

Internet Engineering Task Force (IETF)
Request for Comments: 8539
Updates: 7598
Category: Standards Track
ISSN: 2070-1721

I. Farrer
Deutsche Telekom AG
Q. Sun
Y. Cui
L. Sun
Tsinghua University
March 2019

Software Provisioning Using DHCPv4 over DHCPv6

Abstract

DHCPv4 over DHCPv6 (RFC 7341) is a mechanism for dynamically configuring IPv4 for use as an over-the-top service in an IPv6-only network. Softwires are an example of such a service. For DHCPv4 over DHCPv6 (DHCP 4o6) to function with some IPv4-over-IPv6 softwire mechanisms and deployment scenarios (e.g., RFC 7596 or RFC 7597), the operator needs to know the IPv6 address that the client will use as the source of an IPv4-in-IPv6 softwire tunnel. This address, in conjunction with the client's IPv4 address, and (in some deployments) the Port Set ID are used to create a binding table entry in the operator's softwire tunnel concentrator. This memo defines a DHCPv6 option to convey IPv6 parameters for establishing the softwire tunnel and a DHCPv4 option (to be used only with DHCP 4o6) to communicate the source tunnel IPv6 address between the DHCP 4o6 client and server. It is designed to work in conjunction with the IPv4 address allocation process.

"DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients" (RFC 7598) describes a deterministic DHCPv6-based mechanism for provisioning softwires. This document updates RFC 7598, allowing OPTION_S46_BR (90) to be enumerated in the DHCPv6 client's Option Request Option (ORO) request and to appear directly within subsequent messages sent by the DHCPv6 server.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8539>.

Copyright Notice

Copyright (c) 2019 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 (<https://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 3
- 2. Applicability 4
- 3. Requirements Language 4
- 4. Solution Overview 5
 - 4.1. Updating RFC 7598 to Permit the Reuse of
OPTION_S46_BR (90) 5
- 5. DHCP 4o6 IPv6/IPv4 Binding Message Flow 6
- 6. DHCP Options 7
 - 6.1. DHCPv6 Software Source Binding Prefix Hint Option 7
 - 6.2. DHCP 4o6 Software Source Address Option 8
- 7. Client Behavior 9
 - 7.1. Client Initialization 9
 - 7.2. Renewing or Rebinding the IPv4 Address Lease and
Software Source Address 10
 - 7.2.1. Changing the Bound IPv6 Software Source Address 10
 - 7.3. Releasing the IPv4 Address Lease and Software
Source Address 11
 - 7.4. OPTION_S46_BIND_IPV6_PREFIX Validation Behavior 11
 - 7.5. Client and Server Software Source Address Mismatch 11
 - 7.6. Use with Dynamic, Shared IPv4 Addresses 12
- 8. Server Behavior 12
 - 8.1. Changing the Bound IPv6 Source Address 12
 - 8.2. Handling Conflicts between Clients' Bound IPv6 Source
Addresses 12
- 9. Security Considerations 13
 - 9.1. Client Privacy Considerations 14
- 10. IANA Considerations 15
- 11. References 16
 - 11.1. Normative References 16
 - 11.2. Informative References 17
- Acknowledgements 17
- Authors' Addresses 18

1. Introduction

Deterministic IPv4-over-IPv6 transition technologies require that elements be preconfigured with binding rules for routing traffic to clients. This places a constraint on the choice of address used as the client's software source address: it must use a predetermined prefix, which is usually configured on the home gateway device. [RFC7598] describes a DHCPv6-based mechanism for provisioning such deterministic softwires.

A dynamic provisioning model, such as using DHCPv4 over DHCPv6 (DHCP 4o6) [RFC7341], allows much more flexibility in the location of the IPv4-over-IPv6 softwire source address. In this model, the IPv6 address is dynamically communicated back to the service provider, allowing the corresponding softwire configuration to be created in the border relay (BR).

The DHCP 4o6 client and softwire client could be run on end devices attached to a network segment using any routable IPv6 prefix allocated to an end user, located anywhere within an arbitrary home network topology. Dynamic allocation also helps to optimize IPv4 resource usage, because only clients that are actively renewing their IPv4 lease hold on to the address.

This document describes a mechanism for dynamically provisioning softwires created using DHCP 4o6, including provisioning the client with the address of the softwire BR and informing the service provider of a client's binding between the dynamically allocated IPv4 address and Port Set ID and the IPv6 address that the softwire initiator will use for accessing IPv4-over-IPv6 services.

