dhc Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 3, 2016

S. Gandhewar
Juniper Networks, Inc.
October 1, 2015

# DHCP Relay Initiated Release
## draft-gandhewar-dhc-relay-initiated-release-01

Abstract

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

A DHCP client may not always send a DHCPRELEASE message when it no longer needs the IP address and network resources for the associated services it is using. This document specifies a way to request release message to be initiated by an intermediate DHCP network device, e.g. DHCP relay, on behalf of DHCP client. This helps to relinquish network resources sooner than the lease expiration time.

Table of Contents



## 1. Introduction

DHCP [RFC2131] provides a framework for configuring clients with network addresses and other network parameters. It includes a relay agent capability where DHCP server may not be directly connected to the DHCP client. A relay agent is an intermediate node that passes DHCP messages between DHCP clients and DHCP servers. As per [RFC2131], 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 DHCP devices.

```
+---------+     +---------+       +---------+     +---------+
|  DHCP   |-----|  DHCP   |--...--|  DHCP   |-----|  DHCP   |
| Server  |     | Relay n |       | Relay 1 |     |  Client |
+---------+     +---------+       +---------+     +---------+
```

Figure 1: Typical DHCP Network

While providing an IP address to the DHCP Client, Service Providers (e.g. Broadband Service Providers), creates a logical interface per client, programs various routes (e.g. access routes, framed routes) for the client to access the network and services, attaches services (e.g. voice, video, data), maintains policy, applies QoS. Along with these resources there is a need for memory and bandwidth per client. Since all these resources are limited on a network device (e.g. Broadband Network Gateway), it defines the scaling capacity of the device. Subscription rate for the Service Providers is thus limited by the availability of the IP addresses as well as the resources on their network device.

A DHCP client may be connected to the DHCP server through multiple DHCP network devices, e.g. multiple DHCP relay and/or relay-proxy. These network resources remain reserved for the client at all the DHCP network devices until the lease expires.

In some situations, there might be need to clear the client binding administratively. The process of administratively clearing the client binding is very cumbersome. The administrator needs to access every single DHCP network device (relay, relay-proxy) and also the DHCP server, and clear the DHCP client binding at each of these devices manually.

In some situations when the DHCP client is replaced (e.g. replacing the set-top-box) due to the device failure or upgrade, the older DHCP client might not have sent the DHCPRELEASE message on its failure. In this case, the previously assigned IP address and network resources for the older (stale) client will stay reserved and unused until the lease expires.

Same is the situation where clients move frequently without sending DHCPRELEASE e.g. in the case of mobile networks, network resources stay reserved and unused. Similarly, network resources stay reserved and unused where DHCP clients login and logout frequently without sending DHCPRELEASE e.g. Wi-Fi access centers.

As per DHCP protocol it is not mandatory for the DHCP client to send a DHCPRELEASE message while disconnecting. As per the statistics from Service Providers, 95% of the cases DHCP client does not send DHCPRELEASE message when it no longer needs the service. It is also possible that the UDP datagram carrying a DHCPRELEASE message may get dropped due to network issues.

All the resources including the IP address remain reserved for the client at all the DHCP network devices until the lease expires. Service Providers needs to take into account such situations and are forced to lower the subscription rate. Thus it reduces the scaling per network device. Also it causes errors for the time based billing.

It is possible for the first DHCP network device, i.e. "DHCP Relay 1" in Figure 1 which is closest to the DHCP client, to detect that the DHCP client is replaced, moved or is no longer present on the network. In this scenario, the relay agent doesn’t have any mechanism to inform the server to release the client’s binding and subsequently relinquish network resources.

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 the client and send it to the server. Thus, all the DHCP network devices along the path will 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 FORCERENEW message before sending reply to the relay. It is outside the scope of this document.

Generation of the relay initiated release SHOULD be a configurable behavior at the first relay. The configuration at Relay SHOULD be further granular to indicate the situation under which relay should initiate the release e.g. administratively clearing DHCP binding, client replaced, client moved, client unavailable, etc.

Forwarding of the relay initiated release related messages SHOULD be a configurable behavior at the intermediate DHCP network devices.

Acceptance of relay initiated release SHOULD also be a configurable behavior at the server.

## 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].

## 3. New Message and Option Value Definitions

This document specifies 2 new DHCP message types (option 53 from Section 9.6 of [RFC2132]):

- o DHCPRELEASEBYRELAY
- o DHCPRELAYREPLY

The format of these messages is same as defined in [RFC2131].

This document specifies 2 new values for the Status Code Option (option 151 from Section 6.2.2 of [RFC6926]):

- o NoBinding
- o NotConfigured

### 3.1. DHCPRELEASEBYRELAY

This message MAY be generated by the first DHCP network device ("DHCP Relay 1" in Figure 1), on behalf of the DHCP client. This gives an indication to the server that the client binding can be cleared.

### 3.2. DHCPRELAYREPLY

This is the reply from DHCP server in response to the DHCPRELEASEBYRELAY message. The server conveys success or failure of the DHCPRELEASEBYRELAY.

