Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

G. Ren
L. He
Y. Liu
Tsinghua University

March 13, 2017

Multi-requirement Extensions for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
draft-ren-dhc-mredhcpv6-00

Abstract

This memo provides multi-requirement extensions for DHCPv6, which allow hosts to generate or fetch addresses according to the user or network requirements, and DHCP servers to centrally manage all types of addresses including SLAAC-configured addresses, DHCPv6-configured addresses, and manual-configured addresses. Moreover, a general extension for address generation is designed to allow multiple types of requirements to be introduced into the DHCPv6 exchanges.

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 September 14, 2017.

Copyright Notice

Table of Contents

1. Introduction

There are two address auto-configuration methods in IPv6: Stateless Address Autoconfiguration (SLAAC) [RFC4862], and the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315]. Several address generation mechanisms have been proposed, including IEEE EUI-64 [RFC2464], CGAs [RFC3972], Temporary [RFC4941], and Stable, privacy [RFC7217]. The many types of IPv6 address generation and configuration methods available have brought about flexibility and diversity.

However, the current IPv6 address assignment and management are still confronted with certain problems, including a mixed operation problem of multiple IPv6 address generation mechanisms, a synchronization problem with a change in IPv6 addresses, an efficiency problem of processing large-scale concurrent IPv6 address requests, and a general model problem in introducing external services into the address assignment process.

Faced with various network requirements, various entities that prefer to remain up to date on all types of addresses, and various extensions for external services, it is important to balance the flexibility of address generation and configuration, user privacy, and network manageability. To solve the four problems above, the multi-requirement extensions for DHCPv6 are proposed, which can be achieved by extending DHCPv6 under the premise of changing the current protocols as little as possible.

This memo provides multi-requirement extensions for DHCPv6, which allow hosts to generate addresses through SLAAC or fetch addresses assigned from DHCPv6 servers according to the user or network requirements. At the same time, the extensions allow DHCP servers to centrally manage all kinds of addresses including SLAAC-configured addresses, DHCPv6-configured addresses, and manual-configured addresses. Moreover, a general extension for address generation is designed to allow multiple types of requirements to be introduced into the DHCPv6 exchanges.

2. Terminology

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

Familiarity with DHCPv6 and its terminology, as defined in [RFC3315], is assumed.

Other terminology:

Requirements	A functional need that a particular design or process of the address generation and assignment must be able to perform.
External Services	Services that are introduced into the DHCP exchanges according to specific requirements, such as traceback, transition, and mobility.
External Service Client	An entity requesting a specific external service.
External service Server	An entity providing a specific external service to external service clients.

3. Problem Statement

3.1. Address Configuration Methods

SLAAC and DHCPv6 are two auto-configuration mechanisms in IPv6 [RFC2460]. SLAAC can configure hosts with one or more addresses composed of a network prefix advertised by a local router, and an Interface Identifier (IID) that typically embeds a hardware address (e.g., an IEEE LAN MAC address) [RFC4291]. DHCPv6 can provide a device with addresses assigned by a DHCPv6 server and other configuration information carried in the options.

3.2. Address Generation Mechanisms

Several IID generation mechanisms have been proposed for standardization, all of which have their own specific requirements. IEEE 64-bit Extended EUI-64 [RFC2464] generates IIDs based on IEEE 802 48-bit Media Access Control (MAC) addresses quickly and economically. Cryptographically Generated Addresses (CGAs) [RFC3972] are another method for generating an IID, which binds a hash of the host’s public key to an IPv6 address in the SEcure Neighbor Discovery (SEND) protocol [RFC3971]. The owners of CGAs can sign messages using the corresponding private keys to protect their messages. Temporary addresses defined in [RFC3041] (later made obsolete by [RFC4941]) are randomly generated for outgoing connections to protect the host’s privacy, and are changed daily. However, temporary addresses make it difficult to conduct network management (e.g.,

increase the complexity of event logging and access controls). Therefore, [RFC7217] specifies an algorithm that generates a unique random stable, semantically opaque IID per IPv6 link for each network without sacrificing the security and privacy of users. The DHCPv6 variant of this method is specified in [RFC7943].

3.3. Determinants of IPv6 Address Allocations

3.3.1. Routers

The ICMPv6-based [RFC4443] Router Advertisement (RA) message specified in Neighbor Discovery (ND) [RFC4861] contains M and A flags that allow a host to generate or fetch different types of addresses (SLAAC addresses and DHCPv6 addresses) when they are set. At the same time, several routers may exist in the same network, all with different flags and prefix settings.

3.3.2. DHCPv6 Servers

When the M flag is set, it indicates that addresses are available through DHCPv6 service. In fact, there may be several DHCPv6 servers in a network that can assign addresses to DHCPv6 clients. Each DHCPv6 server can assign addresses of different types, non-temporary and temporary, and different policies, including iterative, identifier-based, hash, and random [RFC7824].

3.3.3. Hosts

A host can configure its addresses in the following ways:

Manual Administrators can configure static addresses for the host.

SLAAC When A flags in the prefix information options (PIOs) of an RA message are set, a host can utilize the prefixes in the PIOs of RA messages to generate addresses automatically. Many different address generation mechanisms can be utilized, including IEEE EUI-64 [RFC2464], CGA[RFC3972], Temporary [RFC4941], and Stable, privacy[RFC7217].

