Softwire Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 23, 2013

Y.C. Cui
Tsinghua University
Q.S. Sun
China Telecom
M.B. Boucadair
France Telecom
T.T. Tsou
Huawei Technologies
Y. Lee
Comcast
I.F. Farrer
Deutsche Telekom AG
September 21, 2012

Lightweight 4over6: An Extension to the DS-Lite Architecture
draft-cui-softwire-b4-translated-ds-lite-08

Abstract

DS-Lite [RFC6333] describes an architecture for transporting IPv4 packets over an IPv6 network. This document specifies an extension to DS-Lite called Lightweight 4over6 which moves the Network Address Translation function from the DS-Lite AFTR to the B4, removing the requirement for a Carrier Grade NAT function in the AFTR. This reduces the amount of centralized state that must be held to a per-subscriber level. In order to delegate the NAPT function and make IPv4 Address sharing possible, port-restricted IPv4 addresses are allocated to the B4s.

Table of Contents

1. Introduction

Dual-Stack Lite (DS-Lite, [RFC6333]) defines a model for providing IPv4 access over an IPv6 network using two well-known technologies: IP in IP [RFC2473] and Network Address Translation (NAT). The DS-Lite architecture defines two major functional elements as follows:

Basic Bridging BroadBand element: A B4 element is a function implemented on a dual-stack capable node, either a directly connected device or a CPE, that creates a tunnel to an AFTR.

Address Family Transition Router: An AFTR element is the combination of an IPv4-in-IPv6 tunnel endpoint and an IPv4-IPv4 NAT implemented on the same node.

As the AFTR performs the centralized NAT44 function, it dynamically assigns public IPv4 addresses and ports to requesting host's traffic (as described in [RFC3022]). To achieve this, the AFTR must dynamically maintain per-flow state in the form of active NAPT sessions. For service providers with a large number of B4 clients, the size and associated costs for scaling the AFTR can quickly become prohibitive. It can also place a large NAPT logging overhead upon the service provider in countries where legal requirements mandate this.

This document describes a mechanism called Lightweight 4 over 6 (lw4o6), which provides a solution for these problems. By relocating the NAPT functionality from the centralized AFTR to the distributed B4s, a number of benefits can be realised:

o NAPT44 functionality is already widely supported and used in today's CPE devices. Lw4o6 uses this to provide private<->public NAPT44, meaning that the service provider does not need a centralized NAT44 function.

o The amount of state that must be maintained centrally in the AFTR can be reduced from per-flow to per-subscriber. This reduces the amount of resources (memory and processing power) necessary in the AFTR.

o The reduction of maintained state results in a greatly reduced logging overhead on the service provider.

Operator's IPv6 and IPv4 addressing architectures remain independent of each other as in DS-Lite. Therefore, flexible IPv4/IPv6 addressing schemes can be deployed.

Lightweight 4over6 provides a solution for a hub-and-spoke softwire architecture only. It does not offer direct, meshed IPv4 connectivity between subscribers without packets traversing the AFTR. If this type of meshed interconnectivity is required, [I-D.ietf-softwire-map] provides a suitable solution.

The tunneling mechanism remains the same for DS-Lite and Lightweight 4over6. This document describes the changes to DS-Lite that are necessary to implement Lightweight 4over6. These changes mainly concern the configuration parameters and provisioning method necessary for the functional elements.

This document is an extended case, which covers address sharing for [I-D.ietf-softwire-public-4over6]. It is also a variant of A+P called Binding Table Mode (see Section 4.4 of [RFC6346]).

This document focuses on architectural considerations and particularly on the expected behavior of the involved functional elements and their interfaces. Deployment-specific issues are discussed in a companion document. As such, discussions about redundancy and provisioning policy are out of scope.

2. Conventions

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].

3. Terminology

The document defines the following terms:

Lightweight 4over6 (lw4o6): Lightweight 4over6 is an IPv4-over-IPv6 hub and spoke mechanism, which extends DS-Lite by moving the IPv4 translation (NAPT44) function from the AFTR to the B4.

Lightweight B4 (lwB4): A B4 element (Basic Bridging BroadBand element [RFC6333]), which supports Lightweight 4over6 extensions. An lwB4 is a function implemented on a dual-stack capable node, (either a directly connected device or a CPE), that supports port-restricted IPv4 address allocation, implements NAPT44 functionality and creates a tunnel to an lwAFTR

Lightweight AFTR (lwAFTR): An AFTR element (Address Family Transition Router element [RFC6333]), which supports Lightweight 4over6 extension. An lwAFTR is an IPv4-in-IPv6 tunnel endpoint which maintains per-subscriber address binding only and does not perform a NAPT44 function.

