Mobility Extensions for IPv6 (MEXT)
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2010

R. Droms
P. Thubert
Cisco
F. Dupont
ISC
W. Haddad
Ericsson
CJ. Bernardos
UC3M
March 8, 2010

DHCPv6 Prefix Delegation for NEMO
draft-ietf-mext-nemo-pd-04

Abstract

One aspect of network mobility support is the assignment of a prefix or prefixes to a Mobile Router (MR) for use on the links in the Mobile Network. DHCPv6 prefix delegation can be used for this configuration task.

Table of Contents

1. Introduction

One aspect of network mobility support is the assignment of a prefix or prefixes to a Mobile Router for use on the links in the Mobile Network. DHCPv6 prefix delegation [RFC3633] (DHCPv6PD) can be used for this configuration task.

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 RFC2119 [RFC2119].

The following terms used in this document are defined in the IPv6 Addressing Architecture document [RFC4291]:

link-local unicast address

link-local scope multicast address

The following terms used in this document are defined in the mobile IPv6 specification [RFC3775]:

home agent (HA)

home link

The following terms used in this document are defined in the Mobile Network terminology document [RFC4885]:

Mobile Router (MR)

Mobile Network (NEMO)

Mobile Network Prefix (MNP)

The following terms used in this document are defined in the DHCPv6 [RFC3315] and DHCPv6 prefix delegation [RFC3633] specifications:

delegating router (DR; acts as a DHCPv6 server)

requesting router (RR; acts as a DHCPv6 client)

DHCPv6 relay agent (DRA)

The following acronym is used in this document:

DHCPv6PD: DHCPv6 prefix delegation

3. Application of DHCPv6 prefix delegation to mobile networks for delegation of home prefixes

The NEMO Basic protocol [RFC3963] extends the mobile IPv6 protocol [RFC3775] to enable network mobility. In this extension, an MR uses the mobile IPv6 protocol to establish and maintain a session with its HA, and uses bidirectional tunneling between the MR and HA to provide a path through which nodes attached to links in the Mobile Network can maintain connectivity with nodes not in the Mobile Network.

The requirements for NEMO [RFC4885] include the ability of the MR to receive delegated prefixes that can then be assigned to links in the Mobile Network. DHCPv6PD can be used to meet this requirement for prefix delegation.

To use DHCPv6PD for Mobile Networks, the HA assumes the role of either the DR or a DHCPv6 relay agent and the MR assumes the role of the RR. Throughout the remainder of this document, the HA will be assumed to be acting as a DHCPv6PD DR or relay agent and the MR will be assumed to be acting as a RR.

If the HA is acting as relay agent, some other device acts as the DR. For example, the server providing DHCPv6 service in the home network might also provide NEMO DHCPv6PD service. Or, a home network with several HAs might configure one of those HAs as a DHCPv6PD server while the other HAs act as relay agents.

The HA and MR exchange DHCPv6PD protocol messages through the tunnel connecting them (as specified in RFC3775). The tunnel acts as the link labeled "DSL to subscriber premises" in figure 1 of the DHCPv6PD specification. See Figure 1 for different possible deployment topologies.

```
        ----      /-----------\      ----
       | MR |-----|  Internet |-----| HA |
       |(RR)|     \-----------/     |(DR)|
        ----                         ----

        ----      /-----------\      -----       ------
       | MR |-----|  Internet |-----| HA  |-----|DHCPv6|
       |(RR)|     \-----------/     |(DRA)|     |Server|
        ----                         -----       ------

        -----     /-----------\      -----
       | MR  |----|  Internet |-----| HA  |
       |(RR) |    \-----------/     |(DR) |
       |(DRA)|                       -----
        -----
```

Figure 1: Different topologies of the application of DHCPv6PD to NEMO for delegation of MNPs

The DHCPv6PD server is provisioned with prefixes to be assigned using any of the prefix assignment mechanisms described in the DHCPv6PD specifications. Other updates to the HA data structures required as a side effect of prefix delegation are specified by the particular network mobility protocol. For example, in the case of Basic Network Mobility Support [RFC3963], the HA would add an entry in its binding cache registering the delegated prefix to the MR to which the prefix was delegated.