3.4. Address-Related Network Entities

After address assignments, many other network service entities record and maintain data entries related to the addresses.

Switches Switches will create entries for the addresses in the forwarding table.

DHCPv6 servers	DHCPv6 servers will record and maintain the address leases for the clients.
Auditing server	An auditing server will record the detailed traffic usage of the addresses.
Gateway	A gateway will use the authenticated address list to control the host’s access to the Internet.
Other External servers	Other external service servers may need to maintain the address-related information.

3.5. Current Problems

The current IPv6 address assignment and management are still confronted with certain problems, including mixed operation problem, synchronization problem, efficiency problem, and general model problem.

3.5.1. Mixed Operation Problem

The first problem is a mixed operation problem of multiple IPv6 address generation mechanisms. Currently, even one host interface can have several addresses generated from different address generation mechanisms. Moreover, hosts in the same network can use different address generation mechanisms for SLAAC to obtain addresses and/or fetch addresses assigned from DHCPv6 servers. Requirements exist for networks to uniformly configure their address generation mechanism. For SLAAC addresses, difficulties arise when conducting address management and some other network services (e.g., authentication), because most operating systems leverage temporary addresses, which vary over time (e.g., after one day). At the same time, persistent connections will be cut off when the addresses vary. To summarize, the addresses of the hosts can be generated according to not only the user requirements but also to the network requirements.

3.5.2. Synchronization Problem

The second problem is a synchronization problem with a change in IPv6 addresses. Many types of network function entities related to addresses exist, as mentioned in Section 3.4. Once a host updates its addresses, or if the address that the host is currently using is re-assigned to another user for a particular reason (e.g., without renewing the lease), the corresponding function entities should also update their corresponding stored entries. [RFC7653] solves a part of this problem by allowing other network entities to keep up with

the DHCPv6 leases. However, the part of the problem caused by SLAAC and manual configurations remains unresolved.

3.5.3. Efficiency Problem

The third problem is an efficiency problem when processing large-scale concurrent IPv6 address requests. When large-scale concurrent IPv6 address requests exist, the routers will use more resources to forward the multicast messages when the hosts conduct duplicate address detection (DAD) [RFC4862]. However, when central management is used for all types of addresses, this address management entity can detect duplicate addresses for the hosts. It is simple to choose between the concurrent processing mechanism of server clustering techniques and the current DAD processing mode, which puts significant pressure on the routers when large-scale concurrent address requests exist.

3.5.4. General Model Problem

The fourth problem is a general model problem in introducing external services into the address assignment process. On the one hand, IP addresses are not only locators they are also identifiers. As identifiers, IP addresses can be mapped to other requirement spaces to support multiple functions, such as traceback, transition, and mobility. On the other hand, some interoperations between DHCP entities with external service entities are designed to provide precise and fine-grained services. For example, IETF defines the interoperations between DHCPv6 relays and radius servers [RFC7037] to provide authorization and identification information between the DHCPv6 relay agent and DHCPv6 server. In short, there are no general uniform protocol extensions or models for introducing external services into the address assignment process.

4. Design Goals

To solve the above problems, the solution should achieve the following goals:

Goal 1 Addresses in a network should be generated according to the user or network requirements. In fact, DHCPv6 servers already assign addresses according to these requirements. DHCPv6 servers can assign temporary or non-temporary addresses to DHCPv6 clients. DHCPv6 also provides several address allocation policies according to the administrative requirements and settings, including iterative, identifier-based, hash and random [RFC7824].

Goal 2 All types of addresses in a network should be within the central management, including SLAAC-configured addresses, DHCPv6-configured addresses, and manual-configured addresses. Because a DHCPv6 server manages a pool of IPv6 addresses and information regarding client configuration parameters, it will be a good option for the DHCPv6 server to manage other types of addresses when necessary.

Goal 3 General uniform protocol extensions and models for introducing external services into the process of address assignment should be built.

5. General Structures

5.1. General Address Generation Type

According to Section 3.2, the general address generation types are summarized below.

Type	Method	Related RFC
1	IEEE EUI-64	RFC 2464
2	CGAs	RFC3972
3	Temporary	RFC4941
4	Stable, privacy	RFC7217/RFC7943

Table 1: General address generation types

5.2. Uniform Address Storage Structure

Because DHCPv6 servers will store all kinds of address assignments, it is necessary to design a uniform address assignment storage structure. Several key elements have been selected to construct the core of the address assignment storage structure.

address IPv6 address.

duid DHCP unique identifier, see Section 9 of [RFC3315].

iaid Identity association, see Section 10 of [RFC3315].

valid_lifetime	Length of the lease.
expire	Expiration time of the lease.
pref_lifetime	Preferred lifetime.
hwaddr	Hardware/MAC address.

address	duid	iaid	valid_lifetime	expire	pref_lifetime	hwaddr

For SLAAC address assignments and manual address configurations, some information may be absent, including duid and iaid. Other information can also be included in the uniform address storage structure, such as the subnet identification, hostname, and lease type.

