

DHC Working Group
Internet-Draft
Updates: [3315](#), [6422](#) (if approved)
Intended status: Standards Track
Expires: September 12, 2013

M. Boucadair
X. Pournard
France Telecom
March 11, 2013

Reconfigure Triggered by DHCPv6 Relay Agents
draft-ietf-dhc-triggered-reconfigure-04

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.

This document updates [RFC 3315](#) and [RFC 6422](#).

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 September 12, 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

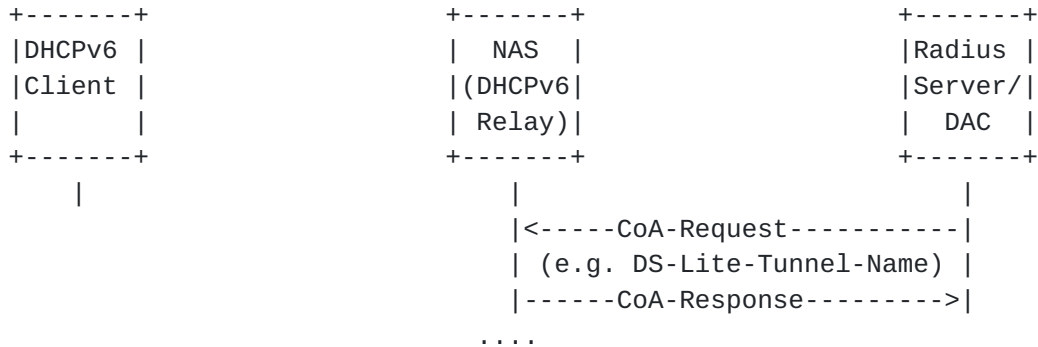
to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Problem	3
1.2.	Requirements Language	4
2.	Proposed Solution	4
3.	Link Address Option	6
4.	RECONFIGURE-REQUEST and RECONFIGURE-REPLY	6
4.1.	Messages Format	6
4.2.	Messages Validation	7
4.2.1.	RECONFIGURE-REQUEST	7
4.2.2.	RECONFIGURE-REPLY	7
4.3.	Creation and Transmission of RECONFIGURE-REQUEST	7
4.4.	Intermediate Relay Agents Behaviour	8
4.5.	Server Behaviour	9
4.6.	Receipt of RECONFIGURE-REPLY	10
5.	Rate Limiting Considerations	10
6.	IANA Considerations	10
7.	Security Considerations	11
8.	Acknowledgements	11
9.	References	11
9.1.	Normative References	11
9.2.	Informative References	12
	Authors' Addresses	12

The change of the configuration may result in RADIUS exchanges [RFC5176] between the NAS/DHCPv6 relay agent and Dynamic

Authorization Client (DAC) server as shown in Figure 2. Note the change of the configuration in the DHCPv6 relay agent can be triggered by any other out-of-band mechanism.



CoA (Change-of-Authorization, [[RFC5176](#)])

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 it so that it can send a Reconfigure message with the updated configuration data accordingly. A solution is sketched in [Section 2](#).

1.2. 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](#)].

2. Proposed Solution

To solve the problem described in [Section 1.1](#), 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 RS00 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.

Furthermore, means to recover state in failure events must be supported, but are not discussed in this document.

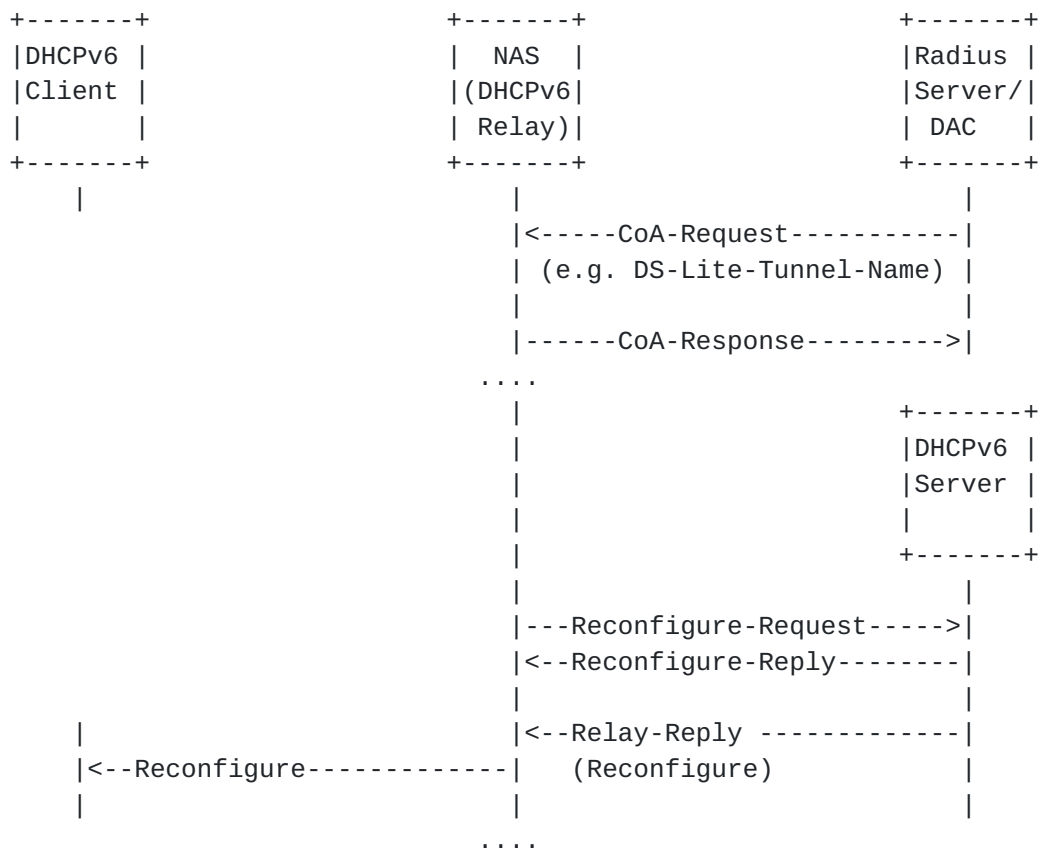


Figure 3: Flow Example with Reconfigure-Request

The support of Reconfigure-Reply simplifies the retransmission procedure of the relay as it provides an explicit indication from the server (see [Section 4.3](#) 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 reconfigure, it stops sending Reconfigure-Request messages.