### 3.3. NoBinding

When the server does not find the binding for which DHCPRELEASEBYRELAY is received, it uses this new value in the Status Code Option.

### 3.4. NotConfigured

When the server is not configured to accept DHCPRELEASEBYRELAY, it uses this new value in the Status Code Option.

## 4. Functionality

The generation of a DHCPRELEASEBYRELAY message SHOULD be a configurable behavior at the DHCP relay. Taking action to release the binding SHOULD also be a configurable behavior at the server and intermediate DHCP network devices. Depending upon the configuration, the server responds with DHCPRELAYREPLY

### 4.1. First DHCP Network Device Behavior

Devices MAY be configured to generate the newly defined DHCPRELEASEBYRELAY message.

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

In order to generate the DHCPRELEASEBYRELAY message this network device needs to store the information related to the client, e.g. hardware address, client identifier, server identifier and giaddr used while obtaining client lease.

#### 4.1.1. Generation and Transmission of DHCPRELEASEBYRELAY Message

This new message is similar to the DHCPRELEASE generated by the client, as explained in [RFC2131]. The construction of the DHCPRELEASEBYRELAY is similar to the construction of any other DHCP messages as described in Section 4.1 of [RFC2131]. Note that this message is generated on behalf of the DHCP client hence all the fields in the message MUST be with respect to the client, as if it was generated by the client.

Set the following fields in the DHCPRELEASEBYRELAY message:

- op - MUST be set to BOOTREQUEST

- xid - MUST be filled as a random number

- chaddr - MUST be filled with hardware address of the client on whose behalf the DHCPRELEASEBYRELAY is being sent

- ciaddr - MUST be filled with client’s network address

- giaddr - MUST be filled and SHOULD be same as what was used when client obtained the lease

Include the following options in the DHCPRELEASEBYRELAY message:

- DHCP message type - MUST be included as DHCPRELEASEBYRELAY

- Client identifier - if the client had used this option while obtaining the lease, it MUST include this option with the same value

- o Server identifier - MUST be included and SHOULD be same as what was used when client obtained the lease

- o Relay Agent Information Option 82 - MAY include this option [RFC3046] with the same value as what was used while obtaining the lease

DHCPRELEASEBYRELAY SHOULD be sent as unicast message to the server.

#### 4.1.2. Receipt of DHCPRELEASEBYRELAY Message

In order to protect against spoofed DHCPRELEASEBYRELAY messages attempting to disconnect the clients, the first DHCP network device SHOULD drop any received DHCPRELEASEBYRELAY messages. It MUST be a configurable behavior if these messages are from the trusted sources and needs to be forwarded to the server.

#### 4.1.3. Receipt of DHCPRELAYREPLY Message

If xid of the DHCPRELAYREPLY does not match with the xid of the DHCPRELEASEBYRELAY which was sent, DHCPRELAYREPLY MUST be silently dropped.

The first DHCP network device ("DHCP Relay 1" in Figure 1), upon receipt of a valid DHCPRELAYREPLY message from the server, considers the completion of DHCPRELEASEBYRELAY event.

The action at this device is based on the Status Code Option. In the absence of Status Code Option or if the value is Success or NoBinding, then this device MUST clear the binding. If the Status Code is not Success or NoBinding, those client bindings MUST remain until the lease expires.

If DHCPRELAYREPLY from the DHCP server is lost then the DHCPRELEASEBYRELAY will be retransmitted, and the server MAY respond with a DHCPRELAYREPLY indicating a Status Code as NoBinding. Therefore, in this message exchange, the relay SHOULD NOT treat a DHCPRELAYREPLY message with a Status Code of NoBinding as an error.

#### 4.1.4. Receiving No Response

The DHCP relay does not receive a response from the server if the DHCPRELEASEBYRELAY or DHCPRELAYREPLY message is lost. In such cases, relay SHOULD resend the DHCPRELEASEBYRELAY message to the server using a backoff algorithm for the retry time that approximates an exponential backoff. Depending on the network bandwidth between the relay and the server, the relay SHOULD choose a delay. This delay grows exponentially as retransmissions fail. The number of retransmissions SHOULD be limited.  The exponential backoff algorithm is specified in Section 4.1 of [RFC3046].

### 4.2.  DHCP Server Behavior

DHCP server ("DHCP Server" in Figure 1) SHOULD be configurable either to accept or reject the newly defined DHCPRELEASEBYRELAY message.

#### 4.2.1.  Receipt of DHCPRELEASEBYRELAY Message

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

If the server is not configured to accept this relay initiated DHCPRELEASEBYRELAY message then it can simply drop the packet or send DHCPRELAYREPLY with status code as NotConfigured.

The server MAY be configured to restrict itself from accepting this message with the same giaddr which was used while obtaining the lease (DISCOVER-OFFER_REQUEST-ACK message exchange).  If server decides not to accept the DHCPRELEASEBYRELAY message from a particular relay, it can simply drop the packet or send DHCPRELAYREPLY with status code as NotAllowed.

On receipt of a valid and acceptable DHCPRELEASEBYRELAY message, if configuration allows, server MAY decide to clear the binding as explained in Section 4.3.4 of [RFC2131].  Server MUST send a DHCPRELAYREPLY message to the relay.

