Dynamic Host Configuration
Internet-Draft
Intended status: Standards Track
Expires: 16 March 2025

C. Porfiri
Ericsson
S. Krishnan
Cisco
J. Arkko
M. Kühlewind
Ericsson
12 September 2024

DHCPv4-over-DHCPv6 (DHCP 4o6) ~~DHCPv4 over DHCPv6~~ with Relay Agent Support

draft-porfiri-dhc-dhcpv4-over-dhcpv6-ra-02

Abstract

This document describes a mechanism for networks with legacy IPv4-only clients to use services provided by DHCPv6 using DHCPv4-over-DHCPv6 (DHCP 4o6) in a Relay Agent. RFC 7341 specifies use of DHCPv4-over-DHCPv6 in the client only. This document specifies a RFC7341-based approach that allows DHCP 4o6 to be deployed as a Relay Agent (4o6RA) that implements the 4o6 DHCP en~~-~~capsulation and decapsulation ~~if~~in contexts where it ~~this~~ is not possible at the client.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-porfiri-dhc-dhcpv4-over-dhcpv6-ra/.

Source for this draft and an issue tracker can be found at https://github.com/mirjak/dhc-dhcpv4-over-dhcpv6-ra.

Commenté [MB1]: I got a 404 error message

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 https://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 16 March 2025.

Copyright Notice

Copyright (c) 2024 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 (https://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 Revised BSD License text as
described in Section 4.e of the Trust Legal Provisions and are
provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

[RFC7341] describes a transport mechanism for carrying DHCPv4 [RFC2131] messages using ~~the~~ DHCPv6 ~~protocol~~ [RFC8415] for the dynamic provisioning of IPv4 addresses and other DHCPv4 specific configuration parameters across IPv6-only networks. The deployment of [RFC7341] requires ~~implementation~~ support in ~~all~~ DHCP clients and at the DHCPv6 server.

However, if ~~the~~ a client is embedded in a host that only supports IPv4 and cannot easily be replaced or updated due to a number of technical or business reasons, this approach does not work.

Similarly, the specifications for DHCPv6 Relay Agents such as LDRA [RFC6221] or L3RA [RFC8415] do not foresee the possibility to handle legacy DHCP, other than implementing DHCP 4o6 in the client.

This document specifies an [RFC7341]-based solution that can be implemented in intermediate nodes such as ~~L2~~ switches or routers, without putting any requirements on clients. No new protocols or extensions are needed, instead this document specifies an amendment to [RFC7341] that allows a Relay Agent to perform the DHCP 4o6 ~~DHCP~~ en- and decapsultion instead of the client.

x. Applicability Scope

Commenté [MB2]: Consider adding an entry in the terminology section to say basically: DHCP=DHCPv4 and/or DHCPv6

Commenté [MB3]: I guess this is about DHCPv4

Commenté [MB4]: Please complete this section. Thanks.

2. Conventions and Definitions

The following terms and acronyms are used in this document:

* DHCPv4: Refers to DHCP as defined in [RFC2131]

* DHCPv4 over DHCPv6 (or 4o6): The architecture, the procedures, and the protocols described in the DHCPv4-over-DHCPv6 ~~document~~specification [RFC7341].

* DHCP Relay Agent (or RA): This is a concept in all of the protocols, BOOTP [RFC0951] [RFC1542], DHCPv4 [RFC2131] [RFC2132], and DHCPv6 [RFC8415], although the details differ between the protocols.

* Lightweight DHCPv6 Relay Agent (or LDRA): This is an extension of the original DHCPv6 Relay Agent ~~mechanism~~, to support also Layer 2 devices performing a Relay Agent function [RFC6221].

* DHCPv4 over DHCPv6 Relay Agent (or 4o6RA): ~~The 4o6 Relay Agent (as specified in this document) is the part of an~~Refers to a Relay Agent that ~~RA implementing~~ implement the 4o6 specified in this document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. DHCPv4 over DHCPv6 Relay Agent (4o6RA)

This document ~~assume~~ assumes ~~an~~ a network, where IPv4-only ~~clients~~ hosts are connected to ~~an~~ a ~~uplink~~ network that supports IPv6 ~~only~~ and limited IPv4 services.

To address such a network setup, this document ~~proposes to~~ extends DHCPv6 Relay Agents with ~~DHCPv4~~ DHCPv4-~~over~~ over-DHCPv6, as shown in Figure 1.