The mechanism operates alongside the DHCP 4o6 message flows to communicate the binding information over the IPv6-only network. The DHCP 4o6 server provides a single point in the network that holds the current client binding information. The service provider can then use this binding information to provision other functional elements, such as the BR(s).

2. Applicability

The mechanism described in this document is only suitable for use for provisioning softwire clients via DHCP 4o6. The options described here are only applicable within the DHCP 4o6 message-exchange process. Current softwire technologies suitable for extending to incorporate DHCP 4o6 with dynamic IPv4 address leasing include [RFC7597] and [RFC7596].

3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Solution Overview

In order to provision a softwire, both IPv6 and IPv4 configurations need to be passed to the client. To map this to the DHCP 4o6 configuration process, the IPv6 configuration is carried in DHCPv6 options [RFC8415], carried inside the DHCPv6 message DHCPV4-RESPONSE (21) sent by the server. OPTION_S46_BR (90) is used to provision the remote IPv6 address for the softwire BR (see Section 4.1). OPTION_S46_BIND_IPV6_PREFIX (137) is optionally sent by the DHCP 4o6 server to indicate to the client a preferred IPv6 prefix for binding the received IPv4 configuration and sourcing tunnel traffic. This may be necessary if there are multiple IPv6 prefixes in use in the customer network (e.g., Unique Local Addresses (ULAs)) or if the specific IPv4-over-IPv6 transition mechanism requires the use of a particular prefix for any reason.

IPv4 configuration is carried in DHCPv4 messages [RFC2131] (inside the DHCP 4o6 option OPTION_DHCPV4_MSG (87)) using the mechanism described in [RFC7341].

In order for the client to communicate the softwire source address, a new DHCPv4 option OPTION_DHCP4O6_S46_SADDR (109) is defined in this document. This is included in DHCPREQUEST messages sent by the client and is stored by the server for the lifetime of the IPv4 address lease.

4.1. Updating RFC 7598 to Permit the Reuse of OPTION_S46_BR (90)

Section 4.2 of [RFC7598] defines option OPTION_S46_BR (90) for communicating remote softwire BR IPv6 address(es) to a client, but it mandates that the option can only be used when encapsulated within one of the softwire container options: OPTION_S46_CONT_MAPE (94) or OPTION_S46_CONT_LW (96). From Section 3 of [RFC7598]:

Softwire46 DHCPv6 clients that receive provisioning options that are not encapsulated in container options MUST silently ignore these options.

This document updates [RFC7598], removing this restriction for OPTION_S46_BR (90), allowing it to be enumerated in the client's ORO request and appear directly within subsequent messages sent by the DHCPv6 server.

5. DHCP 4o6 IPv6/IPv4 Binding Message Flow

Figure 1 shows the relevant extensions to the successful DHCP 4o6 IPv4 allocation client/server message flow for the software source address function. The full process, including error handling, is described in Section 7.

In each step, the DHCPv6 portion of the message and any relevant option is shown above the arrow. The DHCP 4o6 content of the message and its relevant options are below the arrow. All the DHCPv4 messages are encapsulated in DHCPV4-QUERY (20) or DHCPV4-RESPONSE (21) messages. Where relevant, the necessary options and their contents are shown.

