Workgroup:	DHC
Internet-Draft:	draft-porfiri-dhc-dhcpv4-l2ra-fronthaul-latest
Published:	23 October 2023
Intended Status:	Standards Track
Expires:	25 April 2024
Authors:	C. Porfiri	J. Arkko	M. Kühlewind
---	---	---	---
	Ericsson	*Ericsson*	*Ericsson*

Layer 2 Relay Agents in Cellular Fronthaul Networks

Abstract

The fronthaul portion of a cellular network is the part of the network that connects centralized radio controllers and the distributed radio units at the edge of the cellular network. A switched fronthaul network is one where the connectivity is provided through one or more stages of switches.

When performing address assignment and configuration tasks in such networks, knowledge of how the different devices are connected is beneficial. Networks that employ IPv6 can use DHCPv6 to support Relay Agents. However, those networks that continue to be based on IPv4 have no easy way to support this, as the DHCPv4 support for relays is limited.

This document explores how to provide Relay Agent functionality in IPv4-based switched fronthaul networks.

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 25 April 2024.

Copyright Notice

Table of Contents

1. Introduction

The fronthaul portion of a cellular network is the part of the network that connects centralized radio controllers and the distributed radio units at the edge of the cellular network. In recent years fronthaul networks have become increasingly popular due to the distribution of the radio functionality between the radio units and the more centralized, cloud-based higher layer functions.

A switched fronthaul network is one where the connectivity is provided through one or more stages of switches. Such arrangements are becoming common as well.

When performing address assignment and configuration tasks in such networks, knowledge of how the different devices are connected is beneficial as it allows automatic network configuration of the radio units.

Networks that employ IPv6 can use DHCPv6 to support Relay Agents [RFC3315]. This is commonly supported in fronthaul networks. In DHCPv6, a Relay Agent encapsulates the DHCP client message in a new DHCP message which it sends to the DHCP server along with any options it chooses to add to provide information to the DHCP server. This mode of operation supports also networks that include a hierarchy of switches.

However, those networks that continue to be based on IPv4 have no easy way to support this, as the DHCPv4 support for relays is much more limited. For instance, there is no support in DHCPv4 for hierarchical modes of deployment, as the specifications prohibit chaining of Relay Agent Information Options (RAIOs) [RFC3046].

This document explores how to provide Relay Agent functionality in IPv4-based switched fronthaul networks.

1.1. Terminology

The following terms and acronyms are used in this document:

- Baseband Unit (BB)

  A processing unit that handles baseband information. A Baseband Unit is often placed centrally, while the Radio Units (see below) are distributed and need to be co-located with or near the antennas.

- DHCP Relay Agent

  This is a concept in all of the protocols, BOOTP [RFC0951] [RFC1542], DHCPv4 [RFC2131] [RFC2132], and DHCPv6 [RFC3315], although the details differ between the protocols.

- Lightweight DHCPv6 Relay Agent (LDRA)

  This is an extension of the original DHCPv6 Relay Agent mechanism, to support also Layer 2 devices performing a Relay Agent function [RFC6221].

- Radio Unit (RU)

  A distributed radio element in a mobile network. Radio Units sometimes also called Radio Heads.

- Relay Agent Information Option (RAIO)

  This is a DHCP option defined in [RFC3046]. Also commonly referred to as "Option 82". RAIO options were later extended to be able to carry suboptions [RFC6925].

2. Use Case

In some network deployments like Fronthaul in mobile networks, the aggregation of Radio Unit devices (also known as Switched Fronthaul) hides the relationship between the Radio Unit themselves and the physical ports where they are connected.

In order to properly support the Switched Fronthaul device configuration, the DHCP server must know the network topology. This is accomplished by implementing in each Layer 2 switch a Layer 2 Relay Agent functionality.

2.1. Layer 2 Fronthaul Architecture

Figure 1 depicts the context where L2RA agent is exploited for providing the topology information to the DHCP server.

