email: xavier.pougnard@orange.com