6. Solutions

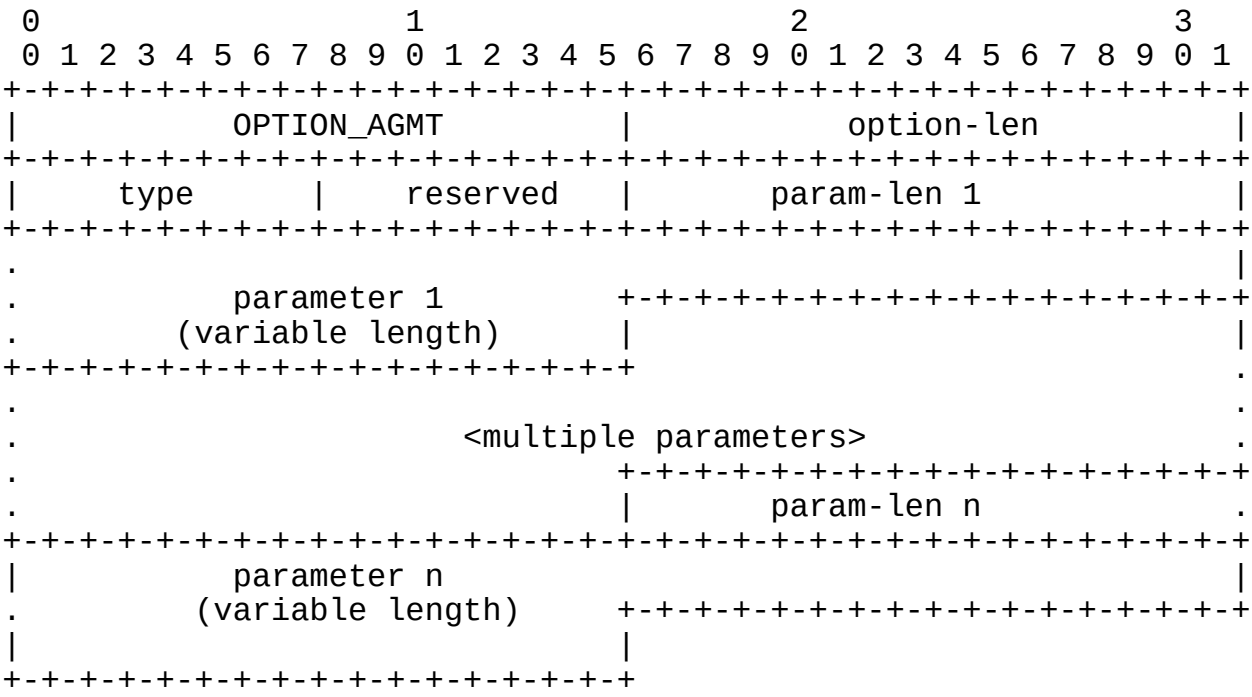
For Goal 1, mechanisms that allow SLAAC-configured addresses and manual-configured addresses to be sent to the DHCPv6 server can be provided. For Goal 2, extensions for both SLAAC and DHCPv6 should be provided. More specifically, extensions of PIO are provided for SLAAC, and new options have been designed for DHCPv6. For Goal 3, a general address generation extension for DHCPv6 is presented herein.

6.1. Sub-solution for DHCPv6

6.1.1. Extension of DHCPv6 Options

6.1.1.1. Address Generation Mechanism Type Option

A server sends this option to inform the client of the address generation mechanism used in the administrative domain. The format of the Address Generation Mechanism Type (AGMT) option is as follows:



Format description:

option-code OPTION_AGMT(TBA1).

option-len 2 + Length of following multiple parameters in octets.

type IID generation mechanism type that the server selects. A value of zero is assigned as the default value.

0 Any IID generation mechanism type.

1 IEEE EUI-64.

2 CGAs.

3 Temporary addresses.

4 Stable, semantically opaque IIDs.

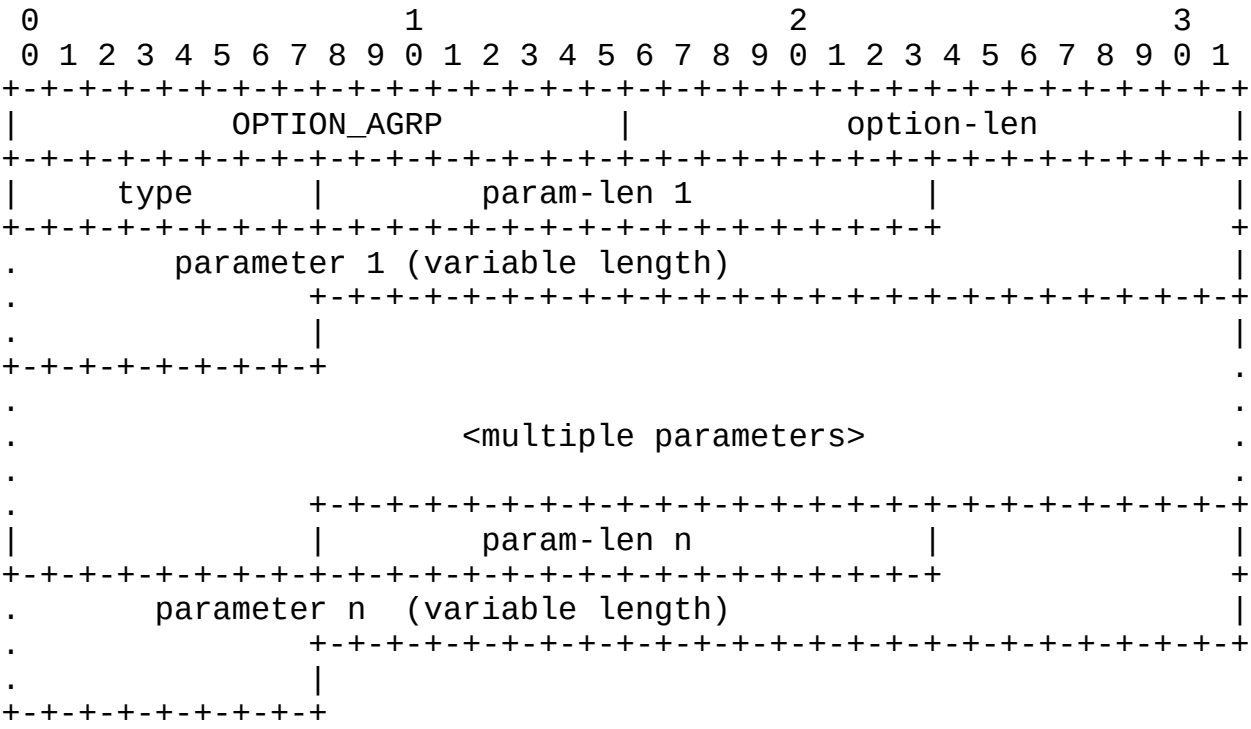
reserved Reserved field for future extensions. The server MUST set this value to zero, and the client MUST ignore its content.

