Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: March 20, 2015

C. Zhou
Huawei Technologies
T. Taylor
PT Taylor Consulting
Q. Sun
China Telecom
M. Boucadair
France Telecom

September 16, 2014

Attribute-Value Pairs For Provisioning Customer Equipment Supporting IPv4-Over-IPv6 Transitional Solutions
draft-zhou-dime-4over6-provisioning-04

Abstract

During the transition from IPv4 to IPv6, customer equipment may have to support one of the various transition methods that have been defined for carrying IPv4 packets over IPv6. This document enumerates the information that needs to be provisioned on a customer edge router to support a list of transition techniques based on tunneling IPv4 in IPv6, with a view to defining reusable components for a reasonable transition path between these techniques. To the extent that the provisioning is done dynamically, AAA support is needed to provide the information to the network server responsible for passing the information to the customer equipment. This document specifies Diameter (RFC 6733) attribute-value pairs to be used for that purpose.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

A number of transition technologies have been defined to allow IPv4 packets to pass between hosts and IPv4 networks over an intervening IPv6 network while minimizing the number of public IPv4 addresses that need to be consumed by the hosts. Different operators will deploy different technologies, and sometimes one operator will use more than one technology, depending on what is supported by the available equipment and upon other factors both technical and economic.

Each technique requires the provisioning of some subscriber-specific information on the customer edge device. The provisioning may be by DHCPv6 [RFC3315] or by some other method. This document is indifferent to the specific provisioning technique used, but assumes a deployment in which that information is managed by AAA (Authentication, Authorization, and Accounting) servers. It further assumes that this information is delivered to intermediate network nodes for onward provisioning using the Diameter protocol [RFC6733].

As described below, in the particular case where the Light Weight IPv4 Over IPv6 (LW4o6) [I-D.ietf-softwire-lw4over6] transition method has been deployed, per-subscriber-site information almost identical to that passed to the subscriber site [I-D.ietf-softwire-map-dhcp] or collected from it [I-D.fsc-softwire-dhcp4o6-saddr-opt] also needs to be delivered to the border router serving that site. The Diameter protocol may be used for this purpose too.

This document analyzes the information required to configure the customer edge equipment for the following set of transition methods:

- o Dual-Stack Lite (DS-Lite) [RFC6333],
- o Light Weight IPv4 Over IPv6 (LW4over6) [I-D.ietf-softwire-lw4over6], and
- o Mapping of Address and Port with Encapsulation (MAP-E) [I-D.ietf-softwire-map].

[I-D.softwire-dslite-multicast] specifies a generic solution for delivery of IPv4 multicast services to IPv4 clients over an IPv6 multicast network. The solution was developed with DS-Lite in mind but it is however not limited to DS-Lite. As such, it applies also for LW4over6 and MAP-E. This document analyzes the information required to configure the customer edge equipment for the support of multicast in the context of DS-Lite, MAP, and LW4over6 in particular.

On the basis of those analyses it specifies a number of attribute-value pairs (AVPs) to allow the necessary subscriber-site-specific configuration information to be carried in Diameter.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The abbreviation "CE" denotes the equipment at the customer edge that terminates the customer end of an IPv6 transitional tunnel. This will usually be a router, but could be a host directly connected to the network.

The term "tunnel source address" is used to denote the IPv6 source address used in the outer header of packets sent from the CE through an LW4over6 transitional tunnel to the border router.

2. Description of the Parameters Required By Each Transition Method

This section reviews the parameters that need to be provisioned for each of the transition methods listed above. This enumeration provides the justification for the AVPs defined in the next section.

A means is required to indicate which transition method(s) a given subscriber is allowed to use. The approach taken in this document is to specify grouped AVPs specific to LW4over6 and MAP-E. The operator can control which of these two transition methods a given subscriber uses by ensuring that AAA passes only the grouped AVP relevant to that method. A grouped AVP is unnecessary for Dual-Stack Lite, since (as the next section indicates) AAA has to provide only one parameter. Hence the absence of either of the grouped AVPs indicates that the subscriber equipment will use Dual-Stack Lite. Provisioning of multicast is an orthogonal activity, since it is independent of the transition method.

