Softwire
Internet-Draft
Intended status: Standards Track
Expires: October 8, 2012

T. Mrugalski
ISC
P. Wu
Tsinghua University

April 6, 2012

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for DHCPv4 over IPv6 Transport

draft-mrugalski-softwire-dhcpv4-over-v6-option-00

Abstract

[I-D.ietf-dhc-dhcpv4-over-ipv6] defines a way for communication between legacy DHCPv4 clients with DHCPv4 servers over IPv6-only transport. It requires the deployment of Client Relay Agent (CRA) that transmits messages to IPv6-Transport Server (TSV) or IPv6-Transport Relay Agent (TRA). The deployed CRA must know the address of a TSV or TRA to forward incoming client's messages. This document defines an DHCPv6 option that may be used to provision the TSV or TRA location to CRAs.

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 October 8, 2012.

Copyright Notice

Table of Contents

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].

2. Introduction

[I-D.ietf-dhc-dhcpv4-over-ipv6] defines a way for communication between legacy DHCPv4 clients with DHCPv4 servers (defined in [RFC2131]) over IPv6-only transport. It requires the deployment of Client Relay Agent (CRA) that transmits messages to IPv6-Transport Server (TSV) or IPv6-Transport Relay Agent (TRA). There are several scenarios envisaged, all of them assume that CRA needs to know the recipient address of the DHCPv4-over-IPv6 traffic.

Depending on the scenario discussed, the DHCPv4 over IPv6 transport endpoint could be either an IPv6-Transport Server (TSV) or an IPv6-Transport Relay Agent (TRA). Both cases are indistinguishable from the CRA's perspective. CRA needs to know TSV's or TRA's IPv6 address in advance to relay traffic.

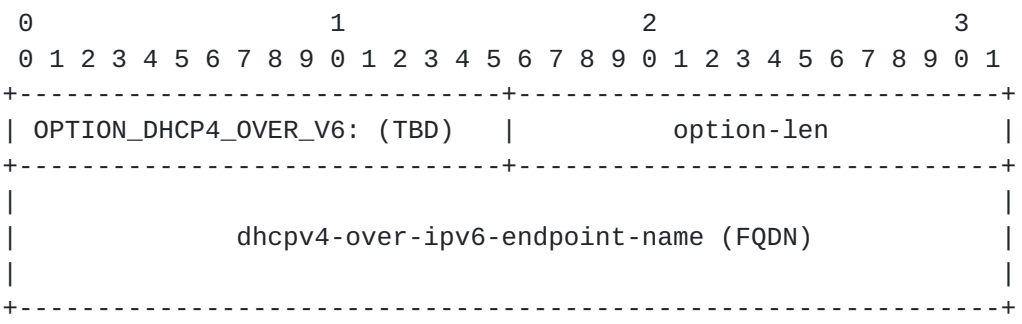
As the CRA uplink is IPv6-only (otherwise there would be no need to deploy DHCPv4 over IPv6), the only feasible way to provision information to CRA is over DHCPv6. Therefore this document specifies a DHCPv6 option that conveys the necessary information to CRA. To be more specific, a single DHCPv6 [RFC3315] option is used, expressing the TRA's or TSV's Fully Qualified Domain Name (FQDN) to the CRA.

3. The DHCPv4-Over-IPv6 DHCPv6 Option

The DHCPv4-over-IPv6 option is a DHCPv6 option. It consists of an option-code and option-len fields (as all DHCPv6 options have), and a variable length dhcpv4-over-ipv6-endpoint-name field containing a fully qualified domain name that refers to the DHCPv4 over IPv6 transport endpoint to which the CRA MAY transport DHCPv4 traffic. This name represents a TRA or TSV, depending on deployment scenario.

The DHCPv4-over-IPv6 option SHOULD NOT appear in any other than the following DHCPv6 messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request and Reply.

The format of the DHCPv4 over IPv6 option is shown in the following figure:



OPTION_DHCP4_OVER_V6: (TBD)

option-len: Length of the dhcpv4-over-ipv6-endpoint-name field, expressed in octets.

dhcpv4-over-ipv6-endpoint-name: A fully qualified domain name of the DHCPv4-over-IPv6 transport endpoint.

Figure 1: AFTR-Name DHCPv6 Option Format

The dhcpv4-over-ipv6-endpoint-name field is formatted as required in DHCPv6 [RFC3315] Section 8 ("Representation and Use of Domain Names"). Briefly, the format described uses a single octet noting the length of one DNS label (limited to at most 63 octets), followed by the label contents. This repeats until all labels in the FQDN are exhausted, including a terminating zero-length label. Any updates to Section 8 of DHCPv6 [RFC3315] also apply to encoding of this field. An example format for this option is shown in Figure 2, which conveys the FQDN "dhcp.example.com.".

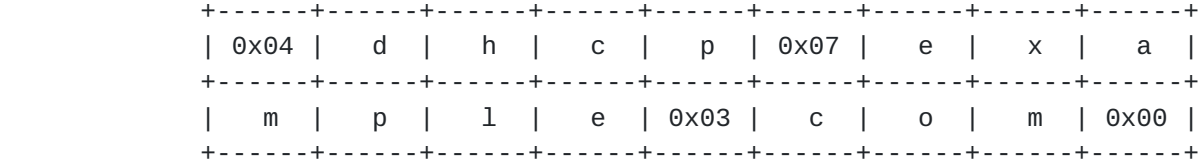


Figure 2: Example dhcpv4-over-ipv6-endpoint-name.

