DHC WG
Internet-Draft
Updates: 2131 (if approved)
Intended status: Standards Track
Expires: December 27, 2013

I. Farrer
Deutsche Telekom AG
June 25, 2013

Dynamic Allocation of Shared IPv4 Addresses using DHCPv4 over DHCPv6
draft-farrer-dhc-shared-address-lease-00

Abstract

This memo describes an update to [RFC2131], which enables the dynamic leasing of shared IPv4 addresses and layer 4 source ports to DHCPv4 over DHCPv6 clients [I-D.ietf-dhc-dhcpv4-over-dhcpv6]. Shared addressing allows a single IPv4 address to be allocated to multiple, active clients simulataneously. Clients sharing the same address are then differentiated by unique L4 source ports.

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 RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 27, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Functional Overview 3
3. Client-server Interaction 4
  3.1. Allocating a Shared, Dynamic IPv4 Address 4
  3.2. Reusing a Previously Allocated Shared, Dynamic IPv4 address 5
4. Client Usage of a Shared Address 5
5. Additional Changes to [RFC2131] Behaviour 6
6. DHCPv4 Port Parameters Option 6
7. Specfic Behaviour for Softwire Clients 7
8. DHCPv4 over DHCPv6 Source Address Option 9
9. Security Considerations 9
10. IANA Considerations 9
11. Acknowledgements 10
12. References 10
  12.1. Normative References 10
  12.2. Informative References 10
Author's Address 11

1. Introduction

[I-D.ietf-dhc-dhcpv4-over-dhcpv6] introduces a "Unified Server" - a DHCP server capable of servicing both DHCPv6 [RFC3315] and DHCPv4 over DHCPv6 requests. This enables the provisioning of DHCPv4 based configuration to IPv6 connected clients over IPv6 only transport networks.

One of the benefits of the DHCPv4 over DHCPv6 based approach is that it allows the dynamic leasing of IPv4 addresses to clients, based on existing mechanisms for address lease management available in DHCPv4 servers. This can make much more efficient use of remaining public IPv4 addresses than static pre-allocation based approaches as only IPv4 clients which are currently active need to be allocated addresses.

Shortages of available public IPv4 addresses mean that it is not always possible for operators to allocate a full IPv4 address to every active customer simultaneously. This problem may be particularly acute whilst the operator is in the migration phase from a native IPv4 network to a native IPv6 network with IPv4 provided as an overlay service. Such migrations are likely to increase the requirement on public IPv4 addresses so that both existing and transition networks can be provided for.

IPv4 address sharing provides a way of easing this problem. A shared IP address is a single IPv4 address which is allocated to a number of clients simultaneously. The clients differentiate themselves through the use of layer 4 source ports, which are unique for each client sharing a single IPv4 address, known as a Port Set ID (PSID).

The client will generally utilize these restricted source ports by implementing a NAPT44 function, translating traffic from the original source address and unrestricted port range to the allocated shared IPv4 address and unique restricted port range.

This technique is also referred to as "extended" or "A+P" addressing [RFC6346].

Due to the nature of address sharing in this manner, it is only suitable for some very specific architectures, such as those described in [I-D.ietf-softwire-map] and [I-D.ietf-softwire-lw4over6]. Use of shared addressing in other, more traditional deployment architectures must be avoided due to the fundamental incompatibilities of assigning a the same /32 IPv4 address to multiple clients such as when they are attached to the same layer 2 segment. Some rules for the use of the allocated shared dynamic address are provided in Section 4 below.

[RFC2131] describes DHCPv4, providing a method for dynamically allocating IPv4 addresses to clients based on three different mechanisms:

- o Automatic Address Allocation
- o Dynamic Address Allocation
- o Manual Address Allocation

This memo describes how the dynamic allocation mechanism can be adapted for allocating shared IPv4 addresses for use by DHCPv4 over DHCPv6 clients and Unified Servers. The approach is referred to as "shared, dynamic" addressing throughout this memo.

