

dhc Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: December 30, 2015

S. Gandhewar  
Juniper Networks, Inc.  
June 28, 2015

DHCPv6 Relay Initiated Release  
draft-gandhewar-dhc-v6-relay-initiated-release-00

Abstract

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is initiated by a DHCPv6 client. A DHCPv6 server can force DHCPv6 client to send RENEW or INFORMATION-REQUEST by sending a RECONFIGURE message. There may be multiple DHCPv6 network devices connected in between a DHCPv6 client and a server, each one reserving resources for the DHCPv6 client. There are no DHCPv6 messages that a relay can initiate in order to control the client binding.

A DHCPv6 client may not always send a RELEASE message when it no longer needs the IPv6 address. This document specifies a way to request release to be initiated by an intermediate DHCPv6 network device, e.g. DHCPv6 relay, on behalf of DHCPv6 client. This helps to relinquish network resources sooner than the lease expiration time.

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 December 30, 2015.

Copyright Notice

Copyright (c) 2015 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 . . . . .	4
3.	Protocol Details . . . . .	4
3.1.	Message Definitions . . . . .	4
3.1.1.	RELEASE-REQUEST . . . . .	4
3.1.2.	RELEASE-REQUEST-REPLY . . . . .	4
3.2.	Message Validation . . . . .	5
3.2.1.	RELEASE-REQUEST . . . . .	5
3.2.2.	RELEASE-REQUEST-REPLY . . . . .	5
4.	Functionality . . . . .	6
4.1.	First DHCPv6 Network Device Behavior . . . . .	6
4.1.1.	Generation and Transmission of RELEASE-REQUEST Message . . . . .	6
4.2.	Intermediate DHCPv6 Network Device Behavior . . . . .	7
4.3.	DHCPv6 Server Behavior . . . . .	7
4.4.	Receipt of RELEASE-REQUEST-REPLY . . . . .	8
5.	Security Considerations . . . . .	8
6.	IANA Considerations . . . . .	9
7.	References . . . . .	9
7.1.	Normative References . . . . .	9
7.2.	Informative References . . . . .	9
	Author's Address . . . . .	10

## 1. Introduction

DHCPv6 [RFC3315] provides a framework for configuring clients with network addresses and other network parameters. It includes a relay agent capability where DHCPv6 server may not be directly connected to the DHCPv6 client. A relay agent is an intermediate node that passes DHCPv6 messages between DHCPv6 clients and DHCPv6 servers. As per [RFC3315], a relay agent cannot generate a message on its own which can control the client binding. Figure 1 below shows a typical network with multiple DHCPv6 devices.

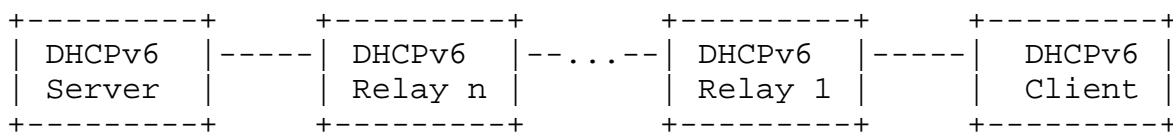


Figure 1: Typical DHCPv6 Network

A DHCPv6 client may be connected to DHCPv6 server through multiple DHCPv6 network devices, e.g. multiple DHCPv6 relays. In the DHCPv6 protocol it is not mandatory for the DHCPv6 client to send a RELEASE message while disconnecting. It is also possible that the UDP datagram carrying a RELEASE message may get dropped due to network issues. Network resources, including IPv6 address, may remain reserved for this client at all the DHCPv6 network devices until the lease expires.

In some situations when the DHCPv6 client is replaced (e.g. replacing the set-top-box) due to failure, the first DHCPv6 client may not have sent the RELEASE message on its failure. In this case, the IPv6 address and network resources for the first client will be reserved and unused until the lease expires.

It is possible for the first DHCPv6 network device, i.e. "DHCPv6 Relay 1" in Figure 1 which is closest to the DHCPv6 client, to detect that the DHCPv6 client is replaced or is no longer present on the network by a health check. This health check may be done by some kind of liveness detection mechanism or some other mechanism. In this scenario, the relay agent doesn't have any mechanism to inform the server about such liveness state.

In some situations, the administrator might want to clear some clients' bindings administratively. In such cases, the administrator may need to access every single DHCPv6 network device (relay, relay-proxy) and also the DHCPv6 server, and clear the DHCPv6 client binding.