2.1. Parameters For Dual-Stack Lite (DS-Lite)

DS-Lite is documented in [RFC6333]. The Basic Bridging BroadBand (B4) element at the customer premises needs to be provisioned with the IPv6 address of the AFTR (border router). Optionally, it could also be configured with the IPv4 address of the B4 interface facing the tunnel, where the default value in the absence of provisioning is 192.0.0.2 and valid values are 192.0.0.2 through 192.0.0.7. Provisioning this information through AAA is problematic because it is most likely used in a case where multiple B4 instances occupy the same device. This document therefore assumes that the B4 interface

address is determined by other means (implementation-dependent or static assignment).

2.2. Light Weight IPv4 Over IPv6 (LW4over6)

Light Weight IPv4 Over IPv6 (LW4over6) is documented in [I-D.ietf-softwire-lw4over6]. LW4over6 requires four items to be provisioned to the customer equipment:

- IPv6 address of the border router.

- IPv6 prefix used by the CE to construct the tunnel source address. In the terminology of [I-D.ietf-softwire-lw4over6], this is the IPv6 Binding Prefix.

- an IPv4 address to be used on the external side of the CE; and

- if the IPv4 address is shared, a specification of the port set the subscriber site is allowed to use. Please see the description in Section 2.3. For LW4over6, all three of the parameters 'a', 'k', and PSID described in that section are required. The default value of the offset parameter 'a' is 0.

As discussed in Section 4 of [I-D.ietf-softwire-lw4over6], it is necessary to synchronize this configuration with corresponding per-subscriber configuration at the border router. The border router information consists of the same public IPv4 address and port set parameters that are passed to the CE, bound together with the full /128 IPv6 address (not just the Binding Prefix) configured as the tunnel source address at the CE.

[I-D.fsc-softwire-dhcp4o6-saddr-opt] proposes a means whereby a DHCPv6 server can influence the choice of this address and collect it from the CE. Depending on the provisioning architecture deployed in a given network, it is possible that the tunnel source address is passed to AAA as an intermediate step before the binding information is passed on to the border router.

2.3. Port Set Specification

When an external IPv4 address is shared, LW4over6 and MAP-E restrict the CE to use of a subset of all available ports on the external side. Both transition methods use the the algorithm defined in Appendix B of [I-D.ietf-softwire-map] to derive the values of the port numbers in the port set. This algorithm features three parameters, describing the positioning and value of the Port Set Identifier (PSID) within each port number of the generated set:

- an offset 'a' from the beginning of the port number to the first bit of the PSID;

- the length 'k' of the PSID within the port number, in bits; and

- the value of the PSID itself.

2.4. Mapping of Address and Port with Encapsulation (MAP-E)

Mapping of Address and Port with Encapsulation (MAP-E) is described in [I-D.ietf-softwire-map]. MAP-E requires the provisioning of the following per-subscriber information at the customer edge device:

- the IPv6 address of one or more border routers, or in MAP-E terminology, MAP border relays.

- the unique End-user IPv6 prefix for the customer edge device. This may be provided by AAA or acquired by other means.

- the Basic Mapping Rule for the customer edge device. This includes the following parameters:

  * the rule IPv6 prefix and length;

  * the rule IPv4 prefix and length. A prefix length of 0 indicates that the entire IPv4 address or prefix is coded in the Extended Address (EA) bits of the End-user IPv6 prefix rather than in the mapping rule.

  * the number of EA bits included in the End-user IPv6 prefix;

  * port set parameters giving the set of ports the CE is allowed to use when the IPv4 address is shared. Please see the description of these parameters in Section 2.3. At a minimum, the offset parameter 'a' is required. For MAP-E this has the default value 6. The parameters 'k' and PSID are needed if they cannot be derived from the mapping rule information and the EA bits (final case of Section 5.2 of [I-D.ietf-softwire-map]).

- whether the device is to operate in mesh or hub-and-spoke mode;

- in mesh mode only, zero or more Forwarding Mapping Rules, described by the same set of parameters as the Basic Mapping Rule;

As indicated in Section 5, bullet 1 of the MAP-E document, a MAP CE can be provisioned with multiple End-user IPv6 prefixes, each associated with its own Basic Mapping Rule. This does not change the

basic requirement for representation of the corresponding information in the form of Diameter AVPs, but adds a potential requirement for multiple instances of this information to be present in the Diameter message, differing in the value of the End-user IPv6 prefix (in contrast to the Forward Mapping Rule instances).