2. Functional Overview

From a functional perspective, shared, dynamic allocation by the unified server is quite similar to the normal DHCPv4 server dynamic allocation process. The underlying difference is that the unified server MAY allocate the same IPv4 address to more than one DHCPv4 over DHCPv6 client simultaneously, providing that each address allocation also includes a range of layer 4 source ports unique to that address (i.e. each PSID may only be allocated once per /32 address).

To enable this, the DHCPv4 over DHCPv6 client needs to be extended to implement OPTION_PORTPARAMSV4 (described below). This is used to indicate to the Unified server that it is capable of supporting shared, dynamic addressing and also for conveying the allocated PSID.

The server must be extended to implement OPTION_PORTPARAMSV4 so that clients able to support shared, dynamic address leasing can be identified and so that shared, dynamic addresses can be allocated and their leases maintained. The server must also manage unique client leases based on the address and PSID tuple, instead of just IPv4 address.

3. Client-server Interaction

The following sections describe the changes to the client and server necessary to implement dynamic, shared address allocation.

3.1. Allocating a Shared, Dynamic IPv4 Address

Section 3.1 of [RFC2131] describes the client-server interaction for allocating an IPv4 address. The process described below detail the required changes for the dynamic, shared addressing mechanism.

The following message flow is transported within the DHCPv6 OPTION_BOOTP_MSG message.

1. The client constructs its DHCPv4 DHCPDISCOVER message (transported within the DHCPv6 BOOTPRELAYV6 message). The DHCPDISCOVER message MUST include the following options:

   * A client Identifier (constructed as per [RFC4361]
   * OPTION_PORTPARAMSV4 (described below)

   The client MAY insert a non-zero value in the PSID-Len field within OPTION_PORTPARAMSV4 to indicate the preferred size of the restricted port range allocation to the unified server.
2. Each Unified server which receives the DHCPDISCOVER message containing OPTION_PORTPARAMSV4 within the BOOTPRELAYV6 message may respond with a DHCPOFFER message which contains an available

IPv4 address in the 'yiaddr' field. The response MUST also include OPTION_PORTPARAMSV4 containing a restricted port-range. If the received OPTION_PORTPARAMSV4 field contains a non-zero PSID-Len field, the Unified server MAY allocate a port set of the requested size to the client (depending on policy).

3. The client evaluates all received DHCPOFFER messages and selects one based on the configuration parameters received (e.g. the size of the offered port set). The client then sends a DHCPREQUEST containing a server identifier and the corresponding OPTION_PORTPARAMSV4 received in the DHCPOFFER message.
4. The server identified in the DHCPREQUEST message (via the siaddr field) creates a binding for the client. The binding includes the client identifier, the IPv4 address and the PSID. These parameters are used by both the server and the client to identify the lease referred to in any future DHCP messages. The server responds with a DHCPACK message containing the configuration parameters for the requesting client.
5. The client receives the DHCPACK message with the configuration parameters. The client MUST NOT perform a final check on the address, such as ARPing for a duplicate allocated address.
6. If the client chooses to relinquish its lease by sending a DHCPRELEASE message, the client MUST include the original client identifier, the leased network address and the allocated restricted source ports included in OPTION_PORTPARAMSV4.

3.2. Reusing a Previously Allocated Shared, Dynamic IPv4 address

If the client remembers the previously allocated address and restricted port range, then the process described in section 3.2 of [RFC2131] must be followed. OPTION_PORTPARAMSV4 MUST be included in the message flow, with the client's requested port set being included in the DHCPDISCOVER message.

4. Client Usage of a Shared Address

As a single IPv4 address is being shared between a number of different clients, the allocated shared address is only suitable for certain functions. The client MUST implement a function to ensure that only the allocated layer 4 ports of the shared IPv4 address are used for sourcing new connections.

The client MUST apply the following rules for any traffic to or from the shared /32 IPv4 address:

- Only port-aware protocols MUST be used.
- All connections originating from the shared IPv4 address MUST use a source port taken from the allocated restricted port range.

- o The client MUST NOT accept inbound connections with destination ports outside of the allocated restricted port range.

In order to prevent addressing conflicts which could arise from the allocation of the same IPv4 addreses, the client MUST NOT configure the received restricted IPv4 address on-link.