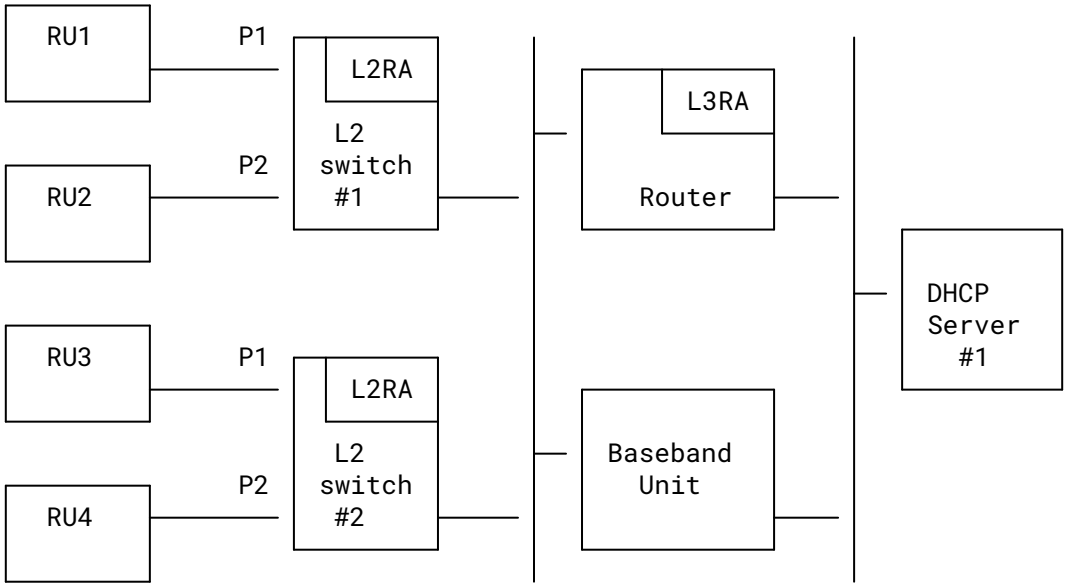

Figure 1: Layer 2 switched fronthaul

In Figure 1 there are a number of Radio Units (RU) that are connected to the Baseband Unit (BB) by means of a Layer 2 switched network. Traffic between RUs and BBs is both IP based and Layer 2 based.

In order to properly address the RU, BB needs to associate the RU's MAC to the L2 switch and to the switch port where the RU is connected to.

In a Layer 2 fronthaul there may be a hierarchy of L2 switches where a pool of RU and BB are connected.

Since each RU is unique, but the uniqueness is only known by BB and it's tied to the topology, BB needs to know what is the connection that is used to access each RU. In practice, the BB needs to know what the mapping between IP and MAC address towards the switch and port is.

2.2. Layer 2 topology discovery in IPv6

When the fronthaul network uses IPv6, DHCPv6 [RFC3315] is used for topology discovery.

The solution exploits DHCPv6 Relay Agent support in the server, whilst Lightweight DHCPv6 Relay Agent (LDRA) [RFC6221] is implemented in the L2 switches. The adoption of LDRA allows to inform DHCPv6 server about the L2 topology.

The following sequence can be used:

- At boot time, the RU sends a DHCPv6 request.
- The L2 switch forwards it with the topology information, as specified in [RFC6221]
- Any other device in the path towards the DHCPv6 server may also be a Relay Agent and provide additional topology information.
- DHCPv6 server will reply to the RU and provide a valid IP address.
- When the RU receives its IP address, the RU will communicate with the BB.
- As soon as BB knows about the RU, it will query the DHCPv6 server about the topology.
- Once the topology is known, the BB can properly manage the RU.

2.3. Layer 2 topology discovery in IPv4

DHCPv4 does not fully support the needed functionality for a Layer 2 Relay Agent. As such, the procedure used for IPv6 cannot be used. In such case only manual configuration is possible.

Specifically, in DHCPv4 lacks the following capabilities:

- There is no support for hierarchy of Relay Agents.
- It is not clear if there is an attribute that could carry interface or port related information, like DHCPv6's Interface-ID [RFC3315] [RFC6221].
- There is no specification for how to employ Relay Agents in a Layer 2 device.

3. Conventions and Definitions

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.

4. Requirements

A solution with similar capabilities to those of the DHCPv6 Relay Agent or Lightweight DHCPv6 Relay Agent mechanisms is needed.

That is, upon initializing themselves, the clients should be able to use the network infrastructure to request configuration information such as IP addresses. And the network infrastructure should be able to understand the topology of how the clients are connected to the network.

