

dhc	T. Lemon
Internet-Draft	Nominum
Updates: 3315 (if approved)	Q. Wu
Intended status: Standards Track	Huawei
Expires: March 09, 2012	September 06, 2011

Relay-Supplied DHCP Options

draft-ietf-dhc-dhcpv6-relay-supplied-options-09

Abstract

DHCPv6 relay agents can not communicate with DHCPv6 clients directly. However, in some cases, the relay agent possesses some information that would be useful to the DHCPv6 client. This document describes a mechanism whereby the DHCPv6 relay agent can provide such information to the DHCPv6 server, which can, in turn, pass this information on to the DHCP client.

This document updates RFC3315 (DHCPv6) by making explicit the implicit requirement that relay agents not modify the content of encapsulation payloads as they are relayed back toward clients.

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 March 09, 2012.

Copyright Notice

Copyright (c) 2011 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](#)
- *1.1. [Requirements Language](#)
- *1.2. [Terminology](#)
- *2. [Protocol Summary](#)
- *3. [Encoding](#)
- *4. [RS00-enabled options](#)
- *5. [DHCP Relay Agent Behavior](#)
- *6. [DHCP Server Behavior](#)
- *7. [Security Considerations](#)
- *8. [IANA Considerations](#)
- *9. [References](#)
- *9.1. [Normative References](#)
- *9.2. [Informative References](#)
- *[Authors' Addresses](#)

1. Introduction

The DHCPv6 specification [\[RFC3315\]](#) allows DHCP relay agents to forward DHCPv6 messages between clients and servers that are not on the same IPv6 link. In some cases the DHCP relay agent has information not available to the DHCP server that would be useful to provide to a DHCP client. For example, the DHCP client may need to learn the EAP local domain name [\[I.D-ietf-hokey-ldn-discovery\]](#) for use in EAP re-authentication [\[RFC5296\]](#), which is known to the relay agent but not the server.

The DHCPv6 protocol specification does not provide a mechanism whereby the relay agent can provide options to the client. This document extends DHCP with a mechanism that allows DHCP relay agents to propose options for the server to send to DHCP clients.

This document is not intended to provide a general mechanism for storing client configuration information in the relay agent. Rather, it is intended to address specific use cases where only the relay agent has information needed by the client. This extension is not applicable to DHCP options in general, but rather provided as a mechanism for new specifications that require this functionality.

1.1. 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].

1.2. Terminology

The following terms and acronyms are used in this document:

DHCP Dynamic Host Configuration Protocol Version 6 [\[RFC3315\]](#)

RS00 Relay-Supplied Options option

2. Protocol Summary

DHCP clients do not support a mechanism for receiving options from relay agents--the relay agent is required to deliver the payload from the DHCP server to the DHCP client without changing it. In order for the DHCP relay agent to provide options to the client, it sends those options to the DHCP server, encapsulated in a Relay-Supplied Options option. The DHCP server can then choose to place those options in the response it sends to the client.

