Rebind Capability in DHCPv6 Reconfigure Messages
draft-ietf-dhc-dhcpv6-reconfigure-rebind-10.txt

Abstract

This document updates RFC 3315 (DHCPv6) to allow the Rebind message type to appear in the Reconfigure Message option of a Reconfigure message. It extends the Reconfigure message to allow a DHCPv6 server to cause a DHCPv6 client to send a Rebind message. The document also clarifies how a DHCPv6 client responds to a received Reconfigure message.

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 October 18, 2012.

Copyright Notice

Copyright (c) 2012 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.
Table of Contents

1. Introduction ................................................. 4
2. Terminology .................................................. 4
3. The Reconfigure Message option of the DHCPv6 Reconfigure Message ................................................. 4
4. Server Behavior .............................................. 5
5. Client Behavior ............................................. 8
6. Clarification of section 19.4.2, RFC 3315 .................. 9
7. Security Considerations ...................................... 9
8. Acknowledgements .......................................... 9
9. IANA Considerations ......................................... 10
10. Change log [RFC Editor please remove] ..................... 10
11. References ................................................ 10
    11.1. Normative References ................................. 10
    11.2. Informative References ............................... 10
Authors’ Addresses .............................................. 11
1. Introduction

DHCPv6 [RFC3315] allows a server to send an unsolicited Reconfigure message to a client. The client’s response to a Reconfigure message, according to section 19 of RFC 3315 is either a Renew or an Information-Request message, depending on the contents of the msg-type field in the Reconfigure Message option of the Reconfigure message. If the client sends a Renew message, it includes a Server Identifier option in the Renew message to specify the server that should respond to the Renew message. The RFC 3315 specification is only suitable for the scenarios that client would communicate with the same DHCPv6 servers.

There are also scenarios that the client must communicate with a different server: for example, a network administrator may choose to shut down a DHCPv6 server and move these clients who most recently communicated with it to another different server. Hence, this document expands the allowed values of the message type field with in reconfiguration message to allow the server to indicate the client to send a Rebind message, which does not include a Server Identifier option and allows any server to respond to the client.

RFC 3315 does not specify that a Reconfigure message must be sent from the server with which the client most recently communicated, and it does not specify which server the client should identify with a Server Identifier option when the client responds to the Reconfigure message. This document clarifies that the client should send a Renew message in response to a Reconfigure message with a Server Identifier option identifying the same server that the client would have identified if the client had sent the Renew message after expiration of the timer T1.

2. 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 [RFC2119].

This document uses IPv6 and DHCPv6 terms as defined in section 4 of [RFC3315].

3. The Reconfigure Message option of the DHCPv6 Reconfigure Message

This section modifies section 22.19 of RFC 3315 to allow the specification of the Rebind message in a Reconfigure message.
A server includes a Reconfigure Message option in a Reconfigure message to indicate to the client whether the client responds with a Renew, an Information-request, or a Rebind message.

The format of this option is:

```
+-------------------+ 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|                    | 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------+-------------------+-------------------+-------------------+
| 0                 | 1                 | 2                 | 3                 |
|                    | OPTION_RECONF_MSG | option-len         |
|                    | msg-type          |                   |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
```

option-code   OPTION_RECONF_MSG (19).
option-len    1.
msg-type      5 for Renew message, 6 for Rebind, 11 for Information-request message.

4. Server Behavior

This section updates specific text in sections 19.1, and 19.2 of RFC 3315.

Section 19.1.1:

OLD:

The server MUST include a Reconfigure Message option (defined in section 22.19) to select whether the client responds with a Renew message or an Information-Request message.

The server MUST NOT include any other options in the Reconfigure except as specifically allowed in the definition of individual options.

A server sends each Reconfigure message to a single DHCP client, using an IPv6 unicast address of sufficient scope belonging to the DHCP client. If the server does not have an address to which it can send the Reconfigure message directly to the client, the server uses a Relay-reply message (as described in section 20.3) to send the Reconfigure message to a relay agent that will relay the message to the client. The server may obtain the address of the client (and the appropriate relay agent, if required) through the information the server has about clients that have been in contact with the server, or through some external agent.
To reconfigure more than one client, the server unicasts a separate message to each client. The server may initiate the reconfiguration of multiple clients concurrently; for example, a server may send a Reconfigure message to additional clients while previous reconfiguration message exchanges are still in progress.

The Reconfigure message causes the client to initiate a Renew/Reply or Information-request/Reply message exchange with the server. The server interprets the receipt of a Renew or Information-request message (whichever was specified in the original Reconfigure message) from the client as satisfying the Reconfigure message request.

NEW:

The server MUST include a Reconfigure Message option (as defined in Section 3) to select whether the client responds with a Renew message, a Rebind message or an Information-Request message.

The server MUST NOT include any other options in the Reconfigure except as specifically allowed in the definition of individual options.

A server sends each Reconfigure message to a single DHCP client, using an IPv6 unicast address of sufficient scope belonging to the DHCP client. If the server does not have an address to which it can send the Reconfigure message directly to the client, the server uses a Relay-reply message (as described in section 20.3) to send the Reconfigure message to a relay agent that will relay the message to the client. The server may obtain the address of the client (and the appropriate relay agent, if required) through the information the server has about clients that have been in contact with the server, or through some external agent.

To reconfigure more than one client, the server unicasts a separate message to each client. The server may initiate the reconfiguration of multiple clients concurrently; for example, a server may send a Reconfigure message to additional clients while previous reconfiguration message exchanges are still in progress.

