Network Working Group
Internet-Draft
Intended status: Experimental
Expires: March 23, 2013

A. Petrescu
CEA, LIST
K. Pentikousis
Huawei Technologies
C. Janneteau
CEA, LIST
M. Mouton
University of Luxembourg

September 19, 2012

Default Router List Option for DHCPv6 (DRLO)
draft-mouton-mif-dhcpv6-drlo-02.txt

Abstract

This document specifies an experimental DHCPv6 default route option which provisions static routing information to client nodes. The option facilitates central configuration of a multi-access client node's default router list with the IPv6 address, MAC address, and lifetime of the route, which is preferred in certain multi-access network environments. In addition, the DHCP option defined in this document can provide operational simplicity in network coverage extension scenarios using inexpensive (and limited resource) consumer-grade equipment. Finally, the proposed DHCP option has been implemented and tested in practice; its experimental use points to benefits with respect to reduced signaling and energy consumption compared to existing default route configuration mechanisms.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 4
3. Applicability and Use Cases 4
  3.1. Large Mobile Network Use Case 4
  3.2. Mi-Fi Coverage Extension Use Case 5
  3.3. M2M Constrained Device Use Case 6
4. Pertinence to the MIF Working Group 8
5. Topologies and Message Exchange Diagrams 8
  5.1. Topologies 8
  5.2. Message Exchange 9
6. DHCPv6 Default router list option 10
  6.1. Option format 10
    6.1.1. Client side 10
    6.1.2. Server side 11
  6.2. Optimization 12
  6.3. Default router lifetime management 13
7. Open issues 13
8. Security Considerations 13
9. IANA Considerations 14
10. Acknowledgements 14
11. References 14
  11.1. Normative References 14
  11.2. Informative References 15
Appendix A. ChangeLog 16
Authors' Addresses 16

1. Introduction

The Neighbor Discovery protocol [RFC4861] is currently considered as the best way for providing a default route information to a client in IPv6 networks. Hence it was not considered necessary for DHCPv6 [RFC3315] to have this feature. But, recently, certain deployment scenarios express a need not to use the neighbor discovery autoconfiguration mechanism.

For example, a distinct trend is shaping up towards centralization in network configuration and management. In this trend, contrary to Stateless Address Autoconfiguration (SLAAC) [RFC4862], which requires provisioning and distributing configuration information at each router, certain configuration information can be centralized in a server and then distributed when needed through DHCPv6. This means that, for instance, all subnet configurations can be managed via a single configuration database containing all IP prefix information, DNS server addresses, timers, and others - in an on demand manner. As we will see below, in practice, there are several scenarios where the administrator of a large, complex network architecture including numerous routers and access points may prefer a more centralized, stateful autoconfiguration solution which capitalizes on the widespread deployment of DHCPv6 to facilitate operation and management for multiaccess networks. Ease of deployment, operation and management are key design consideration for future mobile networks (e.g., see [Penti2011] and the references therein).

This draft specifies an experimental DHCPv6 option which can be used to populate the ND Neighbor Cache as pointed to by the ND Default Router List (this data is colloquially named "a default router list" in the remainder of this document). This option is similar to the DHCPv4 option router [RFC2132]. Contrary to DHCPv4, however, this option also provides router lifetime (thus enabling mechanisms such as automatic renumbering) and optionally the default router's link-layer address. Lifetime and link-layer address are necessary for a coherent implementation of DHCP and ND data structures. They are particularly useful in the context of mobile networks and pertinent to multihoming nodes for managing several default routers in order to address service continuity issues.

Using DHCPv6 to provide a default route to a client was previously advocated in [I-D.droms-dhc-dhcpv6-default-router]. Additionally, [I-D.ietf-mif-dhcpv6-route-option] presents a method to distribute routes, in a generic manner, to DHCP Clients. The route-option draft describes a capability to communicate a default route as a particular case of a route (use destination prefix "::" with prefix length 0, and address of the default router). But (1) this draft needs a means to communicate the MAC address of the default router, and (2) avoids

to communicate multiple default routers to the same Client.

2. Terminology

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].

