RECONFIGURE Triggered by DHCPv6 Relay Agents
draft-ietf-dhc-triggered-reconfigure-00

Abstract

   This document defines a new DHCPv6 message type: RECONFIGURE-REQUEST.
   This 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.

   This document updates RFC3315 and RFC6422.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Problem

[RFC6422] updates the DHCPv6 specification [RFC3315] with a new
feature to let a DHCPv6 relay agent communicate information towards a
DHCPv6 Client, and which is not available at the DHCPv6 server. 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.

```
   +-------+                  +-------+               +-------+
   |DHCPv6 |                  |  NAS  |               |Radius |
   |Client |                  |(DHCPv6|               |Server |
   |       |                  | Relay)|               |       |
   +-------+                  +-------+               +-------+
       |                          |                       |
       |---Solicit--------------->|                       |
       |                          |---Access-Request---------->|
       |                          |<--Access-Accept------------|
       |                          |  (e.g. DS-Lite-Tunnel-Name)|
                                 ....

                                  |                   +-------+
                                  |                   |DHCPv6 |
                                  |                   |Server |
                                  |                   |       |
                                  |                   +-------+
                                  |                       |
                                  |---Relay-Forward----------->|
                                  | (RSOO(DS-Lite-Tunnel-Name))|
                                  |                       |
       |                          |<--Relay-Reply--------------|
       |<--Advertise--------------|
       | (e.g., OPTION_AFTR_NAME) |
                                 ....
```

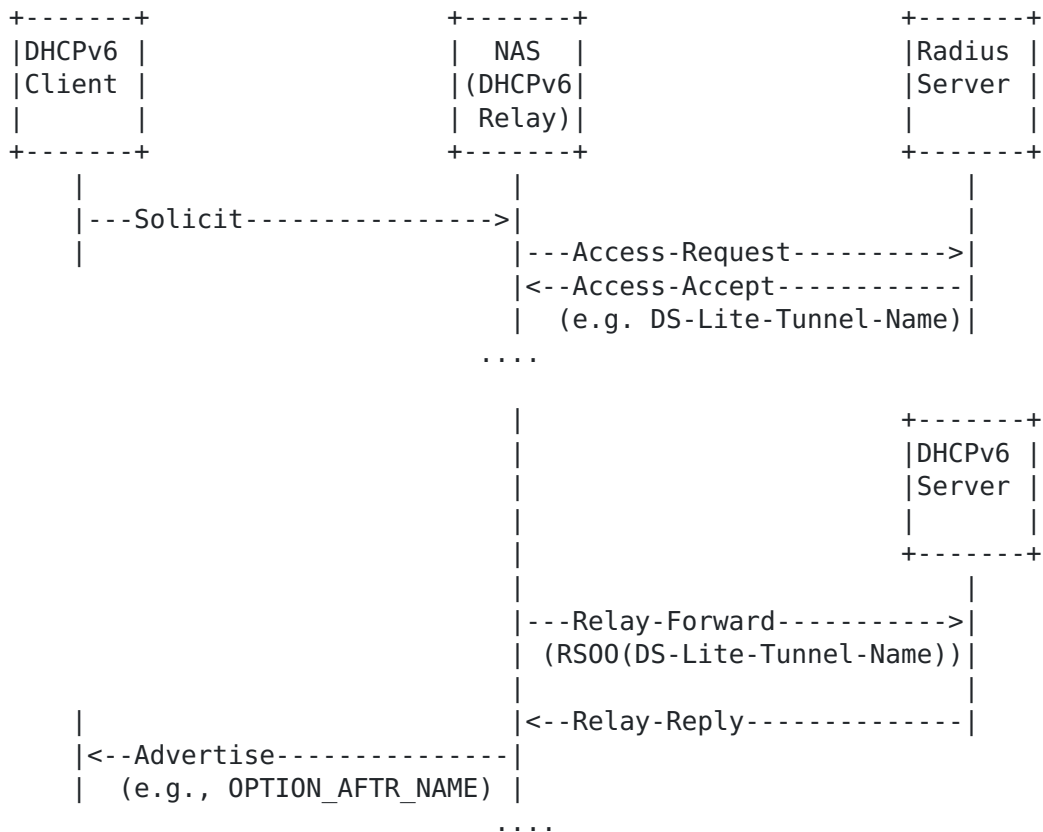   Figure 1: An Example of the RSOO Option Usage