The border router needs to be configured with the superset of the Mapping Rules passed to the customer sites it serves. Since this requirement does not require direct coordination with CE configuration in the way LW4over6 does, it is out of scope of the present document. However, the AVPs defined here may be useful if a separate Diameter application is used to configure the border router.

2.5. Parameters For Multicast

[I-D.softwire-dslite-multicast] specifies a generic solution for delivery of IPv4 multicast services to IPv4 clients over an IPv6 multicast network. The solution can be in particular deployed in a DS-Lite context, but is also adaptable to LW4over6 and MAP-E. [I-D.ietf-softwire-multicast-prefix-option] specifies how DHCPv6 [RFC3315] can be used to provision multicast-related information, particularly:

- ASM_mPrefix64: the IPv6 multicast prefix to be used to synthesize the IPv4-embedded IPv6 addresses of the multicast groups in the ASM mode.

- SSM_mPrefix64: the IPv6 multicast prefix to be used to synthesize the IPv4-embedded IPv6 addresses of the multicast groups in the SSM mode.

- uPrefix64: the IPv6 unicast prefix to be used in SSM mode for constructing the IPv4-embedded IPv6 addresses representing the IPv4 multicast sources in the IPv6 domain. uPrefix64 may also be used to extract the IPv4 address from the received multicast data flows. The address mapping follows the guidelines documented in [RFC6052].

2.6. Summary and Discussion

It appears that two items are common to the different transition methods and the corresponding AVPs to carry them can be reused:

- a representation of the IPv6 address of a border router;

- A set of prefixes for delivery of multicast services to IPv4 clients over an IPv6 multicast network.

[RFC6519] sets a precedent for representation of the IPv6 address of a border router as an FQDN. This can be dereferenced to one or more IP addresses by the provisioning system before being passed to the customer equipment, or left as an FQDN as it as in [RFC6334].

The remaining requirements are transition-method-specific:

- for LW4over6, a representation of a binding between (1) either the IPv6 Binding Prefix or a full /128 IPv6 address, (2) a public IPv4 address, and (3) (if the IPv4 address is shared) a port set identifier;

- for MAP-E, a representation of the unique End-user IPv6 prefix for the CE, if not provided by other means;

- for MAP-E, a representation of a Mapping Rule;

- for MAP-E, an indication of whether mesh mode or hub-and-spoke mode is to be used.

3. Attribute-Value Pair Definitions

This section provides the specifications for the AVPs needed to meet the requirements summarized in Section 2.6. Within the context of their usage, all of these AVPs MUST have the M bit set and the V bit cleared.

3.1. Common Prefix Data Format

A number of the AVPs in this section convey prefixes, and in one case either a prefix or a full address. They all have the same format. Rather than repeat the format in each case, it is specified once here and referred to henceforward as the common prefix data format.

The common prefix data format is an extension of the Address data format defined in Section 4.3.1 of [RFC6733]. Like the Address data format, it is derived from the OctetString basic AVP format. As well as an AddressType, it contains a PrefixLength field. The detailed specification is as follows:

- As with the Address data format, the first two octets represent the AddressType, which contains an Address Family, defined in [IANAADFAM].

- The next two octets are interpreted as a 16-bit unsigned integer representing the PrefixLength.

- o The remaining octets present the prefix or address, most significant octet first. If the prefix does not extend to an octet boundary, the low-order bits of the final octet MUST be padded with zeroes.

3.2. Border-Router-Name AVP

Following on the precedent set by [RFC6334] and [RFC6519], this document identifies a border router using an FQDN rather than an address. The Border-Router-Name AVP (AVP Code TBD01) is of type OctetString. The rules for encoding the FQDN are the same as those for the FQDN variant of the derived type DiameterIdentity (Section 4.3.1 of [RFC6733]).

3.3. 64-Multicast-Attributes AVP

The 64-Multicast-Attributes AVP (AVP Code TBD13) is of type Grouped. It contains the multicast-related prefixes needed for providing IPv4 multicast over IPv6 using DS-Lite, MAP-E, or LW4over6, as specified in [I-D.softwire-dslite-multicast].

The syntax is shown in Figure 1.

```
        64-Multicast-Attributes  ::= < AVP Header: TBD13 >
                       [ ASM-Prefix64 ]
                       [ SSM-Prefix64 ]
                       [ Unicast-Prefix64 ]
                      *[ AVP ]
```

Figure 1: 64-Multicast-Attributes AVP

If either ASM-Prefix64 or SSM-Prefix64 or both are present, Unicast-Prefix64 MUST also be present.