The Reconfigure-Request message can also be used in other scenarios than those that assume the use of RS00. It is out of scope of this

document to describe all these scenarios.

3. Link Address Option

Figure 4 shows the format of the Link Address Option.

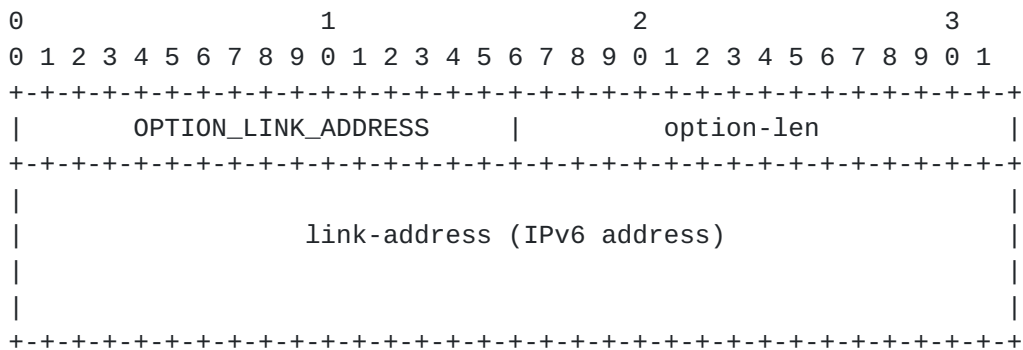


Figure 4: Message Format of Link Address Option

The description of the fields are as follows:

option-code: OPTION_LINK_ADDRESS (To be assigned by IANA, see [Section 6](#)).

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. 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 \[RFC3315\]](#).

4. RECONFIGURE-REQUEST and RECONFIGURE-REPLY

4.1. Messages Format

Two new message type codes are defined:

- o RECONFIGURE-REQUEST (To be assigned by IANA, see [Section 6](#)).
- o RECONFIGURE-REPLY (To be assigned by IANA, see [Section 6](#)).

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

[4.2.](#) Messages Validation

[4.2.1.](#) RECONFIGURE-REQUEST

Clients MUST silently discard any received RECONFIGURE-REQUEST messages.

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

- o the message does not include a Client Identifier Option [[RFC3315](#)].
- o the message does not include a Link Address Option ([Section 3](#)).
- o the message includes a Server Identifier Option [[RFC3315](#)] but the contents of the Server Identifier Option does not match the server's identifier.

[4.2.2.](#) 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:

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

[4.3.](#) 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 3](#)) so that the DHCPv6 server can identify the corresponding client and the link on which the client is located.

The relay agent MAY supply the updated configuration in the RS00 [[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 5](#)), the relay MUST generate several RECONFIGURE-REQUEST messages required to carry all Client Identifier Options. Rate-limit considerations are discussed in [Section 5](#).

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

When retransmission is required, the relay may decide to correct the content of RECONFIGURE-REQUEST message it issues (e.g., update 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.

[4.4.](#) Intermediate Relay Agents Behaviour

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 to reject RECONFIGURE-REQUEST, the relay MUST silently discard any RECONFIGURE-REQUEST it receives. If the

relay is configured to accept RECONFIGURE-REQUEST messages, these messages are relayed as specified in [Section 20.1.1 of \[RFC3315\]](#).

4.5. Server Behaviour

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.

If the server is configured to reject RECONFIGURE-REQUEST, the server MUST silently discard any RECONFIGURE-REQUEST it receives.

Upon receipt of a valid Reconfigure-Request message from a DHCPv6 relay agent (see [Section 4.2](#)), 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 MUST include a Status Code Option [\[RFC3315\]](#) indicating whether the request is successfully processed, failed or partially failed.

- o If the server fails to validate 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.
- o 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 RS00 is supplied, the server MAY use its content to double check whether a Reconfigure is required to be sent to the client. This

assumes the server store the content of RS00 it used to generate configuration data sent to requesting clients.

The server MAY 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 5](#).

4.6. Receipt of RECONFIGURE-REPLY

Depending on the status code enclosed in a received RECONFIGURE-REPLY message, the relay may decide to terminate the request or try a different corrected Reconfigure-Request.

5. 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 (i.e., the rate of Reconfigure messages). 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 (i.e., the rate of Reconfigure messages).

6. 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

7. 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 discard relayed Reconfigure-Request messages or restrict relay chaining (see [[RFC5007](#)] for more discussion about the rationale of this recommended behavior).

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 DHCP Reconfigure message, and the DHCP Reconfigure message can raise security threats (e.g., to control the timing of a DHCP renewal), the DHCP server MUST have some mechanism for determining that the relay agent is a trusted entity. Reconfigure-Request messages originating from unknown relay agents MUST be silently dropped.

8. Acknowledgements

Many thanks to R. Maglione, A. Kostur, G. Halwasia and C. Jacquenet for the comments and review.

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

9. References

9.1. 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.

9.2. Informative References

- [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.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange.com

Xavier Pournard
France Telecom
Lannion,
France

Phone:
Email: xavier.pournard@orange.com