Restricted Port-Set: A non-overlapping range of allowed external ports allocated to the lwB4 to use for NAPT44. Source ports of IPv4 packets sent by the B4 must belong to the assigned port-set. The port set is used for all port aware IP protocols (TCP, UDP, SCTP etc.)

Port-restricted IPv4 Address: A public IPv4 address with a restricted port-set. In Lightweight 4over6, multiple B4s may share the same IPv4 address, however, their port-sets must be non-overlapping.

Throughout the remainder of this document, the terms B4/AFTR should be understood to refer specifically to a DS-Lite implementation. The terms lwB4/lwAFTR refer to a Lightweight 4over6 implementation.

4. Lightweight 4over6 Architecture

The Lightweight 4over6 architecture is functionally similar to DS-Lite. lwB4s and an lwAFTR are connected through an IPv6-enabled network. Both approaches use an IPv4-in-IPv6 encapsulation scheme to deliver IPv4 connectivity services. The following figure shows the data plane with main functional change between DS-Lite and lw4o6:

```
+--------+   +---------+   IPv4-in-IPv6    +-------+      +-------------+
|IPv4 LAN|---|lwB4/NAPT|===================|lwAFTR|------|IPv4 Internet|
+--------+   +---------+                   +-------+      +-------------+
                    ^                          |
                    +-------------------------+
                      NAPT function relocated
                         to lwB4 in lw4o6
```

Figure 1 Lightweight 4over6 Data Plane Overview

There are three main components in the Lightweight 4over6 architecture:

- o The lwB4, which performs the NAPT function and encapsulation/de-capsulation IPv4/IPv6.

- o The lwAFTR, which performs the encapsulation/de-capsulation IPv4/IPv6.

- o The provisioning system, which tells the lwB4 which IPv4 address and port set to use.

The lwB4 differs from a regular B4 in that it now performs the NAPT functionality. This means that it needs to be provisioned with the public IPv4 address and port set it is allowed to use. This information is provided though a provisioning mechanism such as DHCP, PCP or TR-69.

The lwAFTR needs to know the binding between the IPv6 address of each subscriber and the IPv4 address and port set allocated to that subscriber. This information is used to perform ingress filtering upstream and encapsulation downstream. Note that this is per-subscriber state as opposed to per-flow state in the regular AFTR case.

The consequence of this architecture is that the information maintained by the provisioning mechanism and the one maintained by the lwAFTR MUST be synchronized (See figure 2). The details of this synchronization depend on the exact provisioning mechanism and will be discussed in a companion draft.

```
                         +------------+
                 /-------|Provisioning|<-------\
                 |       +------------+        |
                 |                             |
                 V                             V
+---------+   +----------+    IPv4/IPv6      +-------+      +-------------+
|IPv4 LAN|---|lwB4/NAPT|===================|lwAFTR|------|IPv4 Internet|
+---------+   +----------+                   +-------+      +-------------+
```

Figure 2 Lightweight 4over6 Provisioning Synchronization

5. Lightweight B4 Behavior

5.1. Lightweight B4 Provisioning

With DS-Lite, the B4 element only needs to be configured with a single DS-Lite specific parameter so that it can set up the softwire (the IPv6 address of the AFTR). Its IPv4 address can be taken from the well-known range 192.0.0.0/29.

In lw4o6, due to the distributed nature of the NAPT function, a number of lw4o6 specific configuration parameters must be provisioned to the lwB4. These are:

- o IPv6 Address for the lwAFTR (as in DS-Lite)
- o IPv4 External (Public) Address for NAPT44
- o Restricted port-set to use for NAPT44

An IPv6 address from an assigned prefix is also required for the lwB4 to use as the encapsulation source address for the softwire. Normally, this is the lwB4's globally unique WAN interface address which can be obtained via an IPv6 address allocation procedure such as SLAAC, DHCPv6 or manual configuration.

In the event that the lwB4's encapsulation source address is changed

for any reason (such as the DHCPv6 lease expiring), the lwB4's dynamic provisioning process must be re-initiated.

For learning the IPv6 address of the lwAFTR, the lwB4 SHOULD implement the method described in section 5.4 of [RFC6333] and implement the DHCPv6 option defined in [RFC6334]. Other methods of learning this address are also possible.