3.3.1. ASM-Prefix64 AVP

The ASM-Prefix64 AVP (AVP Code TBD14) conveys the value of ASM_mPrefix64 as identified in Section 2.1 and specified in [I-D.softwire-dslite-multicast]. The ASM-Prefix64 AVP uses the common prefix data format. The AddressType field MUST be set to 2 (IPv6). Valid prefix lengths in the PrefixLength field are from 24 to 96. The conveyed multicast IPv6 prefix MUST belong to the ASM range.

3.3.2. SSM-Prefix64 AVP

The SSM-Prefix64 AVP (AVP Code TBD14) conveys the value of SSM_mPrefix64 as identified in Section 2.1 and specified in [I-D.softwire-dslite-multicast]. The SSM-Prefix64 AVP uses the common prefix data format. The AddressType field MUST be set to 2 (IPv6). See the next paragraph regarding the PrefixLength field. The conveyed multicast IPv6 prefix MUST belong to the SSM range.

Note that Section 6 of [RFC3306] requires that bits 33-95 of an SSM address in the FF3x range be set to zero, meaning that the prefix length for an SSM prefix is effectively 96. However, Section 1 of [RFC4607] suggests that the lower limit of 32 bits be preserved to allow potential future use of bits 33-95. Hence applications SHOULD accept prefix lengths between 32 and 96 inclusive.

3.3.3. Unicast-Prefix64 AVP

The Unicast-Prefix64 AVP (AVP Code TBD15) conveys the value of uPrefix64 as identified in Section 2.1 and specified in [I-D.softwire-dslite-multicast]. The Unicast-Prefix64 AVP uses the common prefix data format. The AddressType field MUST be set to 2 (IPv6). As specified by [RFC6052], valid values in the PrefixLength field are 32, 48, 56, 64 and 96.

3.4. Tunnel-Source-Pref-Or-Addr AVP

The Tunnel-Source-Pref-Or-Addr AVP (AVP Code TBD02) conveys either the IPv6 Binding Prefix or the tunnel source address on the CE, as described in Section 2.2. The Tunnel-Source-Pref-Or-Addr AVP uses the common prefix data format. The AddressType field MUST be set to 2 (IPv6). Valid values in the PrefixLength field are from 0 to 128 (full address).

This AVP is defined separately from the LW4over6-Binding AVP (which includes it) to provide flexibility in the transport of the tunnel source address from the provisioning system to AAA.

3.5. Port-Set-Identifier

The Port-Set-Identifier AVP (AVP Code TBD03) is a structured OctetString with four octets of data, hence a total AVP length of 12. The description of the structure which follows refers to refers to the parameters described in Section 2.3.

- o The first (high-order) octet is the Offset field. It is interpreted as an 8-bit unsigned integer giving the offset 'a' from the beginning of a port number to the beginning of the port

set identifier (PSID) to which that port belongs. Valid values are from 0 to 15.

- o The next octet, the PSIDLength, is also interpreted as an 8-bit unsigned integer and gives the length 'k' in bits of the port set identifier (PSID). Valid values are from 0 to (16 - a). A value of 0 indicates that the PSID is not present (probable case for MAP-E, see Section 2.4), and the PSIDValue field MUST be ignored.

- o The final two octets contain the PSIDValue field. They give the value of the PSID itself, right-justified within the field. That is, the value of the PSID occupies the 'k' lowest-order bits of the PSIDValue field.

3.6. LW4over6-Binding

The LW4over6-Binding AVP (AVP Code TBD04) is of type Grouped. It contains the elements of configuration that constitute the binding between an LW4over6 tunnel and IPv4 packets sent through that tunnel, as described in Section 2.2.

```
LW4over6-Binding  ::= < AVP Header: TBD04 >
                  { Tunnel-Source-Pref-Or-Addr }
                  { LW4over6-External-IPv4-Addr }
                  [ Port-Set-Identifier ]
                 *[ AVP ]
```

Figure 2

The Tunnel-Source-Pref-Or-Addr AVP is defined in Section 3.4 and provides either the Binding Prefix or the full IPv6 tunnel source address. This AVP MUST be present.