Note that in the specific case of the example (Figure 2), the length of the dhcpv4-over-ipv6-endpoint-name is 18 octets, and so an option-len field value of 18 would be used.

The option is validated by confirming that all of the following conditions are met:

1. the option-len is greater than 3;

2. the option data can be contained by the option length, and the option length does not run off the end of the packet;

3. the individual label lengths do not exceed the option length;

4. the dhcpv4-over-ipv6-endpoint-name is of valid format as described in DHCPv6 Section 8 [RFC3315];

5. there are no compression tags;

6. there is at least one label of nonzero length.

4. DHCPv6 Server Behavior

A DHCPv6 server SHOULD NOT send more than one DHCPv4-over-IPv6 option. It SHOULD NOT permit the configuration of multiple names within one DHCPv4-over-IPv6 option. Both of these conditions are handled as exception by the client, so an operator using software that does not perform these validations should be careful not to configure multiple domain names.

RFC 3315 Section 17.2.2 [RFC3315] describes how a DHCPv6 client and server negotiate configuration values using the Option Request Option (OPTION_ORO). As a convenience to the reader, we mention here that a server will not reply with a DHCPv4-over-IPv6 option if the client has not explicitly enumerated it in its Option Request Option. In other words, server SHOULD send this option only if client explicitly requested it in ORO.

5. DHCPv6 Client Behavior

A client that supports the DHCPv4 over IPv6 functionality and conforms to this specification MUST include OPTION_DHCP4_OVER_V6 on its OPTION_ORO.

Because it requires DNS name to address resolution, the client SHOULD also wish to include the OPTION_DNS_SERVERS [RFC3646] option on its OPTION_ORO.

If the client receives the DHCPv4-over-IPv6 option, it MUST verify the option contents as described in Section 3.

If the CRA entity receives more than one DHCPv4-over-IPv6 option, it MUST use only one instance of that option.

If the DHCPv4-over-IPv6 option contains more than one FQDN, as distinguished by the presence of multiple root labels, the CRA entity system MUST use only the first FQDN listed in configuration. It SHOULD warn its operator about such condition.

The CRA entity performs standard DNS resolution using the provided FQDN to resolve a AAAA Resource Record, as defined in [RFC3596] and STD 13 [RFC1034] [RFC1035].

If any DNS response contains more than one IPv6 address (probably for redundancy and high availability consideration), the CRA entity picks only one IPv6 address and uses it as a DHCPv4-over-IPv6 transport endpoint for the interface being configured in the current message exchange. The CRA system MUST NOT establish more than one transport at the same time per interface.

Note that a CRA system may have multiple network interfaces, and these interfaces may be configured differently; some may be connected to networks that call for DHCPv4-over-IPv6, and some may be connected to networks that are using normal dual stack or other means. The CRA entity should approach this specification on an interface-by-interface basis. For example, if the CRA entity is attached to multiple networks that provide the DHCPv4-over-IPv6 option, then the CRA entity MUST configure a DHCPv4 over IPv6 transport for each interface separately as each transport provides IPv4 connectivity for each distinct interface. Means to bind a DHCPv4-over-IPv6 transport configuration to a given interface in a multiple interfaces device are out of scope of this document.

6. Security Considerations

This document does not present any new security issues, but as with all DHCPv6-derived configuration state, it is completely possible that the configuration is being delivered by a third party (Man In The Middle). As such, there is no basis to trust the access the address of which is provisioned following this specification, and it should not therefore bypass any security mechanisms such as IP firewalls.

It should be noted that DHCPv4 over IPv6 traffic may bypass existing firewalls that are typically configured to drop incoming outside DHCPv4 over IPv4 and DHCPv6 over IPv6 traffic.

RFC 3315 [RFC3315] discusses DHCPv6-related security issues.

[RFC6333] discusses DS-Lite related security issues.

7. IANA Considerations

IANA is kindly requested to allocate DHCPv6 option code TBD to the OPTION_DHCP4_OVER_V6. The value should be added to the DHCPv6 option

code space defined in Section 24.3 of [RFC3315].

8. Acknowledgements

Authors would like to thank nobody so far, as we have not received any comments yet.

This work has been partially supported by the Polish Ministry of Science and Higher Education under the European Regional Development Fund, Grant No. POIG.01.01.02-00-045/09-00 (Future Internet Engineering Project).

9. Normative References

[I-D.ietf-dhc-dhcpv4-over-ipv6]
Cui, Y., Wu, P., Wu, J., and T. Lemon, "DHCPv4 over IPv6 Transport", draft-ietf-dhc-dhcpv4-over-ipv6-02 (work in progress), March 2012.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, 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.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

Authors' Addresses

Tomasz Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
USA

Phone: +1 650 423 1345
Email: tomasz.mrugalski@gmail.com

Peng Wu
Tsinghua University
Beijing 100084
P.R.China

Email: pengwu.thu@gmail.com