param-len 1...n This is a 16-bit integer that specifies the length of the following parameters in octets (not including the parameter-length field).

parameter 1...n These UTF-8 strings are parameters needed for servers to inform the clients according to the selected address generation mechanisms. The strings are not NUL-terminated.

6.1.1.2. Address Generation Requiring Parameters Option

The client sends this option to inform the server of the parameters of the corresponding address generation mechanism. The format of the Address Generation Requiring Parameters (AGRP) option is as follows:



Format description:

option-code OPTION_AGRP(TBA2).

option-len 1 + Length of following multiple parameters in octets.

type IID generation mechanism type selected by the server.

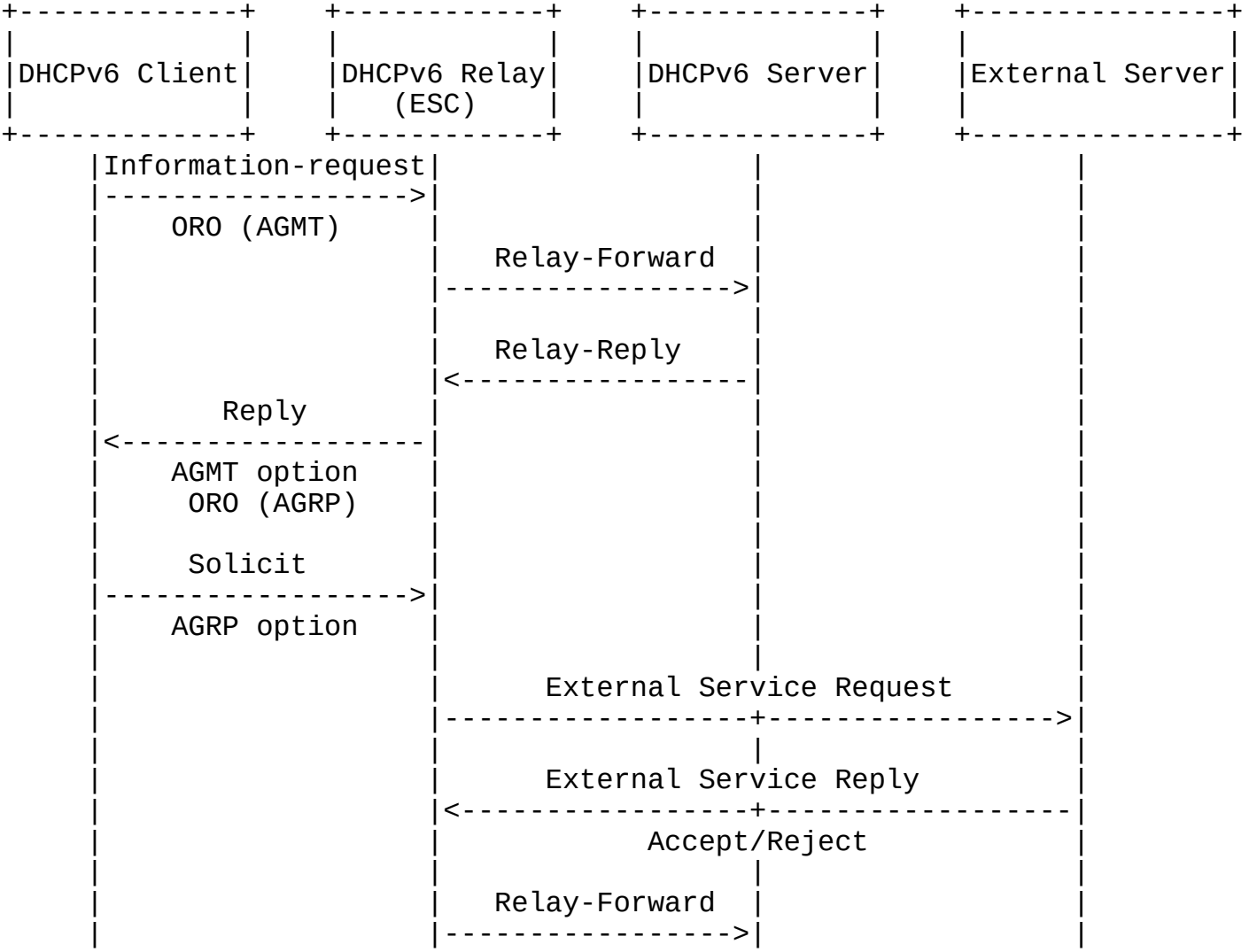
param-len 1...n This is a 16-bit integer that specifies the length of the following parameter in octets (not including the parameter-length field).