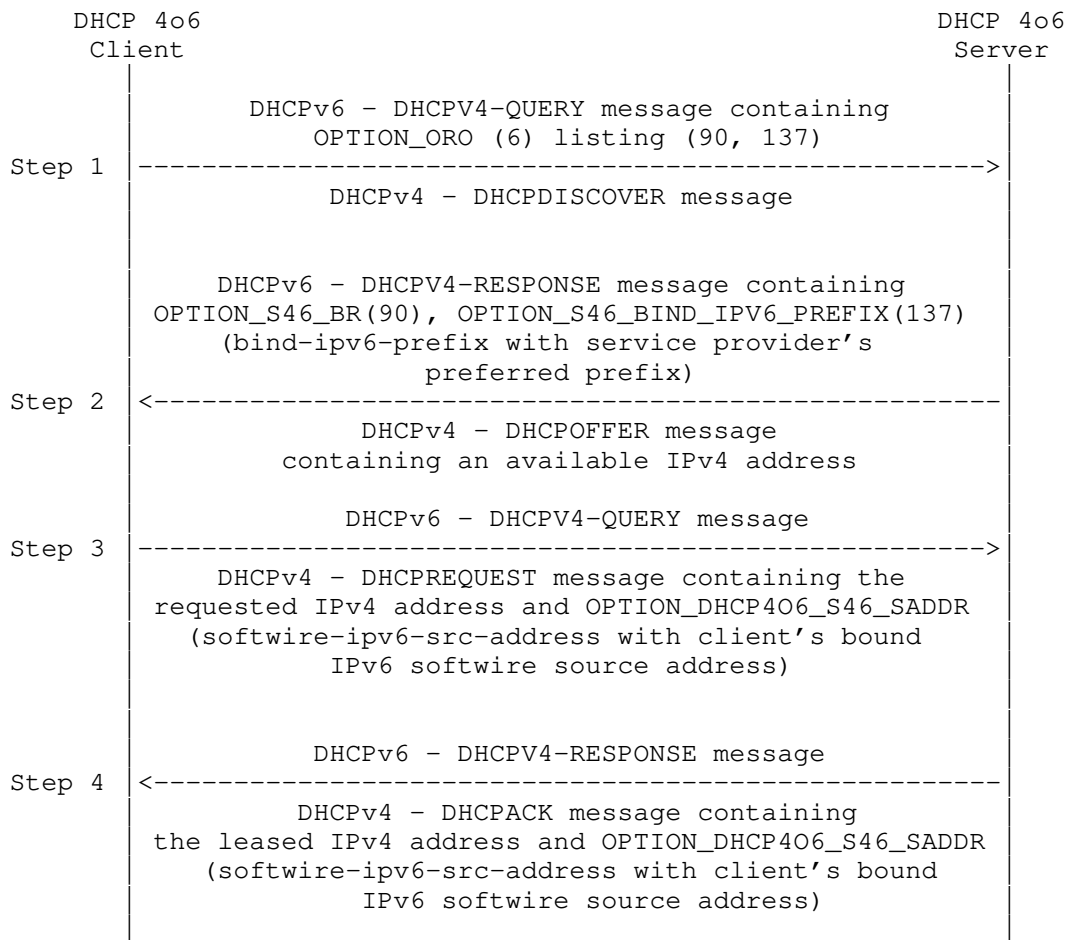


Figure 1: IPv6/IPv4 Binding Message Flow

- Step 1 The client constructs a DHCPv6 "DHCPV4-QUERY (20)" message. This message contains two options: DHCPv6 OPTION_ORO (6) and OPTION_DHCPV4_MSG (87). OPTION_ORO lists "90" (OPTION_S46_BR) and "137" (OPTION_S46_BIND_IPV6_PREFIX). OPTION_DHCPV4_MSG contains a DHCPv4 DHCPDISCOVER message.
- Step 2 The server responds with a DHCPv6 "DHCPV4-RESPONSE (21)" message. This message contains an OPTION_S46_BR (90) containing the IPv6 address of the BR for the client's softwire configuration. The message may also optionally contain OPTION_S46_BIND_IPV6_PREFIX (137). OPTION_DHCPV4_MSG contains a DHCPv4 DHCPOFFER message. The DHCPv4 message contains an available IPv4 address.
- Step 3 The client sends a DHCPv6 "DHCPV4-QUERY (20)" message containing a DHCPv4 DHCPREQUEST message with the requested IPv4 address and OPTION_DHCP4O6_S46_SADDR (109) with the IPv6 address that the client will use as its softwire source address.
- Step 4 The server sends a DHCPv6 "DHCPV4-RESPONSE (21)" message. OPTION_DHCPV4_MSG contains a DHCPv4 DHCPACK message with the allocated IPv4 address. OPTION_DHCP4O6_S46_SADDR with the client's bound softwire source address is included.