The LW4over6-External-IPv4-Addr AVP (AVP Code TBD05) uses the Address derived data format defined in Section 4.3.1 of [RFC6733]. It provides the CE's external IPv4 address within the LW4over6 tunnel associated with the given binding. The AddressType field MUST be set to 1 (IPv4), and the total length of the AVP MUST be 14 octets. This AVP MUST be present.

The Port-Set-Identifier AVP is defined in Section 3.5. It identifies the specific set of ports assigned to the LW4over6 tunnel, when the IPv4 address is being shared.

3.7. MAP-E-Attributes

The MAP-E-Attributes AVP (AVP Code TBD06) is of type Grouped. It contains the configuration data identified in Section 2.4 for all of the mapping rules (Basic and Forwarding) in a single MAP domain. Multiple instances of this AVP will be present if the CE belongs to multiple MAP domains.

```
                 MAP-E-Attributes  ::= < AVP Header: TBD06 >
                        1*{ Border-Router-Name }
                        1*{ MAP-Mapping-Rule }
                          [ MAP-Mesh-Mode ]
                          [ MAP-End-User-IPv6-Prefix ]
                         *[ AVP ]
```

Figure 3

The Border-Router-Name AVP is defined in Section 3.2. It provides the FQDN of a MAP border relay at the edge of the MAP domain to which the containing MAP-E-Attributes AVP relates. At least one instance of this AVP MUST be present.

The MAP-Mapping-Rule AVP is defined in Section 3.8. At least one instance of this AVP MUST be present. If the MAP-E domain supports mesh mode (indicated by the presence of the MAP-Mesh-Mode AVP), additional MAP-Mapping-Rule instances MAY be present. If the MAP-E domain is operating in hub-and-spoke mode, additional MAP-Mapping-Rule instances MUST NOT be present.

The MAP-Mesh-Mode AVP (AVP Code TBD07) uses the OctetString data format but has no data. Hence the AVP length is always 8. The absence of the mesh mode indicator attribute indicates that the CE is required to operate in hub-and-spoke mode.

The MAP-End-User-IPv6-Prefix AVP (AVP Code TBD08) provides the End-user IPv6 prefix assigned to the CE for the MAP domain to which the containing MAP-E-Attributes AVP relates. It uses the common prefix data format defined in Section 3.1. The AddressType field MUST have the value 2 (IPv6). Valid values of the PrefixLength field range from 0 to 128.

The MAP-End-User-IPv6-Prefix AVP is optional because, depending on deployment, the End-user IPv6 prefix may be provided by AAA or by other means. If multiple instances of the MAP-E-Attributes AVP containing the MAP-End-User-IPv6-Prefix AVP are present, each instance of the latter MUST have a different value.

3.8. MAP-Mapping-Rule

The MAP-Mapping-Rule AVP (AVP Code TBD09) is of type Grouped, and is used only in conjunction with MAP-based transition methods. Mapping rules are required both by the MAP border relay and by the CE. The components of the MAP-Mapping-Rule AVP provide the contents of a mapping rule as described in Section 2.4.

The syntax of the MAP-Mapping-Rule AVP is as follows:

```
         MAP-Mapping-Rule  ::= < AVP Header: TBD09 >
                            { Rule-IPv4-Addr-Or-Prefix }
                            { Rule-IPv6-Prefix    }
                            { EA-Field-Length     }
                            { Port-Set-Identifier }
                           *[ AVP ]
```

Figure 4

The Rule-IPv4-Addr-Or-Prefix AVP (AVP Code TBD10) conveys the rule IPv4 prefix and length as described in Section 2.4. It uses the common prefix data format defined in Section 3.1. The AddressType field MUST have the value 1 (IPv4). Valid values of the PrefixLength field range from 0 to 32, based on the different cases identified in Section 5.2 of [I-D.ietf-softwire-map]. This AVP MUST be present.

The Rule-IPv6-Prefix AVP (AVP Code TBD11) conveys the rule IPv6 prefix and length as described in Section 2.4. It uses the common prefix data format defined in Section 3.1. The AddressType field MUST have the value 2 (IPv6). The minimum valid PrefixLength is 0. If the MAP-End-User-IPv6-Prefix AVP is present in the MAP-E-Attributes AVP that encapsulates both that AVP and the MAP-Mapping-Rule AVP instance to which the Rule-IPv6-Prefix AVP belongs, then the maximum value of the latter's PrefixLength field is given by the value of the PrefixLength field in the MAP-End-User-IPv6-Prefix AVP. Otherwise it is 128. This AVP MUST be present.