An lwB4 MUST support dynamic port-restricted IPv4 address provisioning (unlike a DS-Lite B4). Several different mechanisms can be used for provisioning the lwB4 with its port-restricted IPv4 address such as: DHCPv4, DHCPv6, PCP, PPP and IPCP. Some alternatives are mentioned in Appendix A of this document.

In this document, it is RECOMMENDED that the DHCPv4 provisioning method is implemented as it is widely deployed in services providers networks and supports all IPv4 and IPv6 addressing models. The DHCPv4 based provisioning model is described in section 7 of this document.

In the event that the lwB4 receives and ICMPv6 error message (type 1, code 5) originating from the lwAFTR, the lwB4 SHOULD interpret this to mean that no matching entry in the lwAFTR's binding table has been found. The lwB4 MAY then re-initiate the dynamic port-restricted provisioning process. The lwB4's re-initiation policy SHOULD be configurable.

The DNS considerations described in Section 5.5 and Section 6.4 of [RFC6333] SHOULD be followed.

5.2. Lightweight B4 Data Plane Behavior

Several sections of [RFC6333] provide background information on the B4's data plane functionality and MUST be implemented by the lwB4 as they are common to both solutions. The relevant sections are:

5.2. Encapsulation	Covering encapsulation and de-capsulation of tunneled traffic
5.3. Fragmentation and Reassembly	Covering MTU and fragmentation considerations (referencing [RFC2473])
7.1. Tunneling	Covering tunneling and traffic class mapping between IPv4 and IPv6 (referencing [RFC2473] and [RFC4213])

The lwB4 element performs IPv4 address translation (NAPT44) as well as encapsulation and de-capsulation. It runs standard NAPT44 [RFC3022] using the allocated port-restricted address as its external

IPv4 address and port numbers.

Internally connected hosts source IPv4 packets with an [RFC1918] address. When the lwB4 receives such an IPv4 packet, it performs a NAPT44 function on the source address and port by using the public IPv4 address and a port number from the allocated port-set. Then, it encapsulates the packet with an IPv6 header. The destination IPv6 address is the lwAFTR's IPv6 address and the source IPv6 address is the lwB4's IPv6 tunnel endpoint address. Finally, the lwB4 forwards the encapsulated packet to the configured lwAFTR.

When the lwB4 receives an IPv4-in-IPv6 packet from the lwAFTR, it de-capsulates the IPv4 packet from the IPv6 packet. Then, it performs NAPT44 translation on the destination address and port, based on the available information in its local NAPT44 table.

The lwB4 is responsible for performing ALG functions (e.g., SIP, FTP), and other NAPT traversal mechanisms (e.g., UPnP, NAPT-PMP, manual binding configuration, PCP) for the internal hosts. This requirement is typical for NAPT44 gateways available today.

It is possible that a lwB4 is co-located in a host. In this case, the functions of NAPT44 and encapsulation/de-capsulation are implemented inside the host.

If the lwB4 is provisioned with a full port-set (e.g. all ports from 0 to 65535), then it SHOULD behave as a 4 over 6 Initiator as described in [I-D.ietf-softwire-public-4over6].

6. Lightweight AFTR Behavior

6.1. Binding Table Maintenance

The lwAFTR maintains an address binding table containing the binding between the lwB4's IPv6 address, the allocated IPv4 address and restricted port-set. Unlike the DS-Lite extended binding table defined in section 6.6 of [RFC6333] which is a 5-tuple NAT table, each entry in the Lightweight 4over6 binding table contains the following 3-tuples:

- o IPv6 Address for a single lwB4

- o Public IPv4 Address

- o Restricted port-set

The entry has two functions: the IPv6 encapsulation of inbound IPv4 packets destined to the lwB4 and the validation of outbound IPv4-in-IPv6 packets received from the lwB4 for de-capsulation.

The lwAFTR does not perform NAPT and so does not need session entries.

The lwAFTR MUST synchronize the binding information with the port-restricted address provisioning process. If the lwAFTR does not participate in the port-restricted address provisioning process, the binding MUST be synchronized through other methods (e.g. out-of-band static update).

If the lwAFTR participates in the port-restricted provisioning process, then its binding table MUST be created as part of this process.

For all provisioning processes, the lifetime of binding table entries MUST be synchronized with the lifetime of address allocations.