6. DHCP Options

6.1. DHCPv6 Softwire Source Binding Prefix Hint Option

The format of the DHCPv6 source binding prefix hint option is as follows:

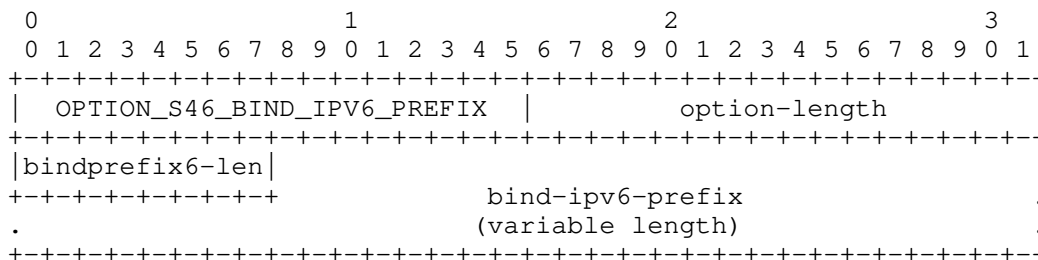


Figure 2: Format of OPTION_S46_BIND_IPV6_PREFIX

- o option-code: OPTION_S46_BIND_IPV6_PREFIX (137)
- o option-length: 1 + length of bind-ipv6-prefix, specified in bytes.

- o bindprefix6-len: 8-bit field expressing the bit mask length of the IPv6 prefix specified in bind-ipv6-prefix. Valid values are 0 to 128.
- o bind-ipv6-prefix: The IPv6 prefix indicating the preferred prefix for the client to bind the received IPv4 configuration to. The length is (bindprefix6-len + 7) / 8. The field is padded on the right with zero bits up to the next octet boundary when bind-ipv6-prefix is not evenly divisible by 8. These padding bits are ignored by the receiver (see Section 7.4).

OPTION_S46_BIND_IPV6_PREFIX is a singleton. Servers MUST NOT send more than one instance of the OPTION_S46_BIND_IPV6_PREFIX option.

6.2. DHCP 4o6 Software Source Address Option

The format of the DHCPv4 over DHCPv6 software source address option is as follows:

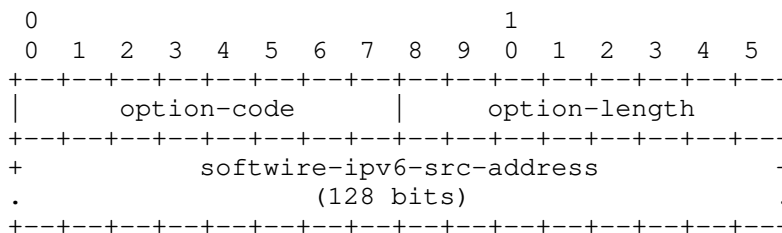


Figure 3: Format of OPTION_DHCP4O6_S46_SADDR

- o option-code: OPTION_DHCP4O6_S46_SADDR (109)
- o option-length: 16.
- o software-ipv6-src-address: 16 bytes long; the IPv6 address that is associated (either being requested for binding or currently bound) with the client's IPv4 configuration.

Note: The function of OPTION_DHCP4O6_S46_SADDR may seem similar to the DHCPv4 message's "chaddr" field or the Client Identifier (61) option in that it provides a unique lower-layer address that the server can use for identifying the client. However, as both of these are required to remain constant throughout the address lease lifetime, they cannot be used with the mechanism described in this document. This is because the client may only be able to construct the IPv6 address to use as the source address after it has received the first DHCPV4-RESPONSE message from the server containing OPTION_S46_BIND_IPV6_PREFIX.

7. Client Behavior

A client requiring dynamic softwire configuration first enables DHCP 4o6 configuration using the method described in Section 5 of [RFC7341]. If `OPTION_DHCP4_O_DHCP6_SERVER` is received in the corresponding `REPLY` message, the client `MAY` continue with the configuration process described below.

Before the dynamic softwire configuration process can commence, the client `MUST` be configured with a suitable IPv6 prefix to be used as the local softwire endpoint. This could be obtained using DHCPv6, Router Advertisement (RA) / Prefix Information Option (PIO), or another mechanism.

7.1. Client Initialization

When constructing the initial DHCP 4o6 `DHCPDISCOVER` message, the client includes a DHCPv6 `OPTION_ORO` (6) within the options field of the `DHCP-QUERY` message. `OPTION_ORO` contains the option codes for `OPTION_S46_BR` (90) and `OPTION_S46_BIND_IPV6_PREFIX` (137).

On receipt of the DHCP 4o6 server's reply (a `DHCPV4-RESPONSE` containing a `DHCPOFFER` message), the client checks the contents of the `DHCPV4-RESPONSE` for the presence of a valid `OPTION_S46_BR` option. If this option is not present, or does not contain at least one valid IPv6 address for a BR, then the client `MUST` discard the message, as without the address of the BR the client cannot configure the softwire and so has no interface to request IPv4 configuration for.