3.1. When the MR uses DHCPv6

The MR initiates a DHCPv6 message exchange for prefix delegation whenever it establishes an MR-HA tunnel to its HA. If the MR does not have any active delegated prefixes (with unexpired leases), the MR initiates a DHCPv6 message exchange with a DHCPv6 Solicit message as described in section 17 of RFC 3315 and section 12.1 of RFC 3633. Once the MR has been delegated a set of prefixes from the HA, the MR sends a new Binding Update including the delegated prefixes, carried in Mobile Network Prefix options (see Figure 2). Note that this requires a minor modification to the NEMO Basic Support protocol as described in RFC 3963. RFC 3963 does not assume the MR can change from implicit to explicit BU signaling mode, while this specification requires the MR to first perform a MIPv6 registration to the HA providing DHCPv6PD services (via implicit signaling, no MNP carried in the BU), then obtain a set of delegated prefixes via DHCPv6PD, and then send a new BU to the Home Agent, now carrying the delegated prefixes as Mobile Network Prefixes (explicit signaling mode).

In case the MR has one or more active delegated prefixes, the MR

initiates a DHCPv6 message exchange with a DHCPv6 Rebind message as described in section 18.1.2 of RFC 3315 and section 12.1 of RFC 3633. In this case, only one BU signaling sequence is required.

```
                 MR                           HA
                (RR)                         (DR)
                  |       Binding Update       |
                  |------------------------->|
                  |       (HoA, CoA)           |
                  |                            |
                  |       Binding Ack          |
                  |<-------------------------|
                  |                            |
                  |       DHCPv6 Solicit       |
                  |--=====================->|
                  |                            |
                  |       DHCPv6 Advertise     |
                  |<-=====================--|
                  |                            |
                  |       DHCPv6 Request       |
                  |--=====================->|
                  |                            |
                  |       DHCPv6 Reply         |
                  |<-=====================--|
                  | (Mobile Network Prefix)    |
                  |                            |
                  |     Binding Update         |
                  |------------------------->|
                  |     (HoA, CoA, MNP)        |
                  |                            |
                  |       Binding Ack          |
                  |<-------------------------|
                  |                            |
```

Figure 2: Signaling sequence for the case the HA acts as DHCPv6PD Delegating Router

3.2. Use of MR-HA tunnel for DHCPv6 messages

The DHCPv6 specification requires the use of link-local unicast and link-local scope multicast addresses in DHCPv6 messages (except in certain cases as defined in section 22.12 of the DHCPv6 specification). Section 10.4.2 of the mobile IPv6 specification describes forwarding of intercepted packets, and the third paragraph of that section begins:

However, packets addressed to the mobile node's link-local address MUST NOT be tunneled to the mobile node.

The DHCPv6 messages exchanged between the HA and the MR originate only with the HA and the MR, and therefore are not "intercepted packets" (i.e. the sender of the packets is a third node on the home link) and may be sent between the HA and the MR through the tunnel.

Even though the MR-HA tunnel is a point to point connection, the MR SHOULD use multicast DHCPv6 messages as described in RFC 3315 over that tunnel.

3.3. DHCPv6 Relay Agent for transmission of DHCPv6 messages

A DHPCv6 relay agent function [RFC3315] can be used as an alternative to multicast DHCPv6 messages over the tunnel between the MR and the HA. In this configuration, the relay agent function is co-located in the MR with the DHCPv6 client function (see Figure 3. Rather than using multicast to send DHCPv6 messages through the tunnel to the DHCPv6 server, the DHCPv6 client in the MR hands any outbound DHCPv6 messages to the co-located relay agent. Responses from the DHCPv6 server are delivered to the relay agent function in the MR, which extracts the encapsulated message and delivers it to the DHCPv6 client in the MR.

```
                         MR
                       (RR)                        HA
                       (DRA)                      (DR)
                         |       Binding Update    |
                         |------------------------>|
                         |       (HoA, CoA)        |
                         |                         |
                         |       Binding Ack       |
                         |<------------------------|
                     --  |                         |
                    /  \ |                         |
                    \   *|                         |
              DHCPv6 -- >|       DHCPv6 Solicit    |
              Solicit    |--=====================->|
                         |                         |
                         |       DHCPv6 Advertise  |
                     --  |<-=====================--|
                    /  \ |                         |
                    \   *|       DHCPv6 Request    |
              DHCPv6 -- >|--=====================->|
              Request    |                         |
                         |       DHCPv6 Reply      |
                         |<-=====================--|
                         | (Mobile Network Prefix) |
                         |                         |
                         |     Binding Update      |
                         |------------------------>|
                         |     (HoA, CoA, MNP)     |
                         |                         |
                         |       Binding Ack       |
                         |<------------------------|
                         |                         |
```