3. Encoding

In order to supply options for the DHCP server to send to the client, the relay agent sends a Relay-Supplied Options option in the Relay-Forward message. This option encapsulates whatever options the relay agent wishes to provide to the DHCPv6 server.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                               |                               |
|      OPTION_RS00             |      option-length             |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                               |
|      options...              |
+--+--+--+--+--+--+--+--+--+--+
```

OPTION_RS00

Relay-Supplied Options code (TBD).

option-length

Length of Relay-Supplied Options option.

options

One or more DHCPv6 options.

4. RS00-enabled options

The RS00 MUST NOT contain any option that is not specifically called out as an RS00-enabled option. Specifications that describe RS00-enabled options MUST reference this specification, and MUST state that the option they define is RS00-enabled. No DHCP option specified prior to the issuance of this specification is RS00-enabled.

A current list of RS00-enabled options can be found in the list titled "Options Permitted in the Relay-Supplied Options option" maintained at <http://www.iana.org/assignments/dhcpv6-parameters>.

DHCP option specifications that define RS00-enabled options MUST add text similar to the following to their IANA considerations section; "random relay option" should be replaced with the name of the option being defined in the specification:

*We request that IANA add the name "random relay option" to the registry titled "Options Permitted in the Relay-Supplied Options Option" maintained at <http://www.iana.org/assignments/dhcpv6-parameters>.

5. DHCP Relay Agent Behavior

Relay agents MAY include a Relay-Supplied Options option in the option payload of a Relay-Forward message being sent toward a DHCP server. When relaying the payload of Relay-Reply messages toward clients, Relay agents MUST NOT modify the payload.

Relay agents MUST NOT send non-RS00-enabled options in the Relay-Supplied Options option.

In order to allow network administrators to control the flow of RS00 options onto the network, relay agents that implement the Relay Supplied Options Option need to have a configuration parameter that determines to whether or not they will relay RS00-containing Relay-Forward messages.

Relay agents that have this configuration parameter and that are configured to disable forwarding of Relay-Forward messages that contain a Relay-Supplied Options option MUST silently discard any such message. Implementations that can be configured in this way MUST examine all Relay-Forward encapsulations, not just the outer encapsulation.

6. DHCP Server Behavior

DHCP servers that implement Relay-Supplied DHCP Options MUST examine each option contained in an RS00 to see if it is an RS00-enabled option. DHCP servers MUST silently discard any option contained in an RS00 that is not RS00-enabled. DHCP server implementations SHOULD have an administrator-configurable list of RS00-enabled options, so that new RS00-enabled options do not require software to be updated.

DHCP servers normally construct a list of options that are candidates to send to the DHCP client, and then construct the DHCP packet according to section 17.2.2 of [DHCPv6 \[RFC3315\]](#).

If the server implementing Relay-Supplied DHCP Options receives an RS00, it SHOULD add any options that appear in the RS00 for which it has no internal candidate to the list of options that are candidates to send to the DHCP client. The server SHOULD discard any options that appear in the RS00 for which it already has one or more candidates. Aside from the addition of options from the RS00, the DHCP server should then construct a DHCP packet as it normally would, and transmit it to the DHCP client as described in DHCPv6 [\[RFC3315\]](#).

DHCP servers may receive multiply-nested Relay-Forward messages containing conflicting values for options contained in Relay Supplied Options options in these messages.

When such a conflict exists, the DHCP server MUST choose no more than one of these options to forward to the client. The DHCP server MUST NOT forward more than one of these options to the client.

By default, the DHCP server MUST choose the innermost value--the value supplied by the relay agent closest to the DHCP client, to forward to the DHCP client.

DHCP server implementations MAY provide other heuristics for choosing which one of a set of such conflicting options to forward to the client, as long as the specified behavior is the default behavior.

[7. Security Considerations](#)

This document provides a mechanism whereby a relay agent can inject options into the response the DHCP server sends to the DHCP client. In general it is expected that RS00-enabled options will be specified because they only make sense when originating from the relay agent. This is true of existing use cases.

In the event that some new RS00-enabled option is specified that can originate from either the server or the relay agent, this should be addressed in the security considerations section of the document that specifies the use of that option.

In some environments, there is an interface on one side of which is the client, and zero or more routers, and on the other side of which is a network managed by a monolithic or effectively monolithic administrative entity. Nodes and routers on the client side of the interface are not controlled by this entity, and are considered "untrusted." Nodes and routers on the network side of this interface are considered trusted.

It is possible for a malicious node acting as a relay agent on the untrusted side of this interface to supply a Relay-Supplied Options option containing one or more RS00-enabled options that would override the same option or options that were provided by a relay agent on the trusted side of the interface.

In environments where this is a possibility, network administrators are advised to use relay agents that are capable of dropping Relay- Forward

messages containing the Relay-Supplied Options option, and are advised to configure those relays to drop such messages.

Note, however, that this will only be effective if the message from the DHCP server to the DHCP client is authenticated as specified in Section 21 of DHCP Version 6 [\[RFC3315\]](#), or using some similar mechanism.

Without this authentication, the malicious node on the untrusted portion of the network can simply modify the DHCP server's response in transit back to the DHCP client, and there is no way for the client to detect that this has happened.

[8. IANA Considerations](#)

IANA is requested to assign one new DHCPv6 option code from the registry of DHCP Option Codes maintained at <http://www.iana.org/assignments/dhcpv6-parameters>. The option code OPTION_RS00 will be assigned to the Relay-Supplied Options option.

IANA is also requested to create a new registry on the same assignments page, titled "Options Permitted in the Relay-Supplied Options Option". This registry will contain a list of DHCPv6 option codes from the DHCP Option Codes list at <http://www.iana.org/assignments/dhcpv6-parameters> as suboptions of the Relay-Supplied Options option. Currently, the list is empty. Options may be added to this list after IETF Review[\[RFC5226\]](#). IETF Review should include careful consideration of the security implications of allowing a relay agent to provide a value for the option being considered for addition to this registry. In the case where an IETF working group chartered to review DHCP protocol extensions exists, it is not sufficient for some other working group to review the registry addition.

[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., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, " Dynamic Host Configuration Protocol for IPv6 (DHCPv6) ", RFC 3315, July 2003.
[RFC5226]	Narten, T. and H. Alvestrand, " Guidelines for Writing an IANA Considerations Section in RFCs ", BCP 26, RFC 5226, May 2008.

[9.2. Informative References](#)

[I.D-ietf-hokey-ldn-discovery]	Zorn, G., Wu, Q. and Y. Wang, " The ERP Local Domain Name DHCPv6 Option ", Internet-Draft draft-ietf-hokey-ldn-discovery-10, April 2011.
[RFC5296]	

Narayanan, V. and L. Dondeti, " EAP Extensions for EAP Re-authentication Protocol (ERP) ", RFC 5296, August 2008.

Authors' Addresses

Ted Lemon Lemon Nominum
2000 Seaport Blvd Redwood City, CA 94063 USA Phone: +1 650 381 6000
EMail: mellon@nominum.com

Qin Wu Wu Huawei Technologies Co., Ltd. 101 Software Avenue, Yuhua
District Nanjing, Jiangsu 210012 China EMail: sunseawq@huawei.com