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.

```
    +-------+                  +-------+                  +-------+
    |DHCPv6 |                  |  NAS  |                  |Radius |
    |Client |                  |(DHCPv6|                  |Server/|
    |       |                  | Relay)|                  |  DAC  |
    +-------+                  +-------+                  +-------+
        |                          |                          |
                                   |<-----CoA-Request----------|
                                   | (e.g. DS-Lite-Tunnel-Name) |
                                   |------CoA-Response--------->|
                                  ....
```

      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 RSOO option have changed. Upon receipt of this
   message, and if it is configured to support such mode, the DHCPv6
   server must build a Reconfigure message. This message is then 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. Means to recover state in failure events must be supported,
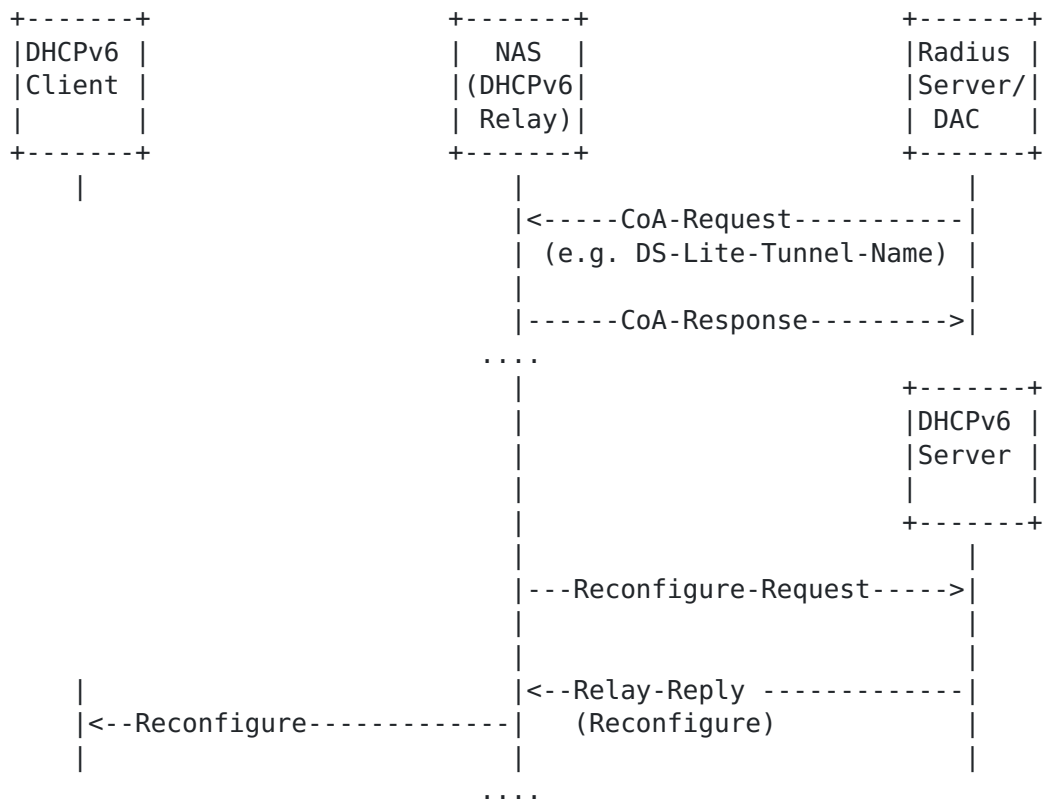   but are not discussed in this document.

```
   +-------+                   +-------+                   +-------+
   |DHCPv6 |                   |  NAS  |                   |Radius |
   |Client |                   |(DHCPv6|                   |Server/|
   |       |                   | Relay)|                   | DAC   |
   +-------+                   +-------+                   +-------+
       |                           |                           |
       |                           |<-----CoA-Request----------|
       |                           | (e.g. DS-Lite-Tunnel-Name) |
       |                           |                           |
       |                           |------CoA-Response--------->|
                                 ....
       |                           |                       +-------+
       |                           |                       |DHCPv6 |
       |                           |                       |Server |
       |                           |                       |       |
       |                           |                       +-------+
       |                           |                           |
       |                           |---Reconfigure-Request----->|
       |                           |                           |
       |                           |                           |
       |                           |<--Relay-Reply ------------|
       |<--Reconfigure------------|   (Reconfigure)           |
       |                           |                           |
                                 ....
```