This document uses also the terminology defined in [RFC3315], [RFC3963] and [RFC4862].

3. Applicability and Use Cases

This section describes use cases relevant to the experimental DHCP option proposed in this document and explains how its deployment can improve network management. We explore three use cases, although we expect that the solution has other applications as well. First, we discuss the use of the proposed option in a large mobile network where the administrator/operator prefers to have centralized control of the default routes used by different nodes. Second, we consider the Mi-Fi coverage extension case where the need is to control the devices connecting to the mobile network in an ad-hoc manner over consumer-grade equipment. Finally, we look into M2M constrained router devices where configuration message exchanges need to be as few as possible, in the interest of energy and other network resource consumption. Scenarios like these have been long described in the research literature; see, for example [Sollner2008] and the references therein.

3.1. Large Mobile Network Use Case

There is no doubt that most users today access the Internet over a wireless network. This trend is expected to continue unabated for the foreseeable future. The current generation of mobile networks features a largely hierarchical structure, in part due the origins of the technologies used in wireless telecommunication networks [Penti2011]. Another part has to do with the strong push for centralized control for technical and business reasons. While it is expected that more distribution, for example, in mobility management is to be expected [I-D.ietf-dmm-requirements], other trends point to the need for more centralized network control loops [Cori2012].

The experimental DHCPv6 option specified in this document is applicable to both cases. In a network where more centralization is preferred, multi-mode nodes can receive different default route configuration (including route lifetime) with the aid of a

centralized database and DHCPv6, as described in Section Section 5.1. This may prove particularly useful for enabling the network to select the best default route for multihomed nodes depending on monitoring information collected from various network elements. In addition, the network can use the option specified in this document to steer traffic from newly attached nodes to a different default router due to network maintenance operations. On the other hand, an IP network adopting control/data plane separation for certain mechanisms can benefit from the use of this option in some subnets depending on several factors. For instance, we expect that this can ease the incremental deployment of the aforementioned mechanisms by maintaining a tightly controlled centralized view of the network.

3.2. Mi-Fi Coverage Extension Use Case

This use case relates to residential access and, in particular, to wireless network extension scenarios, including those involving personal portable devices connected to cellular or other wide-area networks. Devices like these, popularly referred to as "Mi-Fi", enable a user to take advantage of her cellular subscription, for example, and connect other devices to the Internet. Mi-Fi devices can be standalone, i.e. provide no other functionality than acting as interconnection points, are typically small in size (hence mobile), and tend to be inexpensive.

Mi-Fi devices have gained in popularity in recent years as they allow other Wi-Fi-only devices to be connected to the Internet via a cellular network in the absence of Wi-Fi coverage. For example, a Mi-Fi device can connect up to five other devices over its Wi-Fi interface to a cellular network. Typical users carry Mi-Fi devices around and often use them to connect very different sets of Wi-Fi devices even within the same day. For instance, a mobile network subscriber can use the Mi-Fi device to enable Internet connectivity to the user's pad and laptop at home, connect a pod to a streaming Internet radio service while the user is in the car to work, and offer ad-hoc Internet connectivity to friends and colleagues at an IETF meeting. It may be often desirable to configure different default routes through the mobile network. Note that, in practice, said device could be dedicated to the role of providing tethered access or it can be a typical multiaccess smartphone extending network coverage to neighboring nodes.

From the network perspective, the operation of all connected nodes should be still managed efficiently although connectivity is maintained through a low-end consumer device. This includes the default routes as well as IP address lease times. In this use case, the Mi-Fi device does not play the role of a router, but it can act as a DHCP relay or a server. In the former case, the Mi-Fi DHCP

relay agent forwards the request as per usual, indicating its DUID, and the default router assignment occurs at the network side explicitly as each Wi-Fi device connects to the Mi-Fi-based local wireless network. Alternatively, the Mi-Fi device makes the default router assignment locally, based on the configuration information it has received using the proposed option. In either case, the network can configure, on demand, different default routes depending on the Mi-Fi location and point of attachment to the mobile network. Moreover, the network can provide different route lifetimes depending on the operational context. Note that the often battery-powered Mi-Fi device should not broadcast connectivity information in order to keep power consumption low and reduce information leakage. In short, from the device perspective, power consumption is reduced and the Wi-Fi devices do not need any updates, while, from the network perspective, the advantages of centralized management are significant.