The Reconfigure message causes the client to initiate a Renew/Reply, a Rebind/Reply message exchange or an Information-request/Reply message exchange. The server interprets the receipt of a Renew, a Rebind or an Information-request message (whichever was specified in the original Reconfigure message) from the client as satisfying the Reconfigure message request.

Section 19.1.2:
OLD:

If the server does not receive a Renew or Information-request message from the client in REC_TIMEOUT milliseconds, the server retransmits the Reconfigure message, doubles the REC_TIMEOUT value and waits again. The server continues this process until REC_MAX_RC unsuccessful attempts have been made, at which point the server SHOULD abort the reconfigure process for that client.

NEW:

If the server does not receive a Renew, Rebind or Information-request message from the client in REC_TIMEOUT milliseconds, the server retransmits the Reconfigure message, doubles the REC_TIMEOUT value and waits again. The server continues this process until REC_MAX_RC unsuccessful attempts have been made, at which point the server SHOULD abort the reconfigure process for that client.

Section 19.2:

OLD:

19.2. Receipt of Renew or Rebind Messages

The server generates and sends a Reply message to the client as described in sections 18.2.3 and 18.2.8, including options for configuration parameters.

The server MAY include options containing the IAs and new values for other configuration parameters in the Reply message, even if those IAs and parameters were not requested in the Renew message from the client.

NEW:

19.2. Receipt of Renew Messages

In response to a Renew message, the server generates and sends a Reply message to the client as described in sections 18.2.3 and 18.2.8, including options for configuration parameters.

In response to a Rebind message, the server generates and sends a Reply message to the client as described in sections 18.2.4 and 18.2.8, including options for configuration parameters.

The server MAY include options containing the IAs and new values for other configuration parameters in the Reply message, even if those IAs and parameters were not requested in the Renew or Rebind message
from the client.

5. Client Behavior

This section updates specific text in section 19.4 of RFC 3315.

Section 19.4.1:

OLD:

Upon receipt of a valid Reconfigure message, the client responds with either a Renew message or an Information-request message as indicated by the Reconfigure Message option (as defined in section 22.19). The client ignores the transaction-id field in the received Reconfigure message. While the transaction is in progress, the client silently discards any Reconfigure messages it receives.

NEW:

Upon receipt of a valid Reconfigure message, the client responds with a Renew message, a Rebind message or an Information-request message as indicated by the Reconfigure Message option (as defined in Section 3). The client ignores the transaction-id field in the received Reconfigure message. While the transaction is in progress, the client silently discards any Reconfigure messages it receives.

Section 19.4.2:

ADD new second and third paragraphs:

When responding to a Reconfigure, the client creates and sends the Rebind message in exactly the same manner as outlined in section 18.1.4 of RFC 3315, with the exception that the client copies the Option Request option and any IA options from the Reconfigure message into the Rebind message.

If a client is currently sending Rebind messages, as described in section 18.1.4 of RFC 3315, the client ignores any received Reconfigure messages.

Section 19.4.4:

OLD:

The client uses the same variables and retransmission algorithm as it does with Renew or Information-request messages generated as part of a client-initiated configuration exchange. See sections 18.1.3 and
18.1.5 for details. If the client does not receive a response from the server by the end of the retransmission process, the client ignores and discards the Reconfigure message.

NEW:

The client uses the same variables and retransmission algorithm as it does with Renew, Rebind or Information-request messages generated as part of a client-initiated configuration exchange. See sections 18.1.3, 18.1.4 and 18.1.5 of RFC 3315 for details. If the client does not receive a response from the server by the end of the retransmission process, the client ignores and discards the Reconfigure message.

6. Clarification of section 19.4.2, RFC 3315

When sending a Renew message in response to the receipt of a Reconfigure message, the client MUST include a Server Identifier option identifying the server the client most recently communicated with.

7. Security Considerations

This document allows the Rebind message type to appear in the Reconfigure Message option of a Reconfigure message so that the client rebinds to a different DHCPv6 server. A malicious attacker may use a faked Reconfigure message to force the client to disconnect from the current server and relink to a faked server by quickly responding to the client’s Rebind message. A similar attack is available in DHCPv6 by an attacker spoofing itself as a valid DHCPv6 server in response to a Solicit or Request message. These attacks can be prevented by using the AUTH option [RFC3315]. DHCPv6 clients that support Reconfigure-Rebind MUST implement the Reconfigure Key authentication protocol as described in [RFC3315] section 21.5. Other authentication mechanisms may optionally be implemented. For example, the Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6], based on Cryptographically Generated Addresses (CGA) [RFC3972], can provide source address ownership validation, message origin authentication and message integrity without requesting symmetric key pairs or supporting from any key management system.

8. Acknowledgements

Valuable comments were made by Jari Arkko, Sean Turner, Ted Lemon and Stephen Farrell.
9. IANA Considerations

There are no actions for IANA associated with this document.

10. Change log [RFC Editor please remove]

Revision -05

Clarified description of this feature in introduction.

Clarified action of client if it receives a Reconfigure while sending Rebind messages.

Revision -08

Add a new co-author. Refreshed expired draft. Refine the motivation and suitable scenarios, also add some new security considerations. Correct the intended status to standard track.

Revision-10

Adopt OLD-NEW style according to IESG comment and address other IESG comments.

11. References

11.1. Normative References


11.2. Informative References

[I-D.ietf-dhc-secure-dhcpv6]
Authors’ Addresses

D. R. Evans
ARRIS International, Inc.
IPfonix, Inc., 330 WCR 16 1/2
Longmont, CO  80504-9467
USA

Phone: +1 303.682.2412
Email: N7DR@ipfonix.com

Ralph Droms
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA  01719
USA

Phone: +1 978.936.1674
Email: rdroms@cisco.com

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com