                Figure 3: RECONFIGURE-REQUEST Flow Example

   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.

3. RECONFIGURE-REQUEST

3.1. Message Format

   A new message type code is defined:

      RECONFIGURE-REQUEST (To be assigned by IANA, see Section 4).

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

3.2. Message Validation

   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 an OPTION_CLIENTID option.
o the message includes an OPTION_SERVERID option but the contents of
   the OPTION_SERVERID option does not match the server's identifier.

The server MUST be configurable to accept or reject RECONFIGURE-
REQUEST messages. If the server is configured to reject RECONFIGURE-
REQUEST, the server MUST silently discard any RECONFIGURE-REQUEST it
receives.

   Discussion Note: Should the document specify the behavior of
   intermediate relay agents if any?

Because this 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.

3.3. 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 which is affected by the change and then
builds a Reconfigure-Request message: the relay agent sets the "msg-
type" field to RECONFIGURE-REQUEST and sets the "transaction-id "
field to 0. The relay agent MUST include an OPTION_CLIENTID option
[RFC3315] so that the DHCPv6 server can identify the corresponding
client. The relay agent MAY supply the updated configuration in the
RSOO [RFC6422]. The relay agent MAY supply an OPTION_RECONF_MSG
option to indicate which form of Reconfigure to use.

When several clients are concerned with a configuration change, the
relay MUST include several OPTION_CLIENTID options, each of them
identifies a specific client. If including OPTION_CLIENTID options
of all impacted clients exceeds the maximum message size, the relay
MUST generate several RECONFIGURE-REQUEST messages required to carry
all OPTION_CLIENTID options.

   Discussion Note: What to do when all clients bound to the same
   relay agent are impacted by a configuration change? Should the
   document indicate the relay MUST include Relay-ID Option
   (RFC5460)?

3.4. Server Behaviour

   Upon receipt of a valid Reconfigure-Request message from a DHCPv6
   relay agent (see Section 3.2), the server determines the client(s)
   for which a Reconfigure message is to be sent.

   The server MAY use the content of the OPTION_RECONF_MSG option
   supplied by the relay agent to determine which form of Reconfigure to
   use.

   If RSOO 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 RSOO it used to generate
   configuration data sent to requesting clients.

   Then, the server MUST follow the procedure defined in Section 19.1 of
   [RFC3315] to construct a Reconfigure message. This message may be
   sent directly to the DHCPv6 client or to a relay agent [RFC3315].

4. IANA Considerations

   This document requests IANA to assign a new DHCPv6 Message type:

      RECONFIGURE-REQUEST

5. Security Considerations

   Security considerations elaborated in [RFC3315] 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.

6. Acknowledgements

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

7. References

7.1. 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.

7.2. 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 Pougnard
   Orange Labs
   Lannion,
   France

   Phone:
   Email: xavier.pougnard@orange.com