Figure 3: Signaling sequence for the case a DHCPv6 relay agent is co-located in the MR

3.3.1. Relay agent configuration

The use of the relay agent function in the MR allows the MR to unicast DHCPv6 messages to the DHCPv6 server. The relay agent must be configured with the address of the DHCPv6 server or another DHCPv6 relay agent that will forward message on to a DHCPv6 server. For the purposes of NEMO, the relay agent assumes that the HA for the MR hosts the next hop in the path the to the DHCPv6 server: either the DHCPv6 server or a relay agent that will forward message to the DHCPv6 server. Therefore, if the MR acts as a DHCPv6 relay agent, the MR MUST configure the DHCPv6 relay agent to forward DHCPv6 messages to the HA.

3.3.2. Transmission of DHCPv6 messages

In this configuration, i.e., a DHCPv6 relay agent is used and co-located in the MR, when the DHCPv6 client in the MR sends a message, it hands the message to the DHCPv6 relay agent in the MR. The way in which the message is passed to the DHCP relay agent is beyond the scope of this document. The relay agent encapsulates the message from the client according to RFC 3315 in a Relay-forward message and sends the resulting DHCPv6 message to the HA. The relay agent sets the fields in the Relay-forward message as follows:

msg-type   RELAY-FORW

hop-count   1

link-address   A non-link-local address from the MR interface (e.g., home address or, in case the HoA belongs to the MNP, the address of the MR's egress interface of the MR when attached to the Home Link) of the tunnel between the HA and MR

peer-address   A non-link-local address from the MR interface (e.g., home address or, in case the HoA belongs to the MNP, the address of the MR's egress interface of the MR when attached to the Home Link) of the tunnel between the HA and MR

options   MUST include a "Relay Message option" [RFC3315]; MAY include other options added by the relay agent.

3.3.3. Receipt of DHCPv6 messages

In this configuration, messages from the DHCPv6 server will be returned to the DHCPv6 relay agent, with the message for the DHCPv6 client encapsulated in the Relay Message option [RFC3315] in a Relay-reply message. The relay agent function extracts the message for the client from the Relay Message option and hands the message to the DHCPv6 client in the MR. The way in which, the message is passed to the client is beyond the scope of this document.

3.4. Exchanging DHCPv6 messages when MR is at home

When the MR is on its home link, the HA uses the home link to exchange DHCPv6PD messages with the MR. It is the responsibility of the implementation to determine when the MR is on its home link and to avoid use of any existing tunnel.

3.5. Selecting an HA that provides DHCPv6PD

Not all nodes that are willing to act as an HA are required to provide DHCPv6PD. Therefore, when selecting an HA, an MR that requires DHCPv6PD service must identify an HA that will provide the service. The MR can determine if an HA provides DHCPv6PD by initiating a DHCPv6 message exchange in which the MR requests delegated prefix(es). If the HA does not respond or responds but does not delegate any prefix(es) in its response, the MR assumes that the HA does not provide DHCPv6PD service. The MR continues to query all candidate HAs until it finds an HA that provides DHCPv6PD. Note that in this particular case, the MR has also to setup a tunnel with each HA (this requires the MR to perform an MIPv6 registration) it queries.

Querying an HA to determine if it provides DHCPv6PD requires a small modification to the operation of DHCPv6 as described in RFC 3315. Under normal circumstances, a host will continue to send DHCPv6 Solicit messages until it receives a response (see Section 17 of RFC 3315). However, an HA may choose not to respond to the Solicit messages from the MR because the HA does not provide DHCPv6. Therefore, when querying an HA to determine if the HA provides DHCPv6PD service, the MR MUST discontinue sending Solicit messages to the HA after sending 6 Solicit messages, and conclude that the HA will not provide DHCPv6PD service. Sending 6 queries provides enough reliability for scenarios in which the wireless connectivity is lost for a short period after sending the first BU message.

It is recommended that the MR uses a sequential probing of the HAs for DHCPv6PD service.

3.6. Minimizing DHCPv6PD messages

DHCPv6PD in a Mobile Network can be combined with the Rapid Commit option [RFC3315] to provide DHCPv6 prefix delegation with a two message exchange between the mobile node and the DHCPv6PD DR.

3.7. Location of DHCPv6PD Delegating Router function

Support of DHCPv6PD for a Mobile Network is optional.

The use of a DHCPv6 relay agent in DHCPv6PD may require "a protocol or other out-of-band communication to add routing information for delegated prefixes into the provider edge router" (section 14 of RFC 3633). If the DHCPv6PD DR function is implemented in the HA for the MR, no relay agent function is required.