3.3. M2M Constrained Device Use Case

For a constrained M2M Gateway it is advantageous to use solely the DHCPv6 protocol to configure a default route, an address and a delegated prefix, instead of using both protocols ND and DHCPv6.

Machine-to-Machine communication (M2M) has recently been employed in large-scale deployments in various markets such as cellular telecommunications, home networking, smart energy management, eHealth and vehicular communications. A machine device is typically a highly constrained computing and communicating platform: for example an 8-bit processor with a GSM module powered by a button cell. Other, more powerful machine devices, include more than a single means of communication. Without going into detail, it is acknowledged that whereas many different classes of machine devices exist, their key characteristics are generally the following: simplicity, small dimensions, low cost, and unattended operation for extended periods of time.

An M2M Gateway is a machine-class device which has two or more interfaces. One of the interfaces has long range wireless data capability (e.g., LTE-M). This Gateway is in charge of obtaining Internet connectivity and offering Internet connectivity to other machine-class devices. Since it ought to run unattended for extended periods of time, it must be easily auto-configurable. In other words, the most important IP parameters must be configured automatically.

A basic IPv6 configuration includes IPv6 prefix and a default route to global Internet. Devices with limited CPU and memory capacity can benefit from the sole presence of a default route in their routing

tables: it is sufficient to store the default route only in order to be able to reach any other node in the Internet. In this sense, the default route is a very strong candidate for implementation in small devices as it is possible to avoid storing other routes, while still maintaining connectivity to every other device in the Internet. Using a default route instead of a large number of specific routes helps keeping routing table sizes extremely compact, which is essential in the case of machine-class devices.

For these reason, it is important to have a suitable mechanism for assigning default routes to end nodes: M2M Device and M2M Gateway. A Gateway can be considered as an emph(almost)-end node: it is situated one or a few IP hops away from the end.

In addition to the IPv6 prefix (for its own interface(s)) and the default route to the global Internet, the M2M Gateway needs to be configured with an additional IPv6 prefix, call it P. This prefix P is to be used by the devices 'behind' the M2M Gateway - each such device needs to auto-configure an address for itself. This prefix P is the delegated prefix.

The currently defined mechanisms to automatically configure the triplet [IPv6 address, default route, delegated prefix] to a node, such as as the M2M Gateway in our example, are two: Neighbor Discovery and DHCPv6 Prefix Delegation. Hence, two full protocol implementations are needed for an M2M Gateway because, on the one hand, Neighbor Discovery (ND) cannot delegate prefixes and, on the other, DHCPv6 cannot configure default routes. Some implementers find that using two different protocols for obtaining the aforementioned triplet is an unnecessary burden for machine-class devices: the needs in terms of memory size are almost two times as much, the number and size of exchanged messages are almost doubled, and so on. In short, for a constrained M2M Gateway implementation it is advantageous to use solely the DHCPv6 protocol to configure a default route, an address and a delegated prefix, instead of using both ND and DHCPv6.

It would thus be advantageous to define options for the DHCPv6 protocol which can be used to assign the missing parameter from the triplet (i.e. a default route) to an M2M Gateway, instead of using both ND and DHCPv6 to achieve the same task.

Experiments with an actual implementation, which uses the DHCPv6 default route proposed in this draft, have shown a reduction in message counts from 6 to 4 (when comparing the combined use of DHCPv6 and ND, versus solely DHCPv6 with the option proposed herein, to make the same configuration).

4. Pertinence to the MIF Working Group

The Multiple Interfaces WG (MIF) is treating of hosts which have the ability to attach to multiple networks simultaneously. The WG is chartered to produce, among other products, extensions to DHCPv6 to "provision client nodes with small amount of static routing information".

The mechanism described in this draft, can be used to communicate several static default routes (triplets of the form gw-mac-lifetime) to a single host which can have several interfaces.