The EA-Field-Length AVP (AVP Code TBD12) is of type Unsigned32. Valid values range from 0 to 48. See Section 5.2 of [I-D.ietf-softwire-map] for a description of the use of this parameter in deriving IPv4 address and port number configuration. This AVP MUST be present.

The Port-Set-Identifier AVP provides information to identify the specific set of ports assigned to the CE. For more information see Section 2.4and Section 2.3. The Port-Set-Identifier AVP is defined in Section 3.5. It MUST be present.

4. Acknowledgements

Huawei Technologies funded Tom Taylor's work on earlier versions of this document.

5. IANA Considerations

This memo requests to IANA to register the following Diameter AVP codes:

Code	Attribute Name	Reference
TBD01	Border-Router-Name	This document
TBD02	Tunnel-Source-Pref-Or-Addr	This document
TBD03	Port-Set-Identifier	This document
TBD04	LW4over6-Binding	This document
TBD05	LW4over6-External-IPv4-Addr	This document
TBD06	MAP-E-Attributes	This document
TBD07	MAP-Mesh-Mode	This document
TBD08	MAP-End-User-IPv6-Prefix	This document
TBD09	MAP-Mapping-Rule	This document
TBD10	Rule-IPv4-Addr-Or-Prefix	This document
TBD11	Rule-IPv6-Prefix	This document
TBD12	EA-Field-Length	This document
TBD13	64-Multicast-Attributes	This document
TBD14	ASM-Prefix64	This document
TBD15	SSM-Prefix64	This document
TBD16	Unicast-Prefix64	This document

Table 1

6. Security Considerations

The AVPs defined in this document face two threats, both dependent on man-in-the-middle attacks on the Diameter delivery path. The more serious threat is denial of service through modification of the AVP contents leading to misconfiguration. The lesser threat is disclosure of subscriber addresses allowing the attacker to track subscriber activity.

Diameter security is currently provided on a hop-by-hop basis (see Section 2.2 of [RFC6733]). The Diameter end-to-end security problem has not been solved, so man-in-the-middle attacks on Diameter peers along the path are possible. The present document does not propose to solve that general problem, but simply warn that it exists.

7. References

7.1. Normative References

[I-D.ietf-softwire-lw4over6]
Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture (work in progress)", March 2014.

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, "Mapping of Address and Port with Encapsulation (MAP) (work in progress)", January 2014.

[I-D.softwire-dslite-multicast]
Qin, J., Boucadair, M., Jacquenet, C., Lee, Y., and Q. Wang, "Delivery of IPv4 Multicast Services to IPv4 Clients over an IPv6 Multicast Network (work in progress)", March 2014.

[IANAADFAM]
IANA, "Address Family Numbers", <http://www.iana.org/assignments/address-family- numbers>.

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

[RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, August 2002.

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

[RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

7.2. Informative References

[I-D.fsc-softwire-dhcp4o6-saddr-opt]
Farrer, I., Sun, Q., and Y. Cui, "DHCPv4 over DHCPv6 Source Address Option (Work in progress)", June 2014.

[I-D.ietf-softwire-map-dhcp]
Mrugalski, T., Troan, O., Farrer, I., Perrault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for configuration of Softwire Address and Port Mapped Clients (Work in progress)", March 2014.

[I-D.ietf-softwire-multicast-prefix-option]
Boucadair, M., Qin, J., Tsou, T., and X. Deng, "DHCPv6 Option for IPv4-Embedded Multicast and Unicast IPv6 Prefixes", draft-ietf-softwire-multicast-prefix-option-07 (work in progress), September 2014.

[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.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6334] Hankins, D. and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite", RFC 6334, August 2011.

[RFC6519] Maglione, R. and A. Durand, "RADIUS Extensions for Dual-Stack Lite", RFC 6519, February 2012.

Authors' Addresses

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathy.zhou@huawei.com

T. Taylor
PT Taylor Consulting
Ottawa
Canada

Email: tom.taylor.stds@gmail.com

Qiong Sun
China Telecom
P.R.China

Phone: 86 10 58552936
Email: sunqiong@ctbri.com.cn

M. Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com