It may be desirable to use a single DR to manage RRs in a network

with multiple HAs. In this scenario, the HAs will act as DHCP relay agents, forwarding messages between the RRs and the DR.

The use of the DHCPv6 relay agent function with DHCPv6PD requires that there be some mechanism through which routing information for the delegated prefixes can be added to the appropriate routing infrastructure. If the HA is acting as a DHCPv6 relay agent, the HA SHOULD add a route to the delegated prefix and advertise that route after receiving a binding update for the prefix from the RR [RFC3963]. Note that such binding update is received after the first binding update message which is sent by the MR in order to set-up the bidirectional tunnel (see Figure 4).

```
              MR                         HA                      DHCPv6
             (RR)                       (DRA)                    Server
               |       Binding Update    |                         |
               |------------------------>|                         |
               |       (HoA, CoA)        |                         |
               |                         |                         |
               |       Binding Ack       |                         |
               |<------------------------|                         |
               |                         |                         |
               |       DHCPv6 Solicit    |       DHCPv6 Solicit    |
               |--=====================->|------------------------>|
               |                         |                         |
               |       DHCPv6 Advertise  |       DHCPv6 Advertise  |
               |<-=====================--|<------------------------|
               |                         |                         |
               |       DHCPv6 Request    |       DHCPv6 Request    |
               |--=====================->|------------------------>|
               |                         |                         |
               |       DHCPv6 Reply      |       DHCPv6 Reply      |
               |<-=====================--|<------------------------|
               | (Mobile Network Prefix) | (Mobile Network Prefix) |
               |                         |                         |
               |     Binding Update      |                         |
               |------------------------>|                         |
               |     (HoA, CoA, MNP)     | (  HA starts  )         |
               |                         | ( advertising )         |
               |       Binding Ack       | (  routes to  )         |
               |<------------------------| (   the MNP   )         |
               |                         |                         |
```

Figure 4: Signaling sequence for the case the HA acts as DHCPv6 relay agent

In particular, if the MR uses NEMO explicit mode, then it must add the delegated prefix to the prefix list in the Binding Update

messages. If the binding cache is cleared before the prefix valid lifetime, the MR might bind that prefix again using explicit mode, till the lifetime expires.

In implicit mode, the HA must save the delegated prefix with the binding cache entry (BCE) of the Mobile Router. When the BCE is cleared, the HA loses the information about the delegated prefix. Because the MR will use DHCPv6 when it reestablishes its tunnel to the HA (see Section 3.1), the HA will be able to add the delegated prefix back to the BCE.

At the time this document was written, one way in which a DR can explicitly notify a relay agent about delegated prefixes, is to use the "DHCP Relay Agent Assignment Notification Option" [I-D.ietf-dhc-dhcpv6-agentopt-delegate].

Another alternative, if the RR is part of the same administrative domain as the home network to which it is attached through the HA, and the RR can be trusted, the RR can use a routing protocol like OSPF to advertise any delegated prefixes.

NEMO explicit mode is recommended to take advantage of the function already defined for NEMO.

3.8. Other DHCPv6 functions

The DHCPv6 messages exchanged between the MR and the HA may also be used for other DHCPv6 functions in addition to DHCPv6PD. For example, the HA may assign global addresses to the MR and may pass other configuration information such as a list of available DNS recursive name servers [RFC3646] to the MR using the same DHCPv6 messages as used for DHCPV6PD.

The HA may act as a DHCPv6 relay agent for MHs while it acts as a DR for MRs.

4. Security Considerations

This document describes the use of DHCPv6 for prefix delegation in Mobile Networks. It does not introduce any additional security considerations for DHCPv6 beyond those described in the "Security Considerations" section of the DHCPv6 base specification [RFC3315] and the "Security Considerations" of the DHCPv6 Prefix Delegation specification [RFC3633].

The use of DHCPv6, as described in this document, requires only message integrity protection, which can be provided by the mobile

network infrastructure between the MR and the HA.

If the network infrastructure connecting the various communicating nodes does not provide message integrity and source authentication for the DHCPv6PD messages, HAs and MRs SHOULD use DHCPv6 authentication as described in section "Authentication of DHCP messages" of the DHCPv6 specification [RFC3315], to guard against attacks mounted through prefix delegation.