parameter 1...n These UTF-8 strings are parameters needed for the clients to inform the servers of according to the selected address generation mechanism. The strings are not NUL-terminated.

6.1.2. Extension of DHCPv6 Exchange Process

6.1.2.1. Overview

The part of the intent of this memo is to dynamically configure the address generation mechanism. The following figure illustrates the new DHCPv6 exchange process. Briefly, a client requests the address generation mechanism from servers. The servers tell the client which type of address generation mechanism to use. Some parameters can also be sent to the servers to generate new addresses when the clients start to request addresses.



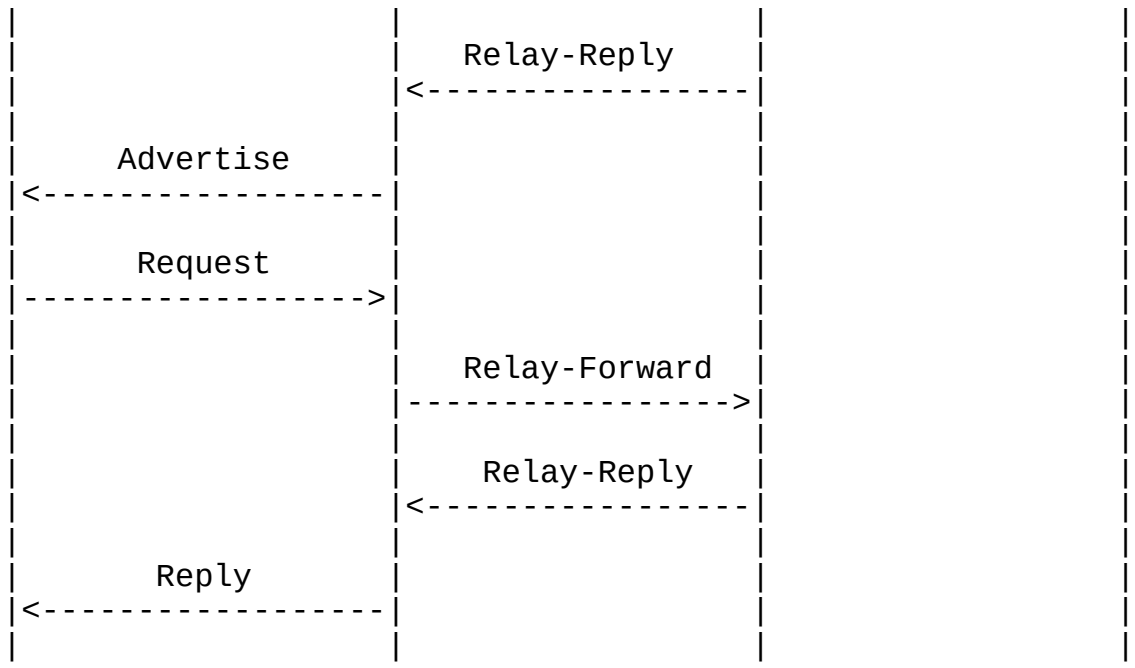


Figure 1: Extension of DHCPv6 Exchange Process

6.1.2.2. Detailed Exchanges

The detailed exchanges of the extensions specified in this memo are as follows:

1 A client requests the AGMT option in the Option Request Option (ORO), which is carried in an Information-request message.

2 The relay agent forwards the Information-request message to the servers.

3 The servers tell the client which type of address generation mechanism to use through the AGMT option within the Reply message. If a server requires the client to provide parameters to generate the addresses, it requests the AGRP option in the ORO.

4 The relay agent forwards the Reply message to the client.

5 If the address generation mechanism selected by the server does not require the client to send other parameters, the client sends a normal Solicit message. Otherwise, the client sends a Solicit message with an AGRP option.

6 When the relay agent receives a Solicit message, it checks whether the selected method requires communication with external servers. If not, it forwards the message to the server. Otherwise, it communicates with the external server to finish the related task (e.g., authentication or authority) as an external service client (ESC) (see Section 6.1.3). Next, it forwards the Solicit message to the server if the communication process succeeds. Otherwise, it drops the message.

7 If there is an AGRP option in the Solicit message, the server uses the parameters in the AGRP option to generate an address and sends an Advertise message with the address to the client. Otherwise, the server handles the message based on [RFC3315].