In the event that the DHCPv4 over DHCPv6 configuration mechanism fails for any reason, the client MUST NOT configure an IPv4 link-local address [RFC3927](taken from the 169.254.0.0/16 range).

The mechanism by which a client implements these rules is outside of the scope of this document.

5. Additional Changes to [RFC2131] Behaviour

The following change to the behaviour described in [RFC2131] is also necessary in order to implement dynamic shared address allocation.

Section 2.2 The client MUST NOT probe a newly received IPv4 address (e.g. with ARP) to see if it is in use by another host.

6. DHCPv4 Port Parameters Option

The Port Paramaters Option for DHCPv4 specifies the restricted set of layer 4 source ports that are necessary to dynamically allocate a shared address. The option uses the same fields as the MAP Port Parameters Option described in Section 4.4 of [I-D.ietf-softwire-map-dhcp], implemented as a DHCPv4 option. This is to maintain compatibility with existing implementations.

The construction and usage of OPTION_PORTPARAMSV4 is

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| option-code   |  Length       |    offset     |   PSID-Len    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              PSID             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: DHCPv4 Port Parameters Option

- o option-code: OPTION_PORTPARAMSV4 (TBA)
- o option-length: 3
- o offset: (PSID offset) 8 bits long field that specifies the numeric value for the MAP algorithm's excluded port range/offset bits (A-bits), as per section 5.1.1 in [I-D.ietf-softwire-map].

Allowed values are between 0 and 16, with the default value being 6 for a MAP client. This parameter is unused by a Lightweight 4over6 client and should be set to 0.

- o PSID-len: Bit length value of the number of significant bits in the PSID field. (also known as 'k'). When set to 0, the PSID field is to be ignored. After the first 'a' bits, there are k bits in the port number representing valid of PSID. Subsequently, the address sharing ratio would be 2^k.
- o PSID: Explicit 16-bit (unsigned word) PSID value. The PSID value algorithmically identifies a set of ports assigned to a CE. The first k-bits on the left of this 2-octets field is the PSID value. The remaining (16-k) bits on the right are padding zeros.

[I-D.ietf-softwire-map] (Section 5.1) provides a full description of how the PSID is interpreted by the client.

When receiveing the Port Parameters option with an explicit PSID, the client MUST use apply this PSID to the interface being configured by DHCPv4 over DHCPv6.

7. Specfic Behaviour for Softwire Clients

[DISCUSSION NOTE: Should the following section be moved into a separte draft as it is more softwire specific?]

Current mechanisms suitable for extending to incorporate dynamic, shared IPv4 addressing include [I-D.ietf-softwire-map] and [I-D.ietf-softwire-lw4over6]. For these mechanisms to function, the operator needs information about the clients allocated IPv4 address, PSID and also the /128 IPv6 prefix which the client will use as the IPv4 in IPv6 tunnel endpoint. This binding information is used by other functional elements in the operator's network (e.g. a softwire tunnel concentrator) for correctly routing traffic to and from clients.

For the shared, dynamic address allocation model, a two-way communication model is necessary so that the Unified Server can indicate to the client the preferred prefix to use for binding the received IPv4 configuration and sourcing tunnel traffic.

As the Unified server is managing the leasing of DHCPv4 to clients, it holds the most accurate IPv4 lease information available in the network. It follows that the unified server should also hold information about the /128 IPv6 prefixes in use by active clients as tunnel endpoints, so that the unified server contains a single comprehensive dynamic IPv4/IPv6 binding table.

To achieve this, the client also needs to inform the Unified server of the /128 prefix that it has bound the IPv4 configuration to.

To provide this function, the DHCPV4oDHCPv6 client MAY implement OPTION_DHCPV4_O_DHCPV6_SADDR (defined below). This option is included by the client within OPTION_BOOTP_MSG messages and is used alongside the DHCPv4 request process.