The `DHCPV4-RESPONSE` message may also include `OPTION_S46_BIND_IPV6_PREFIX`, which is used by the operator to indicate a preferred prefix that the client should bind IPv4 configuration to. If received, the client first checks the option according to Section 7.4. If valid, the client uses this prefix as the "IPv6 binding prefix" and follows to the process described in Section 5.1 of [RFC7596] in order to select an active IPv6 prefix to construct the softwire. If no match is found, or the client doesn't receive `OPTION_S46_BIND_IPV6_PREFIX`, the client `MAY` select any valid IPv6 prefix (of a suitable scope) to use as the tunnel source.

Once the client has selected a suitable prefix, it `MAY` either use an existing IPv6 address that is already configured on an interface or create a new address specifically for use as the softwire source address (e.g., using an Interface Identifier constructed as per Section 6 of [RFC7597]). If a new address is being created, the client `MUST` complete configuration of the new address, performing duplicate address detection (if required) before proceeding.

The client then constructs a DHCPV4-QUERY message containing a DHCPv4 DHCPREQUEST message. OPTION_DHCP4O6_S46_SADDR is included in the options field of the DHCPREQUEST message with the IPv6 address of its softwire source address in the softwire-ipv6-src-address field.

When the client receives a DHCPv4 DHCPACK message from the server, it checks the IPv6 address in OPTION_DHCP4O6_S46_SADDR against its active softwire source address. If they match, the allocation process has concluded. If there is a discrepancy, then the process described in Section 7.5 is followed.

If the client receives a DHCPv4 DHCPNAK message from the server, then the configuration process has been unsuccessful. The client then restarts the process from Step 1 of Figure 1.

7.2. Renewing or Rebinding the IPv4 Address Lease and Softwire Source Address

Whenever the client attempts to extend the lease time of the IPv4 address, OPTION_DHCP4O6_S46_SADDR with the IPv6 address of its softwire source address in the softwire-ipv6-src-address field MUST be included in the DHCPREQUEST message.

7.2.1. Changing the Bound IPv6 Softwire Source Address

Across the lifetime of the leased IPv4 address, it is possible that the client's IPv6 address will change, e.g., if there is an IPv6 renumbering event.

In this situation, the client MUST inform the server of the new address. This is done by sending a DHCPREQUEST message containing OPTION_DHCP4O6_S46_SADDR with the new IPv6 source address.

When the client receives a DHCPv4 DHCPACK message from the server, it checks the IPv6 address in OPTION_DHCP4O6_S46_SADDR against its active softwire source address. If they match, the allocation process has concluded. If there is a discrepancy, then the process described in Section 7.5 is followed.

If the client receives a DHCPv4 DHCPNAK message in response from the server, then the change of the bound IPv6 softwire source address has been unsuccessful. In this case, the client MUST stop using the new IPv6 source address. The client then restarts the process from Step 1 of Figure 1.

7.3. Releasing the IPv4 Address Lease and Softwire Source Address

When the client no longer requires the IPv4 resource, it sends a DHCPv4 DHCPRELEASE message to the server. As the options field is unused in this message type, OPTION_DHCP4O6_S46_SADDR is not included.

7.4. OPTION_S46_BIND_IPV6_PREFIX Validation Behavior

On receipt of the OPTION_S46_BIND_IPV6_PREFIX option, the client makes the following validation checks:

- o The received bindprefix6-len value is not larger than 128.
- o The number of bytes received in the bind-ipv6-prefix field is consistent with the received bindprefix6-len value (calculated as described in Section 6.1).

If either check fails, the receiver discards the invalid option and proceeds to attempt configuration as if the option had not been received.

The receiver MUST only use bits from the bind-ipv6-prefix field up to the value specified in the bindprefix6-len when performing the longest prefix match. bind-ipv6-prefix bits beyond this value MUST be ignored.

7.5. Client and Server Softwire Source Address Mismatch

If the client receives a DHCPACK message with an OPTION_DHCP4O6_S46_SADDR containing an IPv6 address that differs from its active softwire source address, the client SHOULD wait for a randomized time interval and then resend the DHCPREQUEST message with the correct softwire source address. Section 4.1 of [RFC2131] describes the retransmission backoff interval process.