The distinction among the default routes (once installed on a client) can be realized according to various criteria: (1) use a form of Preferences, new extensions similar to RFC 4191, (2) use the Lifetime communicated by the mechanism of this draft to distinguish among default routes according to new rules, (3) use a random function to pick a default route, (4) use a new interface name in the ORO and in the Ack to specify which default route uses which interface, (5) use a new field containing a source address which the client must use for a particular default route, and more.

5. Topologies and Message Exchange Diagrams

5.1. Topologies

This section describes two simple topologies which abstract the use cases described above: one involving a server and a client and another implying in addition a relay.

Client/Server topology:

```
                       +-------+        +-------+
                       |DHCPv6|--------|DHCPv6|
                       |server|  link  |client|
                       +-------+        +-------+
```

Figure 1: Simple Client-Server topology

In this topology, a client with no IPv6 configuration needs to obtain an Internet access and does not intend to use SLAAC. It asks the DHCPv6 Server the three necessary settings: an IPv6 address, a default router address and a DNS server in a solicit message. The DHCPv6 Server receives this Solicit message and sends back the parameters necessary fo IPv6 configuration.

Client/Relay/Server topology:

```
                  +------+        +------+        +------+
                  |DHCPv6|--....--|DHCPv6|--------|DHCPv6|
                  |server|ethernet|relay |ethernet|client|
                  +------+        +------+        +------+
```

Figure 2: Simple Client-Relay-Server topology

Again, a client with no IPv6 configuration tries to obtain an Internet access and doesn't want to use SLAAC. It asks the DHCPv6 server the same way as in previous figure but the DHCPv6 server is not on the same link. The DHCPv6 relay takes client DHCPv6 message and delivers it to the server. The server knows that the message is relayed and send its responses back to the relay.

5.2. Message Exchange

There are two main message exchange scenarios corresponding to the use or not of a relay. The message exchange when the client is not on the same link with the server is the following:

```
                     +------+                     +------+
                     |DHCPv6|                     |DHCPv6|
                     |client|                     |server|
                     +------+                     +------+
                          |                          |
                          |    DHCPv6 Solicit        |
                          |------------------------->|
                          |                          |
                          |    DHCPv6 Advertise      |
                          |<-------------------------|
                          |                          |
                          |    DHCPv6 Request        |
                          |------------------------->|
                          |                          |
                          |    DHCPv6 Reply          |
                          |<-------------------------|
                          |                          |
```

Figure 3: Client-Server message exchange

A normal exchange between a new Client and a DHCPv6 Server consists of four messages: Solicit, Advertise, Request, and Reply. In a Solicit/Request packet a Client lists wanted options in the Option Request Option (ORO). This option is composed of a list of option

codes. The DHCPv6 Server answers those packets with Advertise/Reply packets containing values for the options asked by the Client.

The message exchange when using a relay, because the client and the server are not on the same link is illustrated in Figure 4.

```
       +------+                    +------+                     +------+
       |DHCPv6|                    |DHCPv6|                     |DHCPv6|
       |client|                    |relay |                     |server|
       +------+                    +------+                     +------+
           |                          |                            |
           |    DHCPv6 Solicit        |      DHCPv6 Relay-forw     |
           |------------------------->|===========================>|
           |                          |                            |
           |    DHCPv6 Advertise      |      DHCPv6 Relay-reply    |
           |<-------------------------|<===========================|
           |                          |                            |
           |    DHCPv6 Request        |      DHCPv6 Relay-forw     |
           |------------------------->|===========================>|
           |                          |                            |
           |    DHCPv6 Reply          |      DHCPv6 Relay-reply    |
           |<-------------------------|<===========================|
           |                          |                            |
```

Figure 4: Client-Relay-Server message exchange

The relay receives the message from the client and forwards it to the server in a Relay-forw message. The server replies to the relay with an advertise/reply message encapsulated in a Relay-reply message. The content of this message is extracted by the relay and sent to the client.