The option comprises of two IPv6 prefixes (with associated prefix length fields):

cipv6-prefix-hint Sent by the server to indicate to the client the preferred prefix to bind IPv4 configuration to. If this field contains a prefix, the client MUST perform a longest prefix match betweeen cipv6 -prefix-hint and all prefixes configured on the device. The selected prefix MUST then be used to bind the received IPv4 configuration to. If this field is left blank, then the client MAY select any valid IPv6 prefix.

cipv6-bound-prefix Used by the client to inform the Unified Server of the IPv6 prefix that it has bound the IPv4 configuration to. This SHOULD be a /128 prefix configured on the client.

If used, this option MUST be present within all future OPTION_BOOT_MSG transactions between the client and the server.

The message flow for this process (aligned to the DHCPv4 address allocation process) is as follows:

DHCPv4 Message	cipv6-prefix-hint	cipv6-hin tlen	cipv6-bound-prefix	cipv6-boun dlen
DHCPDISCOVER	blank	blank	blank	blank
DHCPOFFER	Preferred prefix	Preferred prefix Length	blank	blank
DHCPREQUEST	Preferred prefix	Preferred prefix length	Bound prefix	Bound prefix Length
DHCPACK	Preferred prefix	Preferred prefix	Bound prefix	Bound prefix

```
|           |               |   length  |              |   Length   |
+-----------+---------------+-----------+--------------+------------+
```

Table 1: IPv6/IPv4 Binding Message Flow

8. DHCPv4 over DHCPv6 Source Address Option

The DHCPv4 over DHCPv6 Source address option is used by the Unified server to indicate an IPv6 prefix to use for DHCPv4 over DHCPv6 functions. It is also used by the client to inform the unified server of the prefix it has selected for binding DHCPv4 over DHCPv6 functions to.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| OPTION_DHCPV4_O_DHCPV6_SADDR  |          Length               |
+-------------------------------+-------------------------------+
.            cipv6-prefix-hint (variable length)                .
+-----------------------------------------------------------------+
| cipv6-hintlen |          cipv6-bound-prefix                   .
+---------------+          (variable length)    +---------------+
.                                                |cipv6-boundlen |
+-----------------------------------------------------------------+
```

- o option-code: OPTION_DHCPV4_O_DHCPV6_SADDR (TBA2)
- o option-length: 2 + length of cipv6-prefix-hint + length of cipv6 -bound-prefix, specified in bytes
- o cipv6-prefix-hint:
- o cipv6-hintlen: 8 bit field expressing the bit mask length of the IPv6 prefix specified in cipv6-prefix-hint
- o cipv6-bound-prefix: The IPv6 prefix that the client is using to bind the allocated DHCPv4 configuration to
- o cipv6-boundlen: 8 bit field expressing the bit mask length of the IPv6 prefix specified in cipv6-bound-prefix. Default: 128

9. Security Considerations

TBD

10. IANA Considerations

IANA is kindly requested to allocate the following DHCPv4 option code: TBD for OPTION_PORTPARAMSV4 and the DHCPv6 option code: OPTION_DHCPV4_O_DHCPV6_SADDR.

11. Acknowledgements

Thanks to Qi Sun and Olaf Bonness for thier reviews.

12. References

12.1. Normative References

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

12.2. Informative References

[I-D.ietf-dhc-dhcpv4-over-dhcpv6]
Sun, Q., Cui, Y., Siodelski, M., Krishnan, S., and I. Farrer, "DHCPv4 over DHCPv6 Transport", draft-ietf-dhc-dhcpv4-over-dhcpv6-00 (work in progress), April 2013.

[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", draft-ietf-softwire-lw4over6-00 (work in progress), April 2013.

[I-D.ietf-softwire-map-dhcp]
Mrugalski, T., Troan, O., Dec, W., Bao, C., leaf.yeh.sdo@gmail.com, l., and X. Deng, "DHCPv6 Options for Mapping of Address and Port", draft-ietf-softwire-map-dhcp-03 (work in progress), February 2013.

[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)", draft-ietf-softwire-map-07 (work in progress), May 2013.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, 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.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.

[RFC6148] Kurapati, P., Desetti, R., and B. Joshi, "DHCPv4 Lease Query by Relay Agent Remote ID", RFC 6148, February 2011.

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

Author's Address

Ian Farrer
Deutsche Telekom AG
Bonn
Germany

Email: ian.farrer@telekom.de