With the relay initiated release message, when a relay detects client's unavailability or needs to clear the client binding administratively, it can generate the release message on behalf of client and send it to the server. Thus, all of the DHCPv6 network devices can be in synchronization with respect to the client's binding information and network resources can be relinquished earlier than the lease expiry. The server MAY choose to integrate some mechanism to confirm with the client, e.g. generate RECONFIGURE message before sending reply to the relay. It is outside the scope of this document.

## 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 RFC 2119 [RFC2119].

## 3. Protocol Details

### 3.1. Message Definitions

This document specifies 2 new DHCPv6 message types:

- o RELEASE-REQUEST
- o RELEASE-REQUEST-REPLY

#### 3.1.1. RELEASE-REQUEST

This is the relay initiated release request message. The format of the RELEASE-REQUEST is same as the Client/Server message formats described in Section 6 of [RFC3315].

The RELEASE-REQUEST message MAY be generated by the first DHCPv6 network device ("DHCPv6 Relay 1" in Figure 1), on behalf of the DHCPv6 client. The RELEASE-REQUEST message contains one or more Client Data Options as described in Section 4.1.2.2 of [RFC5007], requesting release for one or more clients.

The RELEASE-REQUEST message MUST contain the Server Identifier Option. It MAY contain Interface-Id Option indicating common values for all the clients requesting the release. This reduces the redundant data when there are multiple clients with common information.

Each Client Data Option MUST include the Client Identifier Option OPTION\_CLIENTID. It MUST also include options containing the IAs - OPTION\_IAADDR, OPTION\_IAPREFIX, etc. - for the addresses it is releasing. If the Interface-Id option is different from the one included directly under RELEASE-REQUEST message then it MUST be included here.

#### 3.1.2. RELEASE-REQUEST-REPLY

This is the reply for the RELEASE-REQUEST message. The format of the RELEASE-REQUEST-REPLY is same as the Client/Server message formats described in Section 6 of [RFC3315].

The message RELEASE-REQUEST-REPLY will be generated by the DHCPv6 Server to communicate the status of the request. The server conveys the success or failure of the RELEASE-REQUEST by including Status Code Option at different levels:

- o Status Code Option directly inside RELEASE-REQUEST: Indicates success or failure of the complete RELEASE-REQUEST message.
- o Status Code Option inside Client Data Option: Indicates failure to release all the addresses for a particular client. Client Data Option MUST include the Client-Id Option.
- o Status Code Option inside IA Option: Indicates failure to release a particular address for a particular client. Client Data Option MUST include the Client-Id Option and the IA option.

The RELEASE-REQUEST-REPLY message MAY contain one or more Client Data Options, described in Section 4.1.2.2 of [RFC5007], responding to the request to release for each of the clients.

The RELEASE-REQUEST-REPLY message SHOULD contain the Interface-Id option if it was included in RELEASE-REQUEST message.

## 3.2. Message Validation

### 3.2.1. RELEASE-REQUEST

Clients MUST silently discard any received RELEASE-REQUEST messages.

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

- o The message does not include a Client Data Option.
- o The Client Data Option does not include a Client Identifier Option.
- o The message includes a Server Identifier Option but the contents of the Server Identifier Option do not match the server's identifier.

### 3.2.2. RELEASE-REQUEST-REPLY

Clients MUST silently discard any received RELEASE-REQUEST-REPLY messages.

Servers MUST silently discard any received RELEASE-REQUEST-REPLY messages.

Relay MUST discard any received RELEASE-REQUEST-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 RELEASE-REQUEST message.
- o The message does not include a Status Code Option.

#### 4. Functionality

The generation of a RELEASE-REQUEST message can be a configurable behavior at DHCPv6 network device. Similarly, taking action to release the binding can also be a configurable behavior at the DHCPv6 server and intermediate DHCPv6 network devices.

##### 4.1. First DHCPv6 Network Device Behavior

Devices MAY be configured to generate the newly defined RELEASE-REQUEST message.

The first DHCPv6 network device ("DHCPv6 Relay 1" in Figure 1) can be configured such that when it detects the client is no longer available on the network or is replaced or the binding information needs to be deleted administratively, the device can generate the RELEASE-REQUEST message.

In order to generate the RELEASE-REQUEST message this network device needs to store the information related to the client, e.g. the client identifier and the server identifier used while obtaining the client lease.

##### 4.1.1. Generation and Transmission of RELEASE-REQUEST Message

Set the "msg-type" field to RELEASE-REQUEST.

Generate a transaction ID and insert it in the "transaction-id" field.

MUST include Server-Id Option.

MAY include Relay-Id option [RFC5460].