6. DHCPv6 Default router list option

6.1. Option format

6.1.1. Client side

In its DHCPv6 requests, the client sends a list of required options in the option request option (ORO). The format of this option is the following:

```
      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_ORO          |           option-len          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |    requested-option-code      |                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                              ...                              |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: DHCPv6 option request option field

The proposed option (to fill in the field requested-option-code in the diagram above) is named in this draft OPTION_DEFAULT_ROUTER_LIST. It is possible to concatenate this value with several other existing requested-option-code's.

The value of this code of this option is TBD (to be defined) and/or TBA (to be assigned).

6.1.2. **Server side**

The default router list option is illustrated below:

```
      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_DEFAULT_ROUTER_LIST  |          option-len           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     |                        router_address                         |
     |                                                               |
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |        router_lifetime        |    lla_len    |               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
     .                 router_link_layer_address(opt)                .
     .                              ...                              .
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: DHCPv6 default router list option field

As this option contains a list, the pattern containing router_address, router_lifetime, lla_len and optionnaly router_link_layer_address can be repeated.

option-code

OPTION_DEFAULT_ROUTER_LIST (TBA)

option-len

length of the default router list option in bytes. It has a value of minimum 23 (decimal representation).

router_address

default router IPv6 address (16 bytes)

router_lifetime

16-bit unsigned integer. Router lifetime in units of seconds. Limit value is 9000, while the value 0 SHOULD NOT appear, as explained in section 6 of [RFC 4861].

lla_len

8-bit unsigned integer. The size of the link layer address of the router in bytes. Equals to 0 if no link layer address is given.

router_link_layer_address

link layer address of the router. Its length is not known in advance and need to be inquired in lla_len field. This field is optional.

This option contains an optional variable length field router_link_layer_address. Router_address and router_lifetime field's size are fixed.

There are two alternative possibilities of using router information in the list:

- Not using router_link_layer_address: DHCPv6 server communicates router_address and router_lifetime with lla_len equals to 0. Default router's information is finished at the end of lla_len.

- Using router_link_layer_address: DHCPv6 server communicates router_address and router_lifetime with lla_len equals to k, where k is the size of the link-layer address. After the field lla_len the default router's information is finished after reading k more bytes.

6.2. Optimization

An optimization is possible: removing lla_len field for the last element of a default router list when that is not necessary. Prima facie, one may consider that removing one byte may not be worth the effort of the implementation complexity. This is why this draft

proposes to apply this optimization in only one simple but fairly frequent case: if the last element (i.e. the triplet address-MAC-lifetime) of a list (i.e., if there are more than one elements) has no link-layer address. As a matter of fact it has the advantage of removing 8 zero bits. This case occurs each time a network administrator does not want to use the router_link_layer_address. This case is frequent enough to justify an optimization. Moreover this optimization has been implemented and does not require a huge amount of intellectual effort (around 10 extra lines of code).

6.3. Default router lifetime management

This draft proposes to use default router lifetime in the same manner as [RFC4861]. This has the following consequences.

When a default router lifetime is equal to 0 it MUST be deleted from the Default Router list, Neighbor cache and other related Forwarding Information Bases.

Following [RFC4861] Section 6, this document proposes to limit the lifetime to 9000 (decimal) seconds.

7. Open issues

In addition to the default router address, lifetime and link-layer address, the neighbor discovery mechanism also provides MTU, hop limit, reachable time, retransmission timer, and textual name of the interface. This information can be defined in other DHCPv6 options extending this draft, if needed.

The DHCP and Neighbor Discovery protocols manage router lifetime differently. DHCPv6 [RFC3315] specifies lifetimes typically in a 4-byte field. On the other hand, the Neighbor Discovery protocol defines a 2-byte field for lifetime. In addition, it defines a lifetime limit equaling 9000 making the use of 4-byte fields unnecessary. Because of this, this draft proposes adopts the ND approach and includes a 2-byte field for router lifetime.

The simultaneous use of DHCP and Router Advertisement mechanisms to communicate default routes is out of the scope of this specification.

8. Security Considerations

Security considerations referring to DHCPv6 are described in [RFC3315] and other more recent Internet Drafts. The new option described here should not add new threats. However, it is worth

mentioning that the high importance of a default route (it must work when everything else fails) represents also a high risk when successful attacks - if at all - happen.

9. IANA Considerations

The proper working of this extension to DHCPv6 to support default routers rely on using a unique number for OPTION_DEFAULT_ROUTER_LIST.