8 The remaining steps are the same as with the original DHCPv6 process.

6.1.3. Extension of External Service Result Fetching Process

The figure below shows the communication process between a DHCPv6 relay, or server, and an ESC, which only includes two messages: an External Service Request message and an External Service Reply message. Notice that the ESC can be located on the same device with the DHCPv6 relay agent or DHCPv6 server.

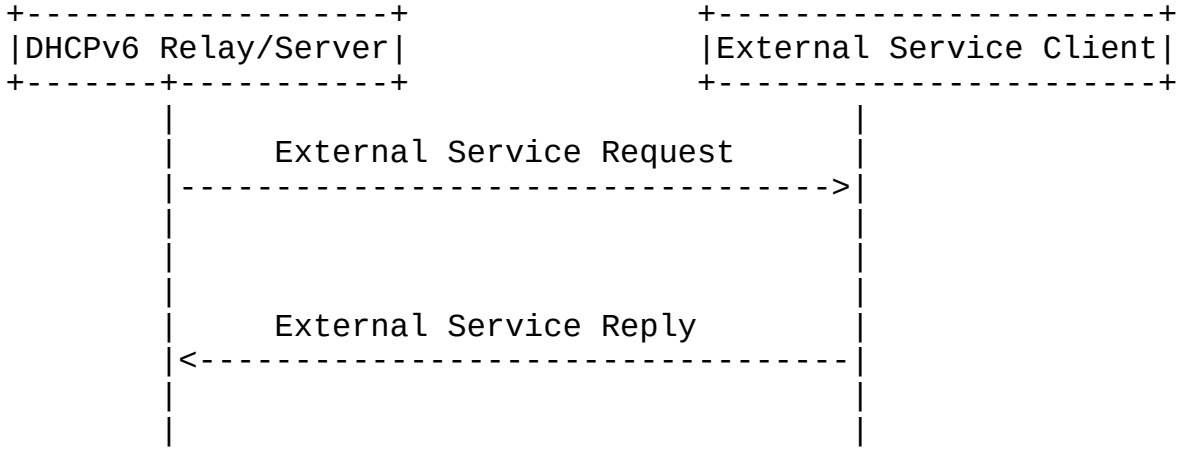


Figure 2: Extension of External Service Result Fetching Process

The format of the External Service Message is as follows:

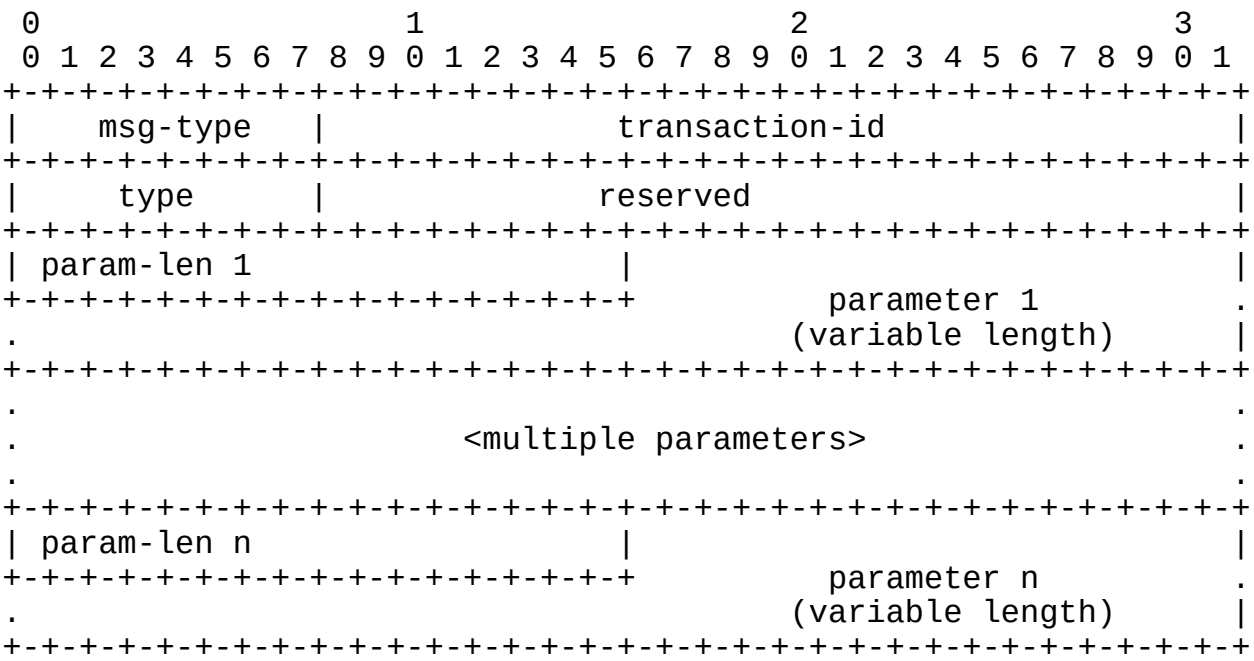


Figure 3: External Service Message Format

Format description:

msg-type The message type, including EXTERNAL_SERVICE_REQUEST(TBA3) and EXTERNAL_SERVICE_REPLY(TBA4).

transaction-id The transaction id copied from a Solicit message to identify this message exchange.

type External service type.

reserved Reserved field for future extensions. The server MUST set this value to zero, and the client/server MUST ignore its content.

param-len 1...n This is a 16-bit integer that specifies the length of the following parameter in octets (not including the parameter-length field).

parameter 1...n These UTF-8 strings are parameters required for external services. The strings are not NUL-terminated.