6.2. lwAFTR Data Plane Behavior

Several sections of [RFC6333] provide background information on the AFTR's data plane functionality and MUST be implemented by the lwAFTR as they are common to both solutions. The relevant sections are:

6.2. Encapsulation	Covering encapsulation and de-capsulation of tunneled traffic
6.3. Fragmentation and Reassembly	Fragmentation and re-assembly considerations (referencing [RFC2473])
7.1. Tunneling	Covering tunneling and traffic class mapping between IPv4 and IPv6 (referencing [RFC2473] and [RFC4213])

When the lwAFTR receives an IPv4-in-IPv6 packet from an lwB4, it de-capsulates the IPv6 header and verifies the source addresses and port in the binding table. If both the source IPv4 and IPv6 addresses match a single entry in the binding table and the source port in the allowed port-set for that entry, the lwAFTR forwards the packet to the IPv4 destination.

If no match is found (e.g., no matching IPv4 address entry, port out of range, etc.), the lwAFTR MUST discard the packet. An ICMPv6 type 1, code 5 (source address failed ingress/egress policy) error message MAY be sent back to the requesting lwB4. The ICMP policy SHOULD be configurable.

When the lwAFTR receives an inbound IPv4 packet, it uses the IPv4 destination address and port to lookup the destination lwB4's IPv6 address in its binding table. If a match is found, the lwAFTR encapsulates the IPv4 packet. The source is the lwAFTR's IPv6

address and the destination is the lwB4's IPv6 address from the matched entry. Then, the lwAFTR forwards the packet to the lwB4 natively over the IPv6 network.

If no match is found, the lwAFTR MUST discard the packet. An ICMPv4 type 3, code 1 (Destination unreachable, host unreachable) error message MAY be sent back. The ICMP policy SHOULD be configurable.

The lwAFTR MUST support hairpinning of traffic between two lwB4s, by performing de-capsulation and re-encapsulation of packets. The hairpinning policy MUST be configurable.

If the binding table entry has a full port-set (e.g. all ports from 0 to 65535) allocated for an lwB4 client, then the lwAFTR SHOULD behave as a 4 over 6 concentrator as described in [I-D.ietf-softwire-public-4over6].

7. Provisioning using DHCPv4 over IPv6 Transport

The DHCPv4 based provisioning model uses DHCPv4 format messages within an IPv6 packet as described in [I-D.ietf-dhc-dhcpv4-over-ipv6]. This is used for configuring the lwB4's public IPv4 address and port-set that will be used for the softwire and NAPT44 function.

7.1. lwB4 DHCPv4 Based Provisioning

The lwB4's steps for this configuration model are as follows:

1. The lwB4 learns IPv6 Address of DHCPv4 over IPv6 Server

2. The lwB4 sends a DHCPv4 over IPv6 request (Discover) message

3. The DHCPv4 over IPv6 response contains the public IPv4 address and restricted port-set to configure NAPT44 and the softwire

The lwB4 must implement the Client Relay Agent function described in [I-D.ietf-dhc-dhcpv4-over-ipv6]. This function is responsible for converting the DHCPv4 message's IPv4 transport to an IPv6 transport.

To learn the IPv6 unicast address of the DHCPv4 over IPv6 server or relay, the lwB4 SHOULD implement the DHCPv6 option defined in [I-D .mrugalski-softwire-dhcpv4-over-v6-option].

If the DHCPv4 over IPv6 client has multiple IPv6 addresses assigned, the mechanisms defined in [RFC3484] MUST be applied for selecting the correct address as the source of the DHCPv4 over IPv6 request. A DHCPv4 over IPv6 client embedded within the lwB4 MUST use the same IPv6 address as the data plane encapsulation source address for all DHCPv4 over IPv6 requests.

To implement this provisioning model, the lwB4 MUST support public IPv4 address and restricted port-set allocation over DHCPv4 according to the mechanism described in section 3.1 of [I-D.bajko-pripaddrassign].

7.2. lwAFTR DHCPv4 Based Provisioning

The DHCPv4 over IPv6 based provisioning process can be considered out-of-band from the perspective of the lwAFTR in that the lwAFTR does not need to be directly involved for the mechanism to function correctly. However, the contents of the lwAFTR's binding table MUST be synchronized with the DHCPv4 over IPv6 server.

This is necessary to ensure that the IPv4 address and port-set that is allocated in response to a specific client's DHCP request (e.g. the originating IPv6 address of the request) matches the equivalent entry in the lwAFTR's binding table. If this elements are not kept synchronized, then the lwAFTR will either discard or mis-route packets it receives.

The lwAFTR MAY implement a local DHCPv4 over IPv6 server or Relay Agent as described in [I-D.ietf-dhc-dhcpv4-over-ipv6]. If one of these is implemented, the lwB4s MAY send DHCPv4 over IPv6 messages to the lwAFTR which can then learn the bindings between IPv6 address and IPv4 address with port set directly.

