Network Working Group C. Liu
Internet-Draft Q. Sun
Intended status: Informational J. Wu
Expires: September 22, 2016 Tsinghua University
I. Farrer
Deutsche Telekom AG
March 21, 2016

Dynamic IPv4 Provisioning for Lightweight 4over6
draft-liu-softwire-lw4over6-dynamic-provisioning-01

Abstract

Lightweight 4over6 [RFC7596] is an IPv4 over IPv6 hub-and-spoke mechanism that provides overlay IPv4 services in an IPv6-only access network. It uses a deterministic, DHCPv6 based method for the provisioning of IPv4 addresses and port sets to customer CE devices. This document describes how existing specifications can be used for the dynamic IPv4 provisioning of Lightweight 4over6, based on DHCPv4 over DHCPv6 [RFC7341].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Architecture Overview 4
4. Lightweight4over6 Dynamic Provisioning Process 5
4.1. Client IPv6 Addressing 5
4.2. DHCPv6 Configuration 5
4.3. DHCPv4 over DHCPv6 Function 5
4.4. lwAFTR Binding Table Maintenance 5
4.4.1. Co-located lwAFTR/DHCP4o6 Binding Table Maintenance . 6
5. Security Considerations 6
5.1. Data Retention Requirements 6
6. IANA Considerations 7
7. References 7
7.1. Normative References 7
7.2. Informative References 7
Authors' Addresses 8

1. Introduction

Lightweight 4over6 [RFC7596] provides IPv4 access over an IPv6 network in hub-and-spoke softwire architecture. In Lightweight 4over6, each Lightweight B4 (lwB4) is assigned a full, or shared (port-restricted) IPv4 address to be used for IPv4 communication. Provisioning the lwB4 with its IPv4 address, port set and other parameters necessary for building the softwire is the core function of the Lightweight 4over6 control plane.

[RFC7596] describes the use of DHCPv6 for deterministic IPv4 provisioning. The IPv4 address, port set ID (PSID) and address of the lwAFTR are carried in DHCPv6 options defined in [RFC7598].

However, the deterministic provisioning of the IPv4 parameters imposes restrictions on the deployment:

o The IPv4 address' life time is bound to the client's IPv6 tunnel

endpoint life time

o The tunnel must be initiated from a fixed and predictable /64 prefix in the home network topology

o The IPv4 address and PSID need to be embedded into the IID of the clients' /128 IPv6 address

o IPv4 address resources are permanently reserved for a client whether it is active or not. This results in less efficient public IPv4 address usage

This document describes the deployment of Lightweight 4over6 using DHCPv4 over DHCPv6 for dynamic IPv4 address provisioning. The main advantages of using a dynamic provisioning model over a deterministic model are as follows:

o No inherent restrictions on the IPv6 source address within the customer internal network that the client uses for sourcing its tunneled traffic

o The lifetimes of IPv6 and IPv4 addresses are decoupled, allowing for more flexibility in the service provider's addressing policy

o Inactive clients' addresses can be released/reclaimed for allocation to active clients, so more efficient address usage is possible

Since DHCPv4 over IPv4 cannot be used natively in a single stack IPv6 network, DHCPv4 over DHCPv6 (DHCP4o6) [RFC7341] allows DHCPv4 functionality to be trasported over a pure in IPv6 network by placing DHCPv4 messages within DHCPv6 messages.

[I-D.fsc-softwire-dhcp4o6-saddr-opt] defines a DHCP4o6 based mechanism for the lwB4 to inform the server of its IPv6 tunnel source address.

The architecture which is described in this document can be implemented with or without the sharing of IPv4 addresses between multiple clients. If IPv4 address sharing is required, then [RFC7618] describes the changes necessary extensions to the DHCPv4

server and client provisioning for the allocation and lease management of shared IPv4 addresses.

2. Terminology

Terminology defined in [RFC7341] and [RFC7596] is used extensively throughout this document.

Unless stated otherwise, the term "lwB4" should be understood to mean a stateful lwB4 using DHCP4o6 for dynamic IPv4 provisioning.