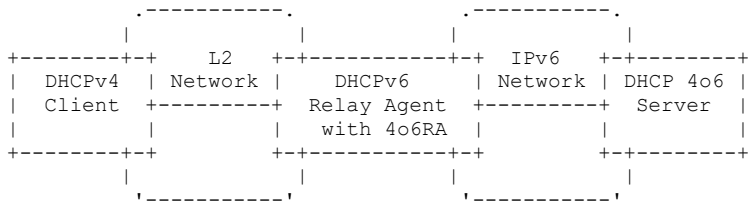

Figure 1: Architecture ~~Overview~~ Example with ~~legacy~~ Legacy DHCP ~~client~~Client

This document specifies the encapsulation and decapsulation described in [RFC7341] to be performed in the Relay Agent whereas the DHCPv4

Commenté [MB5]: As there is no «DHCPv4» as such.

Commenté [MB6]: I would avoid this acronym (as RA is widely used for Router Avertissements)

Commenté [MB7]: May be put some words to define it.

Commenté [MB8]: Need to distinguish the host vs. DHCP client

Commenté [MB9]: I suggest to delete this. Do you mean «upsteram»?

Commenté [MB10]: Contradicts with the mention right after.

~~Client~~ client does not require any change. In this case it is up to the
Relay Agent to provide the full 4o6 DHCP ~~set of functionality~~suppot whereas
~~the~~ a legacy client is not aware of being served via a 4o6 DHCP service. All prerequisites and configuration that apply to the DHCP client
in Section 5 of [RFC7341] ~~apply~~ shall be applied to the 4o6RA instead.

To maintain interoperability with existing DHCPv6 relays and servers, the message format is unchanged from [RFC8415]. The 4o6RA implements the same message types as a normal DHCPv6 Relay Agent (Section 6 of [RFC7341]).

In this specification, the 4o6RA creates the DHCPV4-QUERY Message and encapsulates the DHCP request message received from the legacy DHCPv4 client.

When DHCPV4-RESPONSE Message is received by the 4o6 Relay Agent, it looks for the DHCPv4 Message option within this message. If this option is not found, the DHCPv4-response message MUST be discarded. If the DHCPv4 Message option is present, the 4o6RA MUST extract the DHCPv4 message and forward the encapsulated DHCPv4-response to the ~~legacy~~ requesting DHCPv4 client.

~~Any~~ Layer 2 Relay Agents receiving DHCPV4-QUERY or DHCPV4-RESPONSE messages ~~will~~ are expected to handle them as specified in Section 6 of [RFC6221].

~~The~~ DHCPv6 servers must be compliant with 4o6 according to [RFC7341]. No additional requirements on DHCPv6 servers are set by this specification.

xxx

4. Sample Case: Using 4o6RA for Topology Discovery

In some networks the configuration of a client host may depend on the topology. However, when a ~~new client~~ host ~~gets connected~~ attaches to ~~the~~a network, it may be unaware of the topology and respectively how it has to be configured.

~~The~~ DHCPv4 [RFC2131] and DHCPv6 [RFC3315] ~~protocol~~ specifications describe how addresses can be allocated to clients based on network topology information provided by ~~the~~ a DHCP relay, typically ~~infrastructure~~.

In IPv6 networks, t~~T~~opology discover can be realized using DHCPv6 Relay Agents [RFC6221] ~~that~~ which insert relay agent options in DHCPv6 message exchanges ~~in order~~ to identify the client-facing interfaces, (e.g., using the Serial Number or other hardcoded information). Then, a
reference host that is responsible for providing configuration to the client host can obtain topology information from the DHCPv6 server.

Commenté [MB11]: There aspects that might not be applicable to the relay, e.g.,

«Before applying for an IPv4 address via a DHCPv4-query message, the client must identify a suitable network interface for the address. Once the request is acknowledged by the server, the client can configure the address and other relevant parameters on this interface. »

Please check those and tag those that are not applicable.

Commenté [MB12]: Shouldn't the relay be configured, e.g., with DHCP 4o6 Server's addresses?

Commenté [MB13]: I don't think we can impose anything here by spec.

Commenté [MB14]: As there might be many.

Commenté [MB15]: Some text about the behavior of intermediate v4 relays would be appropriate (this will be basically pointing to Section 10 of 7341).

Commenté [MB16]: I don't parse this.

Commenté [MB17]: Simply say «when a host connects»

Commenté [MB18]: Who?

Commenté [MB19]: I don't parse this.

Address/prefix allocation decisions are integral to the allocation of addresses and prefixes in DHCP. The argument is described in details in [RFC7969], here we want to guarantee that 4o6RA does not break any legacy capability when related to the use of topology.

Commenté [MB20]: I'm afraid some more elaboration is needed. RFC7969 describes how to identify client's Location by DHCP servers without requiring any extension.

In the scenario described in [RFC7341], the DHCPv6 Relay Agent knows the interface where the encapsulated DHCP request is received.