6.1.3.1. External Service Request Message

This message is used by the DHCPv6 relay or server to request an external service at the external server. The DHCPv6 relay or server sends this message to the ESC, which extracts the parameters in the message to start an external service communication process. For example, when the DHCPv6 process uses a radius server to authenticate or authorize a client [RFC7037], the message can be used to send the relevant parameters to the radius client.

When the DHCP relay or server creates such a message, it sets the msg-type to EXTERNAL_SERVICE_REQUEST and the type to a specific external service type, copies the transaction-id from the message triggering the external service, and provides the specific parameters required by the external service to the external service client.

6.1.3.2. External Service Reply Message

This message is used by the ESC to reply to the DHCPv6 relay or server with the acceptance or rejection result of the external service.

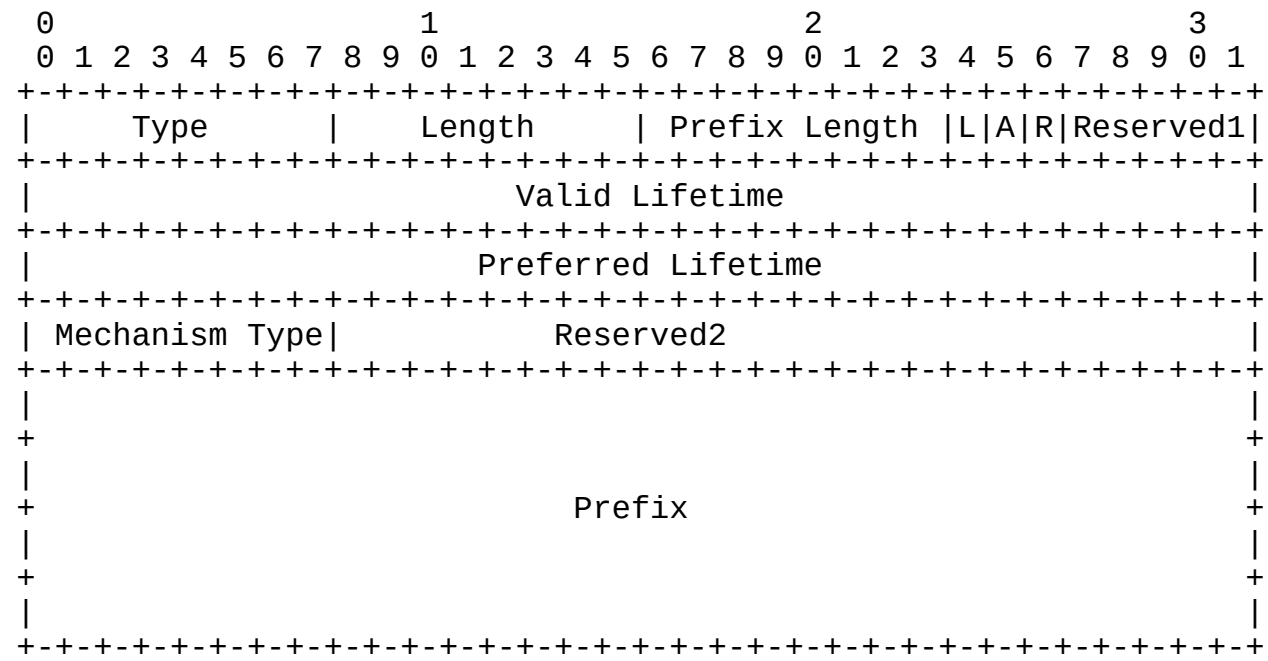
When the external service client creates the message, it sets the msg-type to EXTERNAL_SERVICE_REPLY, copies the transaction-id and type from the External Service Request message, and provides the specific result parameters to the DHCPv6 relay or server.

6.2. Sub-solution for SLAAC

6.2.1. Extension of RA Options

6.2.1.1. Modified Prefix Information Option Format

To support multiple requirements in the address generation for SLAAC, Neighbor Discovery [RFC4861] can be extended to allow a router to advertise the default address generation mechanism for each prefix through the addition of one octet in the format of a PIO for use in the Router Advertisement messages. The format of the PIO is as follows:



This format represents the following changes over that originally specified for Neighbor Discovery [RFC4861]:

Scheme Type 1-octet address generation mechanism type flag. When the A flag is set, it indicates that the PIO recommends the hosts to use the address generation mechanism specified in the Mechanism Type and the prefix specified in Prefix to generate the addresses.

0 Any IID generation mechanism type.

1 IEEE EUI-64.

2 CGAs.

3 Temporary.

4 Stable, privacy.

Reserved2 Reduced from a 4-octet field to a 3-octet field to account for the addition of the above octet.

6.2.2. Extension of Hosts

The hosts should implement the standardized address generation mechanisms mentioned in Section 5.1.

When a host receives RA messages containing a modified PIO, it handles the message based on [RFC4861]. It uses the recommended mechanism type in the PIO to generate the addresses. Note that multiple PIOs may recommend different address generation mechanisms.

