Internet Engineering Task Force (IETF)
Request for Comments: 6422
Updates: 3315
Category: Standards Track
ISSN: 2070-1721

T. Lemon
Nominum
Q. Wu
Huawei

December 2011

Relay-Supplied DHCP Options

Abstract

DHCPv6 relay agents cannot 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 RFC 3315 (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 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/rfc6422.

Table of Contents

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 Re-authentication Protocol (ERP) local domain name [RFC6440] 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:

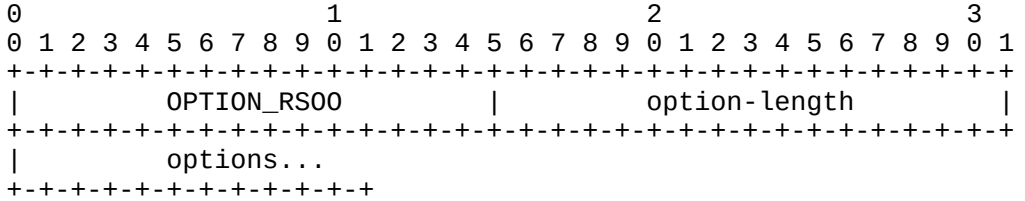
- DHCP: Dynamic Host Configuration Protocol Version 6 [RFC3315]
- RSOO: Relay-Supplied Options option

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 an RSOO. 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 an RSOO in the Relay-Forward message. This option encapsulates whatever options the relay agent wishes to provide to the DHCPv6 server.



OPTION_RSOO

Relay-Supplied Options code (66).

option-length

Length of the RSOO.

options

One or more DHCPv6 options.

4. RSOO-Enabled Options

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

A current list of RSOO-enabled options can be found in the list titled "Options Permitted in the Relay-Supplied Options Option" maintained at http://www.iana.org/.

DHCP option specifications that define RSOO-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/.

5. DHCP Relay Agent Behavior

Relay agents MAY include an RSOO 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-RSOO-enabled options in the Relay-Supplied Options option.

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

Relay agents that have this configuration parameter and that are configured to disable forwarding of a Relay-Forward message containing an RSOO 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 this protocol specification MUST examine each option contained in an RSOO to see if it is an RSOO-enabled option. DHCP servers MUST silently discard any option contained in an RSOO that is not RSOO-enabled. DHCP server implementations SHOULD have an administrator-configurable list of RSOO-enabled options, so that new RSOO-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 the DHCPv6 specification [RFC3315].

If the server implementing this protocol specification receives an RSOO, it SHOULD add any options that appear in the RSOO 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 RSOO for which it already has one or more candidates.

Aside from the addition of options from the RSOO, the DHCP server should then construct a DHCP packet as it normally would, and transmit it to the DHCP client as described in [RFC3315].

DHCP servers may receive multiply-nested Relay-Forward messages containing conflicting values for options contained in RSOOs 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 currently known use cases -- for example, the ERP Local Domain Option [RFC6440] -- RSOO-enabled options are options that will only ever originate on a relay agent, and do not make sense when originating on a DHCP server.

In the event that some new RSOO-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 an RSOO containing one or more RSOO-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 RSOO, and are advised to configure those relay agents 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 [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 has assigned one new DHCPv6 option code from the registry of DHCP Option Codes maintained at http://www.iana.org/. The option code 66 (OPTION_RSOO) has been assigned to the Relay-Supplied Options option.

IANA has created a new registry on the same assignments page, titled "Options Permitted in the Relay-Supplied Options Option". This registry will enumerate the set of all code points from the DHCP Option Codes table for options that may appear in the RSOO. Options may be added to this list after IETF Review [RFC5226]. When adding options to the list, please ensure that the description for the code added matches the description in the DHCP Option Codes table for that code. Option codes that have not been requested to be added according to the stated procedure should not be mentioned at all in the table, and should not be listed as "reserved" or "unassigned".

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., Ed., 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

[RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.

[RFC6440] Zorn, G., Wu, Q., and Y. Wang, "The EAP Re-authentication Protocol (ERP) Local Domain Name DHCPv6 Option", RFC 6440, December 2011.

Authors' Addresses

Ted Lemon
Nominum
2000 Seaport Blvd.
Redwood City, CA 94063
USA

Phone: +1 650 381 6000
EMail: mellon@nominum.com

Qin Wu
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Phone: +86-25-56623633
EMail: sunseawq@huawei.com