3. Architecture Overview

There are four functional elements which make up the architecture. Although these are shown as being seperate entities, it is possibile that one or more of the operator side functions might be performed by a single device.

```
                 ________     __________
                |        |   |          |
                | DHCPv6 |   | DHCP4o6 |
                | Server |   |  Server  |
                |________|   |__________|
                    ^       /            \
                  1 |    2 /              \ 3
                 ___v____ /                \ ________
                |        |                  |        |
                |  lwB4  |<---------------->| lwAFTR |
                |________|    Data Plane    |________|
```

The numbers in each of the provisioning flows are described in more detail below.

Figure 1: Dynamic lw4o6 Provisioning Model

The process for provisioning Lightweight 4over6 using DHCP4o6 is as follows:

1. The lwB4 uses DHCPv6[RFC3315] to obtain its basic configuration. OPTION_DHCP4_O_DHCP6_SERVER (88) is included in the client's ORO.

The IPv6 address of at least one DHCP4o6 server is given in the response.

2. The client sends a DHCPv4 DISCOVER message in a DHCP4o6 message to the DHCP4o6 server(s). The rest of the message flow proceeds as per Section 5 of [I-D.fsc-softwire-dhcp4o6-saddr-opt]. The result is that the client is provisioned with the Ipv6 address of the lwAFTR, an IPv4 address and (optionally) a range of source ports. The server has the /128 IPv6 address that the client will use its tunnel source associated with the IPv4 lease.

3. lwAFTR binding table maintenance is achieved by using NETCONF [RFC6241]. The YANG model for lw4o6 is defined in [I-D.sun-softwire-yang].

4. Lightweight4over6 Dynamic Provisioning Process

This section describes the dynamic provisioning process of Lightweight 4over6 in more detail.

4.1. Client IPv6 Addressing

Before attempting the DHCP4o6 configuration process to obtain IPv4 configuration, the lwB4 needs to have an IPv6 address of a suitable scope to allow communication with the lwAFTR (e.g. a link-local address cannot be used). There are no restrictions on how the client's IPv6 address is provisioned, (e.g. SLAAC, DHCPv6 or some other mechanisms).

4.2. DHCPv6 Configuration

The initial configuration step is for the lwB4 to perform DHCPv6 to retrieve the DHCP 4o6 server's IPv6 address. The DHCPv6 server provides the DHCP 4o6 server's IPv6 address by OPTION_DHCP4_O_DHCP6_SERVER as defined in [RFC7341].

4.3. DHCPv4 over DHCPv6 Function

Once the lwB4 has acquired the IPv6 address of the DHCP4o6 server, stateful configuration using DHCP4o6 is performed to obtain an IPv4 address and port set. The PSID is conveyed using DCHPv4 OPTION_V4_PORTPARAMS (159) as decribed in [RFC7618]. The lwB4 includes one of its active IPv6 addresses as the IPv6 tunnel source address in this message flow with the DHCP 4o6 server, and receives the lwAFTR's tunnel address through DHCP4o6, as described in section 4 of [I-D.fsc-softwire-dhcp4o6-saddr-opt].

4.4. lwAFTR Binding Table Maintenance

In figure 1 above, the lwAFTR is not co-located with the DHCP 4o6 server. With this architecture, NETCONF [RFC6241] is used for syncronising client DHCP4o6 provisioning and the lwAFTR binding table. A YANG model for lw4o6 is defined in [I-D.sun-softwire-yang]. In this deployment model, the DHCP4o6 server and lwAFTR also implements a NETCONF server. When an IPv4 leasing event occurs (e.g. DHCPACK/DHCPRELEASE messages), the DHCP4o6 server informs the operator's centralised configuration database of the change.

The operator's configuration database will then use NETCONF to update the lwAFTR of the relevant change by adding or removing the binding table entry which matches the DHCP4o6 server's IPv4 address lease.