If configuration allows, relay MAY choose to add Interface-Id option [RFC3315].

Include one or more Client Data Options each one containing:

- o Client identifier MUST be included and SHOULD be same as what was used when client obtained the lease.
- o Include options containing the IAs for the addresses it is requesting to be released.
- o If the configuration allows, the relay MAY choose to add Interface-Id option [RFC3315] if it is different from the one included outside of the Client Data Option

Because RELEASE-REQUEST messages MAY be lost, the message SHOULD be retransmitted if no RELEASE-REQUEST-REPLY message is received. The client transmits the message according to Section 14 of [RFC3315], using the following parameters:

- o IRT REL\_TIMEOUT
- o MRT 0
- o MRC REL\_MAX\_RC
- o MRD 0

If RELEASE-REQUEST-REPLY from a DHCP server is lost, then the RELEASE-REQUEST will be retransmitted, and the server MAY respond with a RELEASE-REQUEST-REPLY indicating a status as NoBinding. Therefore, in this message exchange, the relay SHOULD NOT treat a RELEASE-REQUEST-REPLY message with a status of NoBinding as an error.

#### 4.2. Intermediate DHCPv6 Network Device Behavior

The behavior of the intermediate DHCPv6 network device can be configured to either accept or reject these messages. On accepting, it can forward the messages as specified in Section 20.1 and 20.2 of [RFC3315].

#### 4.3. DHCPv6 Server Behavior

DHCPv6 server ("DHCPv6 Server" in Figure 1) SHOULD be configurable to either accept or reject the relay initiated release message RELEASE-REQUEST. Upon receipt of a RELEASE-REQUEST message, the server MUST confirm the validity of the message.

If server does not support the new message type then it MAY simply drop the packet.

If the server is not configured to accept this relay initiated RELEASE-REQUEST message then it MAY simply drop the packet or send RELEASE-REQUEST-REPLY with status as NotConfigured.

If the server decides not to accept the RELEASE-REQUEST from a particular relay, it MAY simply drop the packet or send RELEASE-REQUEST-REPLY with status as NotAllowed.

The server SHOULD iterate through each of the Client Data Options and examine the Client-Id and the addresses in the IAs for validity. If the addresses in the IAs have been assigned by the server, the server deletes the binding of these addresses and makes the addresses available for assignment to other clients. Server keeps note of these addresses in the IAs for generating the RELEASE-REQUEST-REPLY.

After all of the clients have been processed, the server generates a RELEASE-REQUEST-REPLY message and includes a Status Code Option with value Success. It also includes Server Identifier option.

For each of the clients where there is a failure in releasing addresses, server MUST include Client Data Option. In the Client Data Option, it MUST include the Client Identifier option from the RELEASE-REQUEST message. It MUST also include Status Code Option for each of the failed IAs from the RELEASE-REQUEST message. For the clients or IAs for which the server has no binding information, correspondingly, the server MUST include a Status Code Option with the value NoBinding. No other options are included in the IA option.

#### 4.4. Receipt of RELEASE-REQUEST-REPLY

The first DHCPv6 network device ("DHCPv6 Relay 1" in Figure 1), upon receipt of a valid RELEASE-REQUEST-REPLY message, considers the completion of RELEASE-REQUEST event. The action at this device is based on the status. For all of the IAs or clients where the Status Code is not Success or NoBinding, addresses remain unchanged until the lease expires. For all other clients and IAs, bindings MUST be cleared.

### 5. Security Considerations

In order to prevent using RELEASE-REQUEST messages as a denial-of-service attack on the DHCPv6 servers, DHCPv6 relay agents SHOULD combine release requests for multiple clients in one RELEASE-REQUEST as explained in Section Section 4.1.1.

Because the RELEASE-REQUEST message provides a mechanism for releasing the client binding, it can be the cause of security threats. 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 a 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 messages.

DHCPv6 servers MUST silently discard RELEASE-REQUEST messages originating from unknown or untrusted relay agents or reject the RELEASE-REQUEST. Section Section 4.3 specifies the error code to return when the server is configured to reject RELEASE-REQUEST messages.

## 6. IANA Considerations

We request IANA to assign following new message types from the registry of Message Types maintained in:

<http://www.iana.org/assignments/dhcpv6-parameters/>

- o RELEASE-REQUEST
- o RELEASE-REQUEST-REPLY

## 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.

### 7.2. Informative References

[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.

[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.

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

Author's Address

Sunil M. Gandhewar  
Juniper Networks, Inc.

Email: [sgandhewar@juniper.net](mailto:sgandhewar@juniper.net)