(In the use case discussed in Section 2.1, the clients are RUs and the network infrastructure is the switches and the BBs, but the concept is applicable in other circumstances.)

More specifically, these appear to be the minimum requirements:

- A configuration request made by a client must be passed onto to servers that provide configuration information.
- As part of passing a request from a client to the server, the server needs to be made aware of how the client is connected through the network, e.g., such that network devices connecting the client to the servers may add information they wish to relay.
- There needs to be support for adding information from multiple network devices, such as from any of the switches traversed on the path towards the server.
- The configuration servers need to be able to use the information shared by the network devices when processing the client's request.
- There should be no appreciable impact on network capacity or processing.

It is desirable but not required that a solution be based on DHCPv4.

5. Potential Approaches

Any arrangement that fulfils the requirements above is potentially a solution that can be applied in the use case described in Section 2.1.

Historically, the IETF DHC working group has discussed an extension that would support a DHCPv6-like Relay Agent mechanisms in DHCPv4. A proposal for this was made in [I-D.ietf-dhc-dhcpv4-relay-encapsulation], and some of the associated issues were discussed in [I-D.ietf-dhc-l2ra]. This is one potential approach.

It may of course be that the historical draft is not the only possible solution. The draft [I-D.ietf-dhc-dhcpv4-relay-encapsulation] may also be a broader and more generic solution than is strictly speaking necessary to support the requirements in Section 4. For instance, there's likely no need to support both BOOTP and DHCP.

It also seems possible that other arrangements based on new types of Relay Agent Information Options (RAIOs) [RFC3046] could be designed, or the current rules could be relaxed. The current specification requires that when a Relay Agent receives a packet containing an RAIO, it must not

add an RAIO. This prevents chaining of RAIOs, and hence prohibits the hierarchical use case. An alternative design, perhaps based on a new option and rules around detecting loops could perhaps circumvent the need to develop new DHCP messages as was done in [I-D.ietf-dhc-dhcpv4-relay-encapsulation].

For feature parity with DHCPv6, it is desirable but not required that a solution be based on DHCPv4.

6. Security Considerations

Mechanisms to avoid accepting information from untrusted relays are likely necessary. [RFC3046] provided some minimal anti-spoofing support, while [I-D.ietf-dhc-dhcpv4-relay-encapsulation] extended this to require configuration mechanisms to disable forwarding of any relayed information at the network border, i.e., disallowing clients or fraudulent entities from sending DHCP messages claimed to be relayed.

Other, cryptography-based mechanisms may provide further improved security. One example of a cryptography-based mechanism are the DHCP authentication mechanisms and suboptions defined in [RFC3118] and [RFC4030], although it is not clear that they are widely used.

7. IANA Considerations

This document makes no request for IANA.

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>.

[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>.

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

[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>.

[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>.

8.2. Informative References

[I-D.ietf-dhc-dhcpv4-relay-encapsulation] Lemon, T., Deng, H., and L. Huang, "Relay Agent Encapsulation for DHCPv4", Work in Progress, Internet-Draft, draft-ietf-dhc-dhcpv4-relay-encapsulation-01, 11 July 2011, <https://datatracker.ietf.org/doc/html/draft-ietf-dhc-dhcpv4-relay-encapsulation-01>.

[I-D.ietf-dhc-l2ra] Joshi, B. and P. Kurapati, "Layer 2 Relay Agent Information", Work in Progress, Internet-Draft, draft-ietf-dhc-l2ra-06, 25 January 2012, <https://datatracker.ietf.org/doc/html/draft-ietf-dhc-l2ra-06>.

[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>.

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

[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>.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, DOI 10.17487/RFC4030, March 2005, <https://www.rfc-editor.org/rfc/rfc4030>.

[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>.

Acknowledgments

The authors would like to acknowledge that much of the material in this document has been inspired by [I-D.ietf-dhc-dhcpv4-relay-encapsulation] by Ted Lemon, Hui Deng, and Lu Huang, and [I-D.ietf-dhc-l2ra] by Bharat Joshi and Pavan Kurapati. These documents were the original ideas, which the current authors have only adopted and fine-tuned.

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

Authors' Addresses

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

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

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