4.4.1. Co-located lwAFTR/DHCP4o6 Binding Table Maintenance

In this deployment scenario, the DHCP4o6 and lwAFTR functions are both active on the same device. Here, the lwAFTR maintains its binding table as per section 6.1 of [RFC7596] and is synchronized with DHCP4o6 process. The following DHCP4o6 messages trigger binding table modification:

DHCPACK: Generated by the DHCP4o6 server, triggers lwAFTR to add a new entry or modify an existing entry.

DHCPRELEASE: Generated by lwB4, triggers lwAFTR to delete an existing entry.

When the DHCP4o6 server generates a DHCPACK message, the lwAFTR looks

up the binding table using the lwB4's IPv4 address and PSID as index. If there is an existing entry found, the lwAFTR updates the IPv6 address and lifetime fields of the entry; otherwise the lwAFTR creates a new entry accordingly. When the DHCP4o6 server receives a DHCPRELEASE message , the lwAFTR looks up the binding table using the lwB4's IPv6 address, IPv4 address and PSID as index. The lwAFTR deletes the entry either by removing it from the binding table or by marking the lifetime field with an invalid value (e.g. 0).

5. Security Considerations

Security considerations in [RFC7596] and [RFC7341] are also relevant here.

The DHCP message triggered binding table maintenance may be used by an attacker to send fake DHCP messages to lwAFTR. The operator network should deploy [RFC2827] to prevent this kind of attack.

5.1. Data Retention Requirements

In some countries, regulations require a service providers to retain the necessary information to link IP information to a specific customer. With a deterministic provisioning model, any individual client will always receive a pre-determined set of IPv4 provisioning requirements. In this scenario, the logging requirement may be met by retaining information on how the DHCPv6 server has been pre-provisioned, with timestamp information on when changes to the pre-provisioning have come into effect.

The dynamic provisioning model that is described in this document brings an additional logging requirement to the service provider: The retention logs holding allocated IPv4 address and ports, the associated IPv6 tunnel endpoint and timestamps marking the start and

end of the lease. This is a higher logging overheard than deterministic provisioning, but is in line with the amount of logging that service providers currently have.

6. IANA Considerations

This document does not include an IANA request.

7. References

7.1. Normative References

[I-D.fsc-softwire-dhcp4o6-saddr-opt]
Farrer, I., Sun, Q., and Y. Cui, "DHCPv4 over DHCPv6 Source Address Option", draft-fsc-softwire-dhcp4o6-saddr-opt-04 (work in progress), November 2015.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <http://www.rfc-editor.org/info/rfc2827>.

[RFC7341] Sun, Q., Cui, Y., Siodelski, M., Krishnan, S., and I. Farrer, "DHCPv4-over-DHCPv6 (DHCP 4o6) Transport", RFC 7341, DOI 10.17487/RFC7341, August 2014, <http://www.rfc-editor.org/info/rfc7341>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <http://www.rfc-editor.org/info/rfc7596>.

[RFC7618] Cui, Y., Sun, Q., Farrer, I., Lee, Y., Sun, Q., and M. Boucadair, "Dynamic Allocation of Shared IPv4 Addresses", RFC 7618, DOI 10.17487/RFC7618, August 2015, <http://www.rfc-editor.org/info/rfc7618>.

7.2. Informative References

[I-D.sun-softwire-yang]
Sun, Q., Wang, H., Cui, Y., Farrer, I., Boucadair, M., and R. Asati, "YANG Data Model for IPv4-in-IPv6 Softwire", draft-sun-softwire-yang-04 (work in progress), October 2015.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins,

C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

[RFC7598] Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients", RFC 7598, DOI 10.17487/RFC7598, July 2015, <http://www.rfc-editor.org/info/rfc7598>.

Authors' Addresses

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

Phone: +86-10-6278-5822
Email: cong-liu13@mails.tsinghua.edu.cn

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

Phone: +86-10-6278-5822
Email: sunqi@csnet1.cs.tsinghua.edu.cn

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

Phone: +86-10-6278-5983
Email: jianping@cernet.edu.cn

Ian Farrer
Deutsche Telekom AG
CTO-ATI,Landgrabenweg 151
Bonn, NRW 53227
Germany

Email: ian.farrer@telekom.de