8. ICMP Processing

ICMP does not work in an address sharing environment without special handling [RFC6269]. Due to the port-set style address sharing, Lightweight 4over6 requires specific ICMP message handling not required by DS-Lite.

The following behavior SHOULD be implemented by the lwAFTR to provide ICMP error handling and basic remote IPv4 service diagnostics for a port restricted CPE: for inbound ICMP messages, the lwAFTR MAY behave in two modes:

Either:

1. Check the ICMP Type field.

2. If the ICMP type is set to 0 or 8 (echo reply or request), then the lwAFTR MUST take the value of the ICMP identifier field as the source port, and use this value to lookup the binding table for an encapsulation destination. If a match is found, the lwAFTR forwards the ICMP packet to the IPv6 address stored in the entry; otherwise it MUST discard the packet.

3. If the ICMP type field is set to any other value, then the lwAFTR MUST use the method described in REQ-3 of [RFC5508] to locate the source port within the transport layer header in ICMP packet's data field. The destination IPv4 address and source port extracted from the ICMP packet are then used to make a lookup in the binding table. If a match is found, it MUST forward the ICMP reply packet to the IPv6 address stored in the entry; otherwise it MUST discard the packet.

Or:

o Discard all inbound ICMP messages.

The ICMP policy SHOULD be configurable.

The lwB4 SHOULD implement the requirements defined in [RFC5508] for ICMP forwarding. For ICMP echo request packets originating from the private IPv4 network, the lwB4 SHOULD implement the method described in [RFC6346] and use an available port from its port-set as the ICMP Identifier.

For both the lwAFTR and the lwB4, ICMPv6 MUST be handled as described in [RFC2473].

9. Security Considerations

As the port space for a subscriber shrinks due to address sharing, the randomness for the port numbers of the subscriber is decreased significantly. This means it is much easier for an attacker to guess the port number used, which could result in attacks ranging from throughput reduction to broken connections or data corruption.

The port-set for a subscriber can be a set of contiguous ports or non-contiguous ports. Contiguous port-sets do not reduce this threat. However, with non-contiguous port-set (which may be generated in a pseudo-random way [RFC6431]), the randomness of the port number is improved, provided that the attacker is outside the Lightweight 4over6 domain and hence does not know the port-set generation algorithm.

More considerations about IP address sharing are discussed in Section 13 of [RFC6269], which is applicable to this solution.

10. IANA Considerations

This document does not include an IANA request.

11. Author List

The following are extended authors who contributed to the effort:

Jianping Wu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-62785983
Email: jianping@cernet.edu.cn

Peng Wu
Tsinghua University

Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-62785822
Email: pengwu.thu@gmail.com

Chongfeng Xie
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing 100035
P.R.China

Phone: +86-10-58552116
Email: xiechf@ctbri.com.cn

Xiaohong Deng
France Telecom

Email: xiaohong.deng@orange.com

Cathy Zhou
Huawei Technologies
Section B, Huawei Industrial Base, Bantian Longgang
Shenzhen 518129
P.R.China

Email: cathyzhou@huawei.com

Alain Durand
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089-1206
USA

Email: adurand@juniper.net

Reinaldo Penno
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: repenno@cisco.com

Alex Clauberg
Deutsche Telekom AG
GTN-FM4
Landgrabenweg 151
Bonn, CA 53227
Germany

Email: axel.clauberg@telekom.de

Lionel Hoffmann
Bouygues Telecom
TECHNOPOLE
13/15 Avenue du Marechal Juin
Meudon 92360
France

Email: lhoffman@bouyguestelecom.fr

Maoke Chen
FreeBit Co., Ltd.
13F E-space Tower, Maruyama-cho 3-6
Shibuya-ku, Tokyo 150-0044
Japan

Email: fibrib@gmail.com

12. Acknowledgement

The authors would like to thank Ole Troan, Ralph Droms for their comments and feedback.

This document is a merge of three documents: [I-D.cui-softwire-b4-translated-ds-lite], [I-D.zhou-softwire-b4-nat] and [I-D.penno-softwire-sdnat].

13. References

13.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC5508] Srisuresh, P., Ford, B., Sivakumar, S. and S. Guha, "NAT Behavioral Requirements for ICMP", BCP 148, RFC 5508, April 2009.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P. and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

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

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

[RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, August 2011.