Moving 4o6 in the intermediate node rather than at the client breaks the topology propagation as 4o6RA-only does not provide any interface information in the encapsulated message.

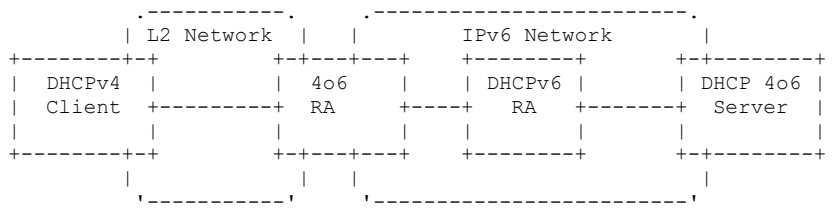

Figure 2: Topology broken path

As shown in Figure 2, the introduction of 4o6 at the edge of the IPv6 network hides the L2 network from the DHCPv6 RA.

In order to preserve the topology information, it is recommended that the implementation of 4o6RA is combined with the implementation of LDRA [RFC6221] and that the implementation has a mechanism for LDRA to get interface information that can be used for the Interface-ID option, as specified in Section 5.3.2 of [RFC6221]. The internal mechanisms to exchange interface information, their format and whether the interface information contains an indication that a 4o6RA is involved are out of the scope for this document.

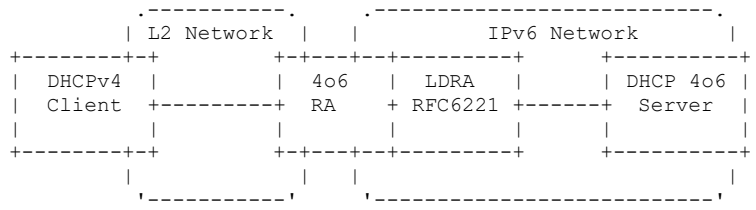

Figure 3: Topology path preserved with LDRA

The assumed architecture is shown in Figure 3 where the whole RA is built up with cooperating 4o6RA and LDRA, and an internal interface to ~~propagated~~ propagate topology information from 4o6RA to LDRA.

In a simple case, where the same node hosts ~~teh~~ the 4o6RA and the DHCP4o6
server, it might be enough to only use 4o6RA, as shown in Figure 4.

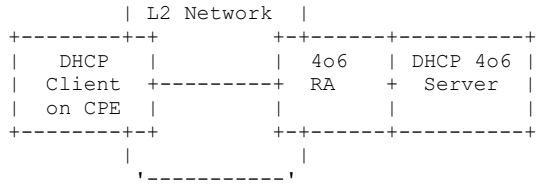

Figure 4: Topology path preserved 4o6 RA in DHCP server

5. Deployment Considerations

As ~~the~~ clients ~~is~~ are not aware of the presence of 4o6RA, the network deployment needs to ensure that all DHCPv4 broadcast~~-~~ and unicast messages from ~~the~~ clients are ~~routed over the~~steered to a 4o6RA. This can, e.g., be achieved by placing the 4o6RA in a ~~cetral~~ central position that can observe all traffic from the clients or use of address translation with the 4o6RA address for unicast messages.

6. Security Considerations

This ~~documents~~ document ~~applies~~ specified the applicability of 4o6 DHCP in a scenario where legacy IPv4 clients are connected to 4o6 DHCP Relay Agent that performs the en- and decapsulation. This document does not change anything else in the 4o6 DHCP specification and therefore the security consideration of [RFC7341] still apply.

Thi~~s~~e mechanism ~~described~~ differs from [RFC7341] as the DHCP client ~~actually~~ sends and ~~receveis~~ receives DHCPv4 messages, whereas in [RFC7341] it only sends DHCPv6 messages. This makes it possible that DHCPv4 messages could reach a DHCPv4 server without using the 4o6RA. While this can cause ~~errornous~~erroneous ~~states~~ state in both ~~the~~ clients and ~~DHCP~~ servers and potentially even lead to ~~misconfigrations~~misconfigurations that impact reachability, this is not seen as a security concern rather than a ~~deloyment~~deployment error.

More generally, ~~the~~ legacy IPv4 clients ~~is~~ are not aware of this mechanism, however, even when 4o6 DHCP is used, the client does not have any control about the information provided by the Relay agent. As such this change does not raise any additional security concerns.

Commenté [MB21]: This is can be exploited for attacks from within the network.

However, this is not a new attack.

You may simply say so.

7. IANA Considerations

This document has no IANA actions.

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, <https://www.rfc-editor.org/rfc/rfc2119>.

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

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/rfc/rfc3315>.