In this sense, and when agreed to take on this path, IANA will be demanded to assign an option code to OPTION_DEFAULT_ROUTER_LIST, if deemed necessary.

Currently, the local prototype implementation uses the number 66 (decimal) for this field.

10. Acknowledgements

The authors would like to acknowledge the useful technical contribution of Mathias Boc, Sofian Imadali and Arnaud Kaiser.

Authors appreciate the particularly stimulating discussion about default route and DHCPv6 in the email lists of DHC, MIF and 6MAN Working Groups.

Recently, Tomasz Mrugalski offered insight about default routes potentially used by draft-dec-dhcpv6-route-option-02. Mikael Abrahamsson suggested communicating a source address when discussing default route and DHCPv6.

This work has been performed in the framework of the ICT project ICT-5-258512 EXALTED, which is partly funded by the European Union. The organisations on the source list [CEA] would like to acknowledge the contributions of their colleagues to the project, although the views expressed in this contribution are those of the authors and do not necessarily represent the project.

11. References

11.1. Normative References

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

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor

Extensions", RFC 2132, 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.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

11.2. Informative References

[Cori2012]
Corici, M I., Hasse, P., Kappler, C., Pentikousis, K., Roth, R., and M. Schramm, "Cost-controlled monitoring information collection in heterogeneous mobile network infrastructures", Proceedings of the IEEE International Conference on Communications Workshops (Telecommunications: From Research to Standards), Ottawa, Canada , June 2012.

[I-D.droms-dhc-dhcpv6-default-router]
Droms, R. and T. Narten, "Default Router and Prefix Advertisement Options for DHCPv6", draft-droms-dhc-dhcpv6-default-router-00 (work in progress), March 2009.

[I-D.ietf-dmm-requirements]
Chan, A., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-02 (work in progress), September 2012.

[I-D.ietf-mif-dhcpv6-route-option]
Dec, W., Mrugalski, T., Sun, T., Sarikaya, B., and A. Matsumoto, "DHCPv6 Route Options", draft-ietf-mif-dhcpv6-route-option-05 (work in progress), August 2012.

[Penti2011]
Pentikousis, K., "Design considerations for mobility management in future infrastructure networks", ITU Telecom

World 2011 Technical Symposium, Geneva, Switzerland , October 2011.

[Sollner2008]
Sollner, M., Gorg, C., Pentikousis, K., Cabero-Lopez, J M., Ponce de Leon, M., and P. Bertin, "Mobility scenarios for the Future Internet: The 4WARD approach", Proceedings of the 11th International Symposium on Wireless Personal Multimedia Communications (WPMC), Saariselk, Finland , September 2008.

Appendix A. ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

From draft-mouton-mif-dhcpv6-drlo-01.txt to draft-mouton-mif-dhcpv6-drlo-02.txt:

- New author entry.
- Extended and detailed the use cases where this DHCPv6 option may be used to communicate a default route.
- Explained that this is experimental, an implementation exists and a gain in number of messages exchanged has been demonstrated.
- Rephrased completely the abstract.

From draft-mouton-mif-dhcpv6-drlo-00.txt to draft-mouton-mif-dhcpv6-drlo-01.txt:

- Date change, author ordering and affiliation.

Authors' Addresses

Alexandru Petrescu
CEA, LIST
Communicating Systems Laboratory, Point Courrier 173
Gif-sur-Yvette, F-91191
France

Phone: +33(0)169089223
Email: alexandru.petrescu@cea.fr

Kostas Pentikousis
Huawei Technologies
Carnotstr. 4
Berlin, D-10585
Germany

Phone:
Email: k.pentikousis@huawei.com

Christophe Janneteau
CEA, LIST
Communicating Systems Laboratory, Point Courrier 173
Gif-sur-Yvette, F-91191
France

Phone: +33(0)169089182
Email: christophe.janneteau@cea.fr

Maximilien Mouton
University of Luxembourg
Interdisciplinary Center for Security, Reliability and Trust
Luxembourg,
Luxembourg

Phone:
Email: maximilien.mouton@uni.lu