[RFC6431] Boucadair, M., Levis, P., Bajko, G., Savolainen, T. and T. Tsou, "Huawei Port Range Configuration Options for PPP IP Control Protocol (IPCP)", RFC 6431, November 2011.

13.2. Informative References

[I-D.bajko-pripaddrassign]
Bajko, G., Savolainen, T., Boucadair, M. and P. Levis, "Port Restricted IP Address Assignment", Internet-Draft draft-bajko-pripaddrassign-04, April 2012.

[I-D.boucadair-dhcpv6-shared-address-option]
Boucadair, M., Levis, P., Grimault, J., Savolainen, T. and G. Bajko, "Dynamic Host Configuration Protocol (DHCPv6) Options for Shared IP Addresses Solutions", Internet-Draft draft-boucadair-dhcpv6-shared-address-option-01, December 2009.

[I-D.cui-softwire-b4-translated-ds-lite]
Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y. and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture", Internet-Draft draft-cui-softwire-b4-translated-ds-lite-07, July 2012.

[I-D.ietf-dhc-dhcpv4-over-ipv6]
Cui, Y., Wu, P., Wu, J. and T. Lemon, "DHCPv4 over IPv6 Transport", Internet-Draft draft-ietf-dhc-dhcpv4-over-ipv6-03, May 2012.

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R. and P. Selkirk, "Port Control Protocol (PCP)", Internet-Draft draft-ietf-pcp-base-26, June 2012.

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Zhai, Y., Matsushima, S. and T. Murakami, "Mapping of Address and Port (MAP)", Internet-Draft draft-ietf-softwire-map-01, June 2012.

[I-D.ietf-softwire-public-4over6]
Cui, Y., Wu, J., Wu, P., Vautrin, O. and Y. Lee, "Public IPv4 over IPv6 Access Network", Internet-Draft draft-ietf-softwire-public-4over6-02, July 2012.

[I-D.mrugalski-softwire-dhcpv4-over-v6-option]
Mrugalski, T. and P. Wu, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for DHCPv4 over IPv6 Transport", Internet-Draft draft-mrugalski-softwire-dhcpv4-over-v6-option-00, April 2012.

[I-D.penno-softwire-sdnat]
Penno, R., Durand, A., Hoffmann, L. and A. Clauberg, "Stateless DS-Lite", Internet-Draft draft-penno-softwire-sdnat-02, March 2012.

[I-D.tsou-pcp-natcoord]
Sun, Q., Boucadair, M., Deng, X., Zhou, C. and T. Tsou, "Lightweight 4over6 Port-set Allocation: Using PCP To Coordinate Between the CGN and Home Gateway", Internet-Draft draft-tsou-pcp-natcoord-07, July 2012.

[I-D.wu-dhc-port-set-option]
Wu, P., Lee, Y., Sun, Q. and T. Lemon, "Dynamic Host Configuration Protocol (DHCP) Options for Port Set Assignment", Internet-Draft draft-wu-dhc-port-set-option-00, April 2012.

[I-D.zhou-softwire-b4-nat]
Zhou, C., Boucadair, M. and X. Deng, "NAT offload extension to Dual-Stack lite", Internet-Draft draft-zhou-softwire-b4-nat-04, October 2011.

Appendix A. Alternatives for Port-Restricted Address Allocation

Besides DHCPv4, other protocols for address and port-set provisioning MAY also be implemented. Some possible alternatives include:

- o PCP[I-D.ietf-pcp-base]: a lwB4 MAY use [I-D.tsou-pcp-natcoord] to retrieve a restricted IPv4 address and a set of ports.

- o DHCPv6: the DHCPv6 protocol MAY be extended to support port-set allocation [I-D.boucadair-dhcpv6-shared-address-option], along with IPv6-mapped IPv4 address allocation.

- o IPCP: IPCP MAY be extended to carry the port-set (e.g., [RFC6431]).

In a Lightweight 4over6 domain, the same provisioning mechanism MUST be enabled in the lwB4s, the AFTRs and the provisioning server.

Authors' Addresses

Yong Cui
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
P.R.China

Phone: +86-10-62603059
Email: yong@csnet1.cs.tsinghua.edu.cn

Qiong Sun
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing, 100035
P.R.China

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

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange.com

Tina Tsou
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-4424
Email: tena@huawei.com

Yiu L. Lee
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: yiu_lee@cable.comcast.com

Ian Farrer
Deutsche Telekom AG
GTN-FM4,Landgrabenweg 151
Bonn, NRW 53227
Germany

Email: ian.farrer@telekom.de