6.2.3. Central Management of SLAAC-configured Address

After finishing the address generation, a host should inform the DHCPv6 server of its SLAAC-configured addresses or manual-configured addresses to help the DHCPv6 server manage all types of addresses in the network. There are several schemes to consider:

Scheme 1: Create two new messages similar to Request and Reply messages of DHCPv6 to inform the DHCPv6 server of the SLAAC-configured or manual-configured addresses.

Scheme 2: Use and modify a current mechanism to inform the DHCPv6 server of the addresses. For example, because every SLAAC-configured address performs a DAD, a Neighbor Solicit message can be modified to support this function.

7. Security Considerations

The known security vulnerabilities of the DHCPv6 protocol may apply to its options. Security issues related with DHCPv6 are described in Section 23 of [RFC3315].

Network administrators should be aware that certain external service messages are encrypted, and that DHCPv6 messages are always unencrypted. It is possible for some external service attributes to contain sensitive or confidential information. Network administrators are strongly advised to prevent such information from being included in DHCPv6 messages.

[secure_dhcpv6] provides a new method for protecting end-to-end communication using public key cryptography.

8. IANA Considerations

This memo defines two new DHCPv6 [RFC3315] messages types. The IANA is requested to assign values for the two messages types in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters: The two new messages type are:

The EXTERNAL_SERVICE_REQUEST(TBA3), described in Section Figure 3.

The EXTERNAL_SERVICE_REPLY(TBA4), described in Section Figure 3.

This memo defines two new DHCPv6 [RFC3315] options. The IANA is requested to assign values for the two options from the DHCPv6 Options Codes table of the DHCPv6 Parameters registry maintained in http://www.iana.org/assignments/dhcpv6-parameters. The two options are:

The Address Generation Mechanism Type option (TBA1), described in Section Section 6.1.1.1.

The Address Generation Requiring Parameters option(TBA2), described in Section Section 6.1.1.2.

IID generation mechanism for multi-requirement extension for DHCPv6. The values in this table are 8-bit unsigned integers. The following initial values are assigned for IID generation mechanism for multi-requirement extension for DHCPv6 in this memo:

Method	Value	RFCs
IEEE EUI-64	0x01	this memo
CGAs	0x02	this memo
Temporary	0x03	this memo
Stable, privacy	0x04	this memo

9. Acknowledgements

Valuable comments from Bernie Volz are appreciated.

10. References

10.1. Normative References

[dhcp_cga] Jiang, S., "Configuring Cryptographically Generated Addresses (CGA) using DHCPv6", 2009.

[dhcp_slaac_problem] Liu, B., "DHCPv6/SLAAC Interaction Problems on Address and DNS Configuration", 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <http://www.rfc-editor.org/info/rfc2464>.

[RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, DOI 10.17487/RFC3041, January 2001, <http://www.rfc-editor.org/info/rfc3041>.

[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>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <http://www.rfc-editor.org/info/rfc3972>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <http://www.rfc-editor.org/info/rfc4429>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, DOI 10.17487/RFC4443, March 2006, <http://www.rfc-editor.org/info/rfc4443>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <http://www.rfc-editor.org/info/rfc4941>.

[RFC6957] Costa, F., Combes, J-M., Ed., Pougnard, X., and H. Li, "Duplicate Address Detection Proxy", RFC 6957, DOI 10.17487/RFC6957, June 2013, <http://www.rfc-editor.org/info/rfc6957>.

[RFC7037] Yeh, L. and M. Boucadair, "RADIUS Option for the DHCPv6 Relay Agent", RFC 7037, DOI 10.17487/RFC7037, October 2013, <http://www.rfc-editor.org/info/rfc7037>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

[RFC7653] Raghuvanshi, D., Kinnear, K., and D. Kukrety, "DHCPv6 Active Leasequery", RFC 7653, DOI 10.17487/RFC7653, October 2015, <http://www.rfc-editor.org/info/rfc7653>.

[RFC7824] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy Considerations for DHCPv6", RFC 7824, DOI 10.17487/RFC7824, May 2016, <http://www.rfc-editor.org/info/rfc7824>.

[RFC7943] Gont, F. and W. Liu, "A Method for Generating Semantically Opaque Interface Identifiers (IIDs) with the Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 7943, DOI 10.17487/RFC7943, September 2016, <http://www.rfc-editor.org/info/rfc7943>.

[secure_dhcpv6] Jiang, S., "Secure DHCPv6", 2016.

10.2. Informative References

[DOMINATION] Mad Dominators, Inc., "Ultimate Plan for Taking Over the World", 1984, <http://www.example.com/dominator.html>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <http://www.rfc-editor.org/info/rfc3552>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC7749] Reschke, J., "The "xml2rfc" Version 2 Vocabulary", RFC 7749, DOI 10.17487/RFC7749, February 2016, <http://www.rfc-editor.org/info/rfc7749>.

Appendix A. Additional Stuff

This becomes an Appendix.

Authors' Addresses

Gang Ren
Tsinghua University
Beijing
CN

Phone: +86-010 6260 3227
Email: rengang@cernet.edu.cn

Lin He
Tsinghua University
Beijing
CN

Email: he-l14@mails.tsinghua.edu.cn

Ying Liu
Tsinghua University
Beijing
CN

Email: liuying@cernet.edu.cn