Internet Engineering Task Force (IETF)
Request for Comments: 6644
Updates: 3315
Category: Standards Track
ISSN: 2070-1721

D. Evans
IPfonix, Inc.
R. Droms
Cisco Systems, Inc.
S. Jiang
Huawei Technologies Co., Ltd

July 2012

Rebind Capability in DHCPv6 Reconfigure Messages

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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6644.

Table of Contents

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 specification defined in RFC 3315 is suitable only for scenarios in which the client would communicate with the same DHCPv6 servers.

There are also scenarios where the client must communicate with a different server; for example, a network administrator may choose to shut down a DHCPv6 server and move the clients who most recently communicated with it to a different server. Hence, this document expands the allowed values of the message type field within the reconfiguration message to allow the server to indicate to 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].

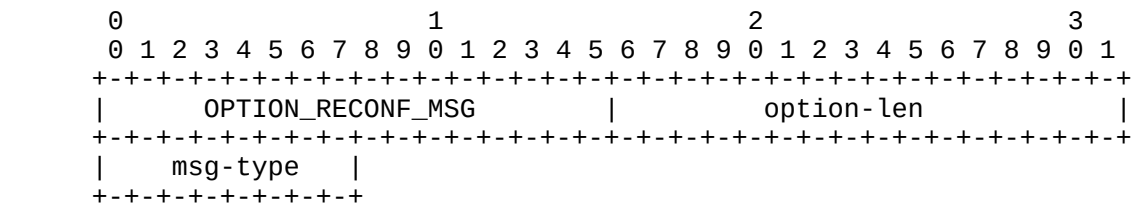
This document uses IPv6 and DHCPv6 terms as defined in Section 4 of [RFC3315].

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:



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 of RFC 6644) 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 identity associations (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 of RFC 6644). 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 with which the client most recently communicated.

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 [SEC-DHCPv6], based on Cryptographically Generated Addresses (CGA) [RFC3972], can provide source address (for the DHCP server/relay) ownership validation, message origin authentication, and message integrity without requiring symmetric key pairs or support from a key management system.

8. Acknowledgements

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

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

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

9.2. Informative References

[SEC-DHCPv6] Jiang, S. and S. Shen, "Secure DHCPv6 Using CGAs", Work in Progress, March 2012.

Authors' Addresses

D. R. Evans
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