The default minimum time for the client to attempt retransmission is 60 seconds. If, after this time has expired, the client has not received a DHCPACK message with the correct bound IPv6 address, client MAY send a DHCPRELEASE message and restart the process described in Section 7. The retry interval should be configurable and aligned with any server policy defining the minimum time interval for client address updates as described in Section 8.1.

7.6. Use with Dynamic, Shared IPv4 Addresses

[RFC7618] describes a mechanism for using DHCPv4 to distribute dynamic, shared IPv4 addresses to clients. The mechanism described in this document is compatible with IPv4 address sharing and can be enabled by following the process described in Section 6 of [RFC7618].

8. Server Behavior

Beyond the normal DHCP 4o6 functionality defined in [RFC7341], the server **MUST** also store the IPv6 softwire source address of the client in the leasing address database, alongside the IPv4 address and client identifier.

An `OPTION_DHCP4O6_S46_SADDR` containing the bound softwire source address **MUST** be sent in every DHCPACK message sent by the server.

The binding entry between the client's IPv6 softwire source address and the leased IPv4 address is valid as long as the IPv4 lease remains valid.

8.1. Changing the Bound IPv6 Source Address

In the event that the server receives a DHCPREQUEST message for an active IPv4 lease containing an `OPTION_DHCP4O6_S46_SADDR` with an IPv6 address that differs from the address that is currently stored, the server updates the stored softwire source address with the new address supplied by the client and sends a DHCPACK message containing the updated softwire source address in `OPTION_DHCP4O6_S46_SADDR`.

The server **MAY** implement a policy enforcing a minimum time interval between a client updating its softwire source IPv6 address. If a client attempts to update the softwire source IPv6 address before the minimum time has expired, the server can either silently drop the client's message or send back a DHCPACK message containing the existing IPv6 address binding in `OPTION_DHCP4O6_S46_SADDR`. If implemented, the default minimum client source address update interval is 60 seconds.

8.2. Handling Conflicts between Clients' Bound IPv6 Source Addresses

In order for traffic to be forwarded correctly, each customer edge's (CE's) softwire IPv6 source address must be unique. To ensure this, on receipt of every client DHCPREQUEST message containing `OPTION_DHCP4O6_S46_SADDR`, the DHCP 4o6 server **MUST** check the received IPv6 address against all existing CE source addresses stored for

active client IPv4 leases. If there is a match for any active lease other than the lease belonging to the client sending the DHCPREQUEST, then the client's IPv6 source address MUST NOT be stored or updated.

Depending on where the client and server are in the address leasing lifecycle, the DHCP 4o6 server then takes the following action:

- o If the DHCP 4o6 does not have a current, active IPv4 address lease for the client, then the DHCP address allocation process has not been successful. The server returns a DHCPNAK message to the client.
- o If the DHCP 4o6 does have a current, active IPv4 address lease, then the source address update process (see Section 8.1) has not been successful. The DHCP 4o6 server can either silently drop the client's message or return a DHCPACK message containing the existing IPv6 address binding in OPTION_DHCP4O6_S46_SADDR.

9. Security Considerations

Security considerations that are applicable to [RFC7341] are also applicable here.

A rogue client could attempt to use the mechanism described in Section 7.2.1 to redirect IPv4 traffic intended for another client to itself. This would be performed by sending a DHCPREQUEST message for another client's active IPv4 lease containing the attacker's softwire IPv6 address in OPTION_DHCP4O6_S46_SADDR.

For such an attack to be effective, the attacker would need to know both the client identifier and the active IPv4 address lease currently in use by another client. This could be attempted in three ways:

1. One customer learning the active IPv4 address lease and client identifier of another customer via snooping the DHCP4o6 message flow between the client and server. The mechanism described in this document is intended for use in a typical ISP network topology with a dedicated Layer 2 access network per client, meaning that snooping of another client's traffic is not possible. If the access network is a shared medium, then provisioning softwire clients using dynamic DHCP4o6 as described here is NOT RECOMMENDED.

2. Learning the active IPv4 address lease and client identifier via snooping the DHCP4o6 message flow between the client and server in the aggregation or core ISP network. In this case, the attacker requires a level of access to the ISP's infrastructure that means they can already intercept or interfere with traffic flows to the client.
3. An attacker attempting to brute-force guess the IPv4 lease address and client identifier tuple. The risk of this can be reduced by using a client identifier format that is not easily guessable, e.g., by using a random-based client identifier (see Section 3.5 of [RFC7844]).