If the server does not find the binding for which it received the DHCPRELEASEBYRELAY message, it MUST send the DHCPRELAYREPLY with status code as Nobinding.

#### 4.2.2.  Generation and Transmission of DHCPRELAYREPLY Message

Construction of the DHCPRELAYREPLY is similar to construction of any other DHCP messages as described in Section 4.1 of [RFC2131].  This message is similar to DHCPACK which is generated by the server, as explained in [RFC2131].

Set the following fields in the DHCPRELAYREPLY message:

o  op - MUST be set to BOOTREPLY

o  xid - MUST be copied from DHCPRELEASEBYRELAY

o  chaddr - MUST be copied from DHCPRELEASEBYRELAY

- o ciaddr - MUST be filled with client’s network address

- o giaddr - MUST be copied from DHCPRELEASEBYRELAY

Include the following options in the DHCPRELAYREPLY message:

- o DHCP message type - MUST be included as DHCPRELAYREPLY

- o Client identifier - MUST be copied from DHCPRELEASEBYRELAY

- o Server identifier - MUST be copied from DHCPRELEASEBYRELAY

- o Relay Agent Information Option 82 - if present, MUST be copied from DHCPRELEASEBYRELAY

- o Status Code - MAY include the option depending upon the result

DHCPRELAYREPLY MUST be sent as unicast message to the address of the relay as recorded in DHCPRELEASEBYRELAY.

## 5. Security Considerations

DHCP protocol as defined in [RFC2131] provides no authentication or security mechanisms. Potential exposure to attacks are discussed in Section 7 of the DHCP protocol specification in [RFC2131]. Unauthorized and malicious network device MAY spoof and send the false DHCPRELEASE message. Similarly unauthorized and malicious network device MAY spoof and send the false DHCPRELEASEBYRELAY message.

A defense using the authentication for DHCP messages [RFC3118] SHOULD be deployed where the networks are not secure or not directly under the control of the server administrator. The DHCPRELEASEBYRELAY and DHCPRELAYREPLY messages SHOULD be authenticated using the procedures described in [RFC3118]. However, implementation of authentication is not a MUST to support DHCPRELEASEBYRELAY and DHCPRELAYREPLY messages.

Although DHCP network devices that send the DHCPRELEASEBYRELAY message perform the functions of a DHCP relay, essentially they are DHCP clients for the purposes of the DHCPRELEASEBYRELAY message. Thus, [RFC3118] is an appropriate mechanism for DHCPRELEASEBYRELAY message authentication.

Since [RFC3118] discusses the normal DHCP client interaction, consisting of a DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK, it is necessary to transpose the operations described in [RFC3118] to the DHCPRELEASEBYRELAY domain. The operations described in [RFC3118] for DHCPDISCOVER are performed for DHCPRELEASEBYRELAY, and the operations described for DHCPOFFER are performed for DHCPRELAYREPLY message.

## 6. IANA Considerations

We request IANA to assign following new message types from the registry of Message Types 53 Values maintained in: http://www.iana.org/assignments/bootp-dhcp-parameters/

- o DHCPRELEASEBYRELAY

- o DHCPRELAYREPLY

We request IANA to assign following new Status Code values from the registry of Status Codes Type 151 Values maintained in: http://www.iana.org/assignments/bootp-dhcp-parameters/

- o NoBinding

- o NotConfigured

## 7. Acknowledgements

We would like to acknowledge Utae Kim (Smart GiGA Network Project, Korea Telekom), Dan Seibel (Sr.  Engineer, TELUS), Ian Farrer (Network Architect, Deutsche Telekom) and Chris Topazi (Access Engineering, Cox Communications) for their valuable contributions, suggestions and support for this document.

We would like to thank Bernie Volz, Ted Lemon, Andrew Sullivan, Ole Troan and Shrivinas Joshi for their valuable comments and suggestions for improving the document.

Many thanks to Tomek Mrugalski, Bernie Volz and Jaya Bhawtankar (Lead Engineer, Coriant) for their support.

We would like to acknowledge Anand Vijayvergiya, Jeff Haas and Ross Callon for their guidance and tirelessly reviewing the document multiple times.

## 8. References

### 8.1. Normative References

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

## 8.2. Informative References


[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <http://www.rfc-editor.org/info/rfc2132>.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, DOI 10.17487/RFC3046, January 2001, <http://www.rfc-editor.org/info/rfc3046>.

[RFC3118] Droms, R. and W. Arbaugh., Ed., "Authentication for DHCP Messages", RFC 3118, DOI 10.17487/RFC3118, June 2001, <http://www.rfc-editor.org/info/rfc3118>.

[RFC6926] Kinnear, K., Stapp, M., Desetti, R., Joshi, B., Russell, N., Kurapati, P., and B. Volz, "DHCPv4 Bulk Leasequery", RFC 6926, DOI 10.17487/RFC6926, April 2013, <http://www.rfc-editor.org/info/rfc6926>.


## Author’s Address


Sunil M. Gandhewar
Juniper Networks, Inc.

Email: sgandhewar@juniper.net