[RFC6221] Miles, D., Ed., Ooghe, S., Dec, W., Krishnan, S., and A. Kavanagh, "Lightweight DHCPv6 Relay Agent", RFC 6221, DOI 10.17487/RFC6221, May 2011, <https://www.rfc-editor.org/rfc/rfc6221>.

[RFC6925] Joshi, B., Desetti, R., and M. Stapp, "The DHCPv4 Relay Agent Identifier Sub-Option", RFC 6925, DOI 10.17487/RFC6925, April 2013, <https://www.rfc-editor.org/rfc/rfc6925>.

[RFC7341] Sun, Q., Cui, Y., Siodelski, M., Krishnan, S., and I. Farrer, "DHCPv4-over-DHCPv6 (DHCP 4o6) Transport", RFC 7341, DOI 10.17487/RFC7341, August 2014, <https://www.rfc-editor.org/rfc/rfc7341>.

[RFC7969] Lemon, T. and T. Mrugalski, "Customizing DHCP Configuration on the Basis of Network Topology", RFC 7969, DOI 10.17487/RFC7969, October 2016, <https://www.rfc-editor.org/rfc/rfc7969>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/rfc/rfc8415>.

8.2. Informative References

[RFC0951] Croft, W. and J. Gilmore, "Bootstrap Protocol", RFC 951, DOI 10.17487/RFC0951, September 1985, <https://www.rfc-editor.org/rfc/rfc951>.

[RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, DOI 10.17487/RFC1542, October 1993, <https://www.rfc-editor.org/rfc/rfc1542>.

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

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

Appendix A. Example Use Case: Topology Discovery for IPv4-only Radio Unit in the RAN Switched Fronthaul

In Radio Access Networks (RANs) the Fronthaul is the network segment that connects Radio Units, the distributed radio elements in a mobile network, to other network elements. The aggregation of Radio Unit devices (also known as Switched Fronthaul) hides the relationship between the Radio Units themselves and the physical ports where they are connected. The Radio Units are the client hosts in the switched Fronthaul network and need to be configured based on their Topology.

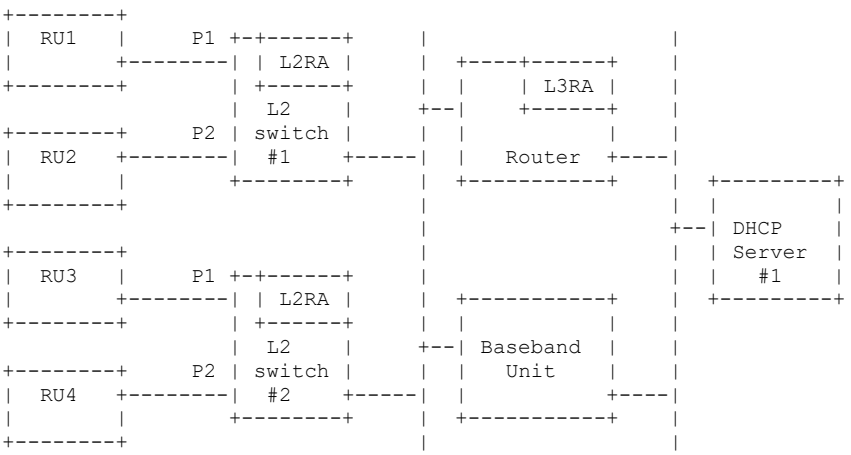

Figure 5: Layer 2 Switched Fronthaul Example

Figure 5 shows multiple Radio Units that are connected to one Baseband Unit by means of a Layer 2 switched network. The Baseband Unit is the central processing unit that handles baseband information. A Baseband Unit is often placed rather centrally, while the Radio Units need to be distributed to be co-located with or near the antennas. Traffic between Radio Units and Baseband Units is both IP-based and Layer-2-based and may pass a hierarchy of L2 switches.

In order to properly address the Radio Unit, the Baseband Unit needs to associate the Radio Unit's MAC address to the L2 switch and respective port where the Radio Unit is connected. To realize this device configuration in the Switched Fronthaul network, DHCPv6 can be used to discover the network Topology.

With the L2 switched network between the clients and the server, one of the clients is responsible for the configuration of the other clients based on their topology. Updating of the software on the clients is not possible often not possible and clients may be

IPv4-only.

Acknowledgments

The authors would also like to acknowledge interesting discussions in this problem space with Sarah Gannon, Ines Ramadza and Siddharth Sharma.

Authors' Addresses

Claudio Porfiri
Ericsson
Email: claudio.porfiri@ericsson.com

Suresh Krishnan
Cisco
Email: suresh.krishnan@gmail.com

Jari Arkko
Ericsson
Email: jari.arkko@ericsson.com

Mirja Kühlewind
Ericsson
Email: mirja.kuhlewind@ericsson.com