An attacker could attempt to redirect existing flows to a client unable to process the traffic. This type of attack can be prevented by implementing network ingress filtering [BCP38] in conjunction with the BR source address validation processes described in [RFC7596] Section 5.2 and [RFC7597] Section 8.1.

A client may attempt to overload the server by sending multiple source address update messages (see Section 7.2.1) in a short time frame. This risk can be reduced by implementing a server policy enforcing a minimum time interval between client address changes, as described in Section 8.1.

9.1. Client Privacy Considerations

[RFC7844] describes anonymity profiles for DHCP clients. These considerations and recommendations are also applicable to clients implementing the mechanism described in this document. As DHCP 4o6 only uses DHCPv6 as a stateless transport for DHCPv4 messages, the "Anonymity Profile for DHCPv4" described in Section 3 is most relevant here.

In addition to the considerations given in [RFC7844], the mechanism that the client uses for constructing the interface identifier for its IPv6 software source address (see Section 7.1) could result in the device being trackable across different networks and sessions, e.g., if the client's software Interface Identifier (IID) is immutable.

This can be mitigated by constructing the software source IPv6 address as per Section 6 of [RFC7597]. Here, the address's IID contains only the allocated IPv4 address (and port set identifier if [RFC7618] is being used). This means no additional client information is exposed to the DHCP 4o6 server; it also means that the IID will change as the leased IPv4 address changes (e.g., between sessions when Section 3.5 of [RFC7844] is implemented).

10. IANA Considerations

IANA has assigned the OPTION_S46_BIND_IPV6_PREFIX (137) option code from the DHCPv6 "Option Codes" registry maintained at <<http://www.iana.org/assignments/dhcpv6-parameters>> as follows:

Value: 137
Description: OPTION_S46_BIND_IPV6_PREFIX
Client ORO: Yes
Singleton Option: Yes
Reference: RFC 8539

IANA has assigned the OPTION_DHCP4O6_S46_SADDR (109) option code from the "BOOTP Vendor Extensions and DHCP Options" registry maintained at <<http://www.iana.org/assignments/bootp-dhcp-parameters>> as follows:

Tag: 109
Name: OPTION_DHCP4O6_S46_SADDR
Data Length: 16
Meaning: DHCPv4 over DHCPv6 Software Source Address Option
Reference: RFC 8539

IANA has updated the entry for DHCPv6 OPTION_S46_BR (90) in the "Option Codes" registry maintained at <<https://www.iana.org/assignments/dhcpv6-parameters>> as follows:

Old Entry:

Value: 90
Description: OPTION_S46_BR
Client ORO: No
Singleton Option: No
Reference: [RFC7598]

New Entry:

Value: 90
Description: OPTION_S46_BR
Client ORO: Yes
Singleton Option: No
Reference: [RFC7598], [RFC8539]

11. References

11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <<https://www.rfc-editor.org/info/rfc2131>>.
- [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, <<https://www.rfc-editor.org/info/rfc7341>>.
- [RFC7598] Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for Configuration of Software Address and Port-Mapped Clients", RFC 7598, DOI 10.17487/RFC7598, July 2015, <<https://www.rfc-editor.org/info/rfc7598>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <<https://www.rfc-editor.org/info/rfc8415>>.

11.2. Informative References

- [BCP38] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000, <<https://www.rfc-editor.org/info/bcp38>>.
- [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, <<https://www.rfc-editor.org/info/rfc7596>>.
- [RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <<https://www.rfc-editor.org/info/rfc7597>>.
- [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, <<https://www.rfc-editor.org/info/rfc7618>>.
- [RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <<https://www.rfc-editor.org/info/rfc7844>>.

Acknowledgements

The authors would like to thank Ted Lemon, Lishan Li, Tatuya Jinmei, Jonas Gorski, and Razvan Becheriu for their contributions and comments.

Authors' Addresses

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

Email: ian.farrer@telekom.de

Qi Sun
Tsinghua University
Beijing 100084
China

Phone: +86-10-6278-5822
Email: sunqi.ietf@gmail.com

Yong Cui
Tsinghua University
Beijing 100084
China

Phone: +86-10-6260-3059
Email: yong@csnet1.cs.tsinghua.edu.cn

Linhui Sun
Tsinghua University
Beijing 100084
China

Phone: +86-10-6278-5822
Email: lh.sunlinh@gmail.com