If the HA and DHCPv6 PD functions are not provided by the same physical node, the HA will act as a DHCPv6 relay agent between the MR and the DHCPv6 server. In this scenario, the mobile network infrastructure will only protect the DHCPv6 traffic between the RR (MR) and the relay agent (HA). The following text, based on Section 21.1 of RFC 3315, describes how appropriate security can be provided between a DHCPv6 relay agent and server.

> DHCPv6 relay agents and servers MAY use IPsec mechanisms for IPv6 [RFC4301] to exchange messages securely. DHCPv6 relay agents and servers that support secure relay agent to server or relay agent to relay agent communication use IPsec under the following conditions:
>
> Selectors — DHCPv6 relay agents are manually configured with the addresses of the DHCPv6 server to which DHCPv6 messages are to be forwarded. Each DHCPv6 server that will be using IPsec for securing DHCPv6 messages must also be configured with a list of the DHCPv6 relay agents to which messages will be returned. The selectors for the DHCPv6 relay agents and servers will be the pairs of addresses defining DHCPv6 relay agents and servers that exchange DHCP messages on the DHCPv6 UDP ports 546 and 547.
>
> Mode — DHCPv6 relay agents and servers use transport mode and ESP. The information in DHCPv6 messages is not generally considered confidential, so encryption need not be used (i.e., NULL encryption can be used).
>
> Key management — If the HA providing the DHCPv6 relay agent function and the DHCPv6 servers are both administered by the same organization, public key schemes are not necessary. Because the relay agents and servers must be manually configured, manually configured key management may suffice, but does not provide defense against replayed

messages. Accordingly, IKE with preshared secrets SHOULD be supported.

Security policy DHCPv6 messages between relay agents and servers should only be accepted from DHCPv6 peers as identified in the local configuration.

Authentication Shared keys, indexed to the source IP address of the received DHCPv6 message, are adequate in this application.

5. IANA Considerations

This document describes the use of DHCPv6 for prefix delegation in Mobile Networks. It does not introduce any additional IANA considerations.

6. Acknowledgments

The authors would like to thank people who have given valuable comments on the mailing list. Specific suggestions from Ryuji Wakikawa, George Tsirtsis, Alexandru Petrescu, Vijay Devarapalli and Marcelo Bagnulo were incorporated into this document.

7. Change Log

This section MUST be removed before this document is published as an RFC.

7.1. Revision -00

This document is based on draft-ietf-nemo-dhcpv6-pd-03 and includes the use of the DHCPv6 relay agent in the MR, as described in Section 3.3, from draft-dupont-mext-dhcrelay-00.

7.2. Revision -01

Added detail in Section 4, "Security Considerations", describing protection required for DHCPv6 and a mechanism for protecting traffic between the DHCPv6 relay agent and server.

Corrected minor typos.

7.3. Revision -02

Removed text describing extensions to DHAAD for discovery of HA that will provide PD.

Added Section 3.5, "Selecting an HA that provides DHCPv6PD," which describes how an MR can discover DHCPv6PD service through polling of multiple HAs.

Added text to Section 4, "Security Considerations", giving detail about the use of IPsec.

7.4. Revision -04

Added some figures to better explaining considered topologies and message exchanges. Credits to Alex Petrescu.

Added some text to clarify that two BUs are required, one to set up the tunnel to the HA so the DHCPv6 signaling can be sent, and one to register the delegated prefixes as MNPs at the HA. This updates RFC 3963 behavior (note added).

Text added to address some comments received on the MEXT mailing list

Corrected minor typos.

Enlisted Carlos J. Bernardos as co-author

8. References

8.1. Normative References

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

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

8.2. Informative References

[I-D.ietf-dhc-dhcpv6-agentopt-delegate]
Droms, R., Volz, B., and O. Troan, "DHCPv6 Relay Agent Assignment Notification (RAAN) Option", draft-ietf-dhc-dhcpv6-agentopt-delegate-04 (work in progress), July 2009.

[RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, July 2007.

Authors' Addresses

Ralph Droms
Cisco
1414 Massachusetts Avenue
Boxborough, MA 01719
USA

Phone: +1 978.936.1674
Email: rdroms@cisco.com

Pascal Thubert
Cisco
Village d'Entreprises Green Side
400, Avenue Roumanille
Biot - Sophia Antipolis 06410
FRANCE

Email: pthubert@cisco.com

Francis Dupont
ISC

Email: Francis.Dupont@fdupont.fr

Wassim Haddad
Ericsson
6210 Spine Road
Boulder, CO 80301
USA

Phone: +1 303.473.6963
Email: Wassim.Haddad@ericsson.com

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/