dhc
Internet-Draft
Intended status: Informational
Expires: August 19, 2016

S. Krishnan
Ericsson
T. Mrugalski
ISC
S. Jiang
Huawei Technologies Co., Ltd

February 16, 2016

Privacy considerations for DHCPv6 draft-ietf-dhc-dhcpv6-privacy-04

Abstract

DHCPv6 is a protocol that is used to provide addressing and configuration information to IPv6 hosts. This document describes the privacy issues associated with the use of DHCPv6 by the Internet users. It is intended to be an analysis of the present situation and does not propose any solutions.

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 August 19, 2016.

Table of Contents

1. Introduction

DHCPv6 [RFC3315] is a protocol that is used to provide addressing and configuration information to IPv6 hosts. DHCPv6 uses several identifiers that could become a source for gleaning information about the IPv6 host. This information may include device type, operating system information, location(s) that the device may have previously visited, etc. This document discusses the various identifiers used by DHCPv6 and the potential privacy issues [RFC6973]. In particular, it also takes into consideration the problem of pervasive monitoring [RFC7258].

Future works may propose protocol changes to fix the privacy issues that have been analyzed in this document. Protocol changes are out of scope for this document.

The primary focus of this document is around privacy considerations for clients to support client mobility and connection to random networks. The privacy of DHCPv6 servers and relay agents are considered less important as they are typically open for public services. And, it is generally assumed that relay agent to server communication is protected from casual snooping, as that communication occurs in the provider's backbone. Nevertheless, the topics involving relay agents and servers are explored to some degree. However, future work may want to further explore privacy of DHCPv6 servers and relay agents.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as [RFC2119] key words.

Naming convention from [RFC3315] and related is used throughout this document. In addition the following terminology is used:

Stable identifier - Any property disclosed by a DHCPv6 client that does not change over time or changes very infrequently and is unique for said client in a given context. Examples include MAC address, client-id, and a hostname. Some identifiers may be considered stable only under certain conditions, for example one client implementation may keep its client-id stored in stable storage while another may generate it on the fly and use a different one after each boot. Stable identifiers may or may not be globally unique.

3. Identifiers in DHCPv6 options and fields

In DHCPv6, there are many options that include identification information or that can be used to extract identification information about the client. This section enumerates various options or fields and the identifiers conveyed in them, which can be used to disclose client identification. The attacks that are enabled by such disclosures are detailed in Section 5.

3.1. Source IPv6 address

Although IPv6 link-local address is technically not a part of DHCPv6, it appears in the DHCPv6 transmissions, so it is mentioned here for completeness.

If the client does not use privacy extensions (see [RFC4941]) or similar solutions and its IPv6 link-local address is based on physical link-layer address, this information is disclosed to the DHCPv6 server and to anyone who manages to intercept this transmission.

There are multiple cases where IPv6 link-local addresses are used in DHCPv6. Initial client transmissions are always sent from the IPv6 link-local addresses even when the server unicast option (see Sections 22.12 and 18 of [RFC3315] for details) is enabled. If there are relay agents, they forward client's traffic wrapped in Relay-forward and store original source IPv6 address in peer-address field.

3.2. DUID

Each DHCPv6 client and server has a DHCPv6 Unique Identifier (DUID) [RFC3315]. The DUID is designed to be unique across all DHCPv6 clients and servers, and to remain stable after it has been initially generated. The DUID can be of different forms. Commonly used forms are based on the link-layer address of one of the device's network interfaces (with or without a timestamp), on the Universally Unique IDentifier (UUID) [RFC6355]. The default type, defined in Section 9.2 of [RFC3315] is DUID-LLT that is based on link-layer address. It is commonly implemented in most popular clients.

It is important to understand DUID lifecycle. Clients and servers are expected to generate their DUID once (during first operation) and store it in a non-volatile storage or use the same deterministic algorithm to generate the same DUID value again. This means that most implementations will use the available link-layer address during its first boot. Even if the administrator enables link-layer address randomization, it is likely that it was not yet enabled during the first device boot. Hence the original, unobfuscated link-layer

address will likely end up being announced as client DUID, even if the link-layer address has changed (or even if being changed on a periodic basis). The exposure of the original link-layer address in DUID will also undermine other privacy extensions such as [RFC4941].

3.3. Client Identifier Option

The Client Identifier Option (OPTION_CLIENTID) [RFC3315] is used to carry the DUID of a DHCPv6 client between a client and a server. There is an analogous Server Identifier Option but it is not as interesting in the privacy context (unless a host can be convinced to start acting as a server). See Section 3.2 for relevant discussion about DUIDs.

3.4. IA_NA, IA_TA, IA_PD, IA Address and IA Prefix Options

The Identity Association for Non-temporary Addresses (IA_NA) option [RFC3315] is used to carry the parameters and any non-temporary addresses associated with the given IA_NA. The Identity Association for Temporary Addresses (IA_TA) option [RFC3315] is analogous to the IA_NA option but for temporary addresses. The IA Address option [RFC3315] is used to specify IPv6 addresses associated with an IA_NA or an IA_TA and is encapsulated within the Options field of such an IA_NA or IA_TA option. The Identity Association for Prefix Delegation (IA_PD) [RFC3633] option is used to carry the prefixes that are assigned to the requesting router. IA Prefix option [RFC3633] is used to specify IPv6 prefixes associated with an IA_PD and is encapsulated within the Options field of such an IA_PD option.

To differentiate between instances of the same type of IA containers for a client, each IA_NA, IA_TA and IA_PD options have an IAID field with a unique value for a given IA type. It is up to the client to pick unique IAID values. At least one popular implementation uses last four octets of the link-layer address. In most cases, that means that merely two bytes are missing for a full link-layer address reconstruction. However, the first three octets in a typical link-layer address are vendor identifier. That can be determined with high level of certainty using other means, thus allowing full link-layer address discovery.

3.5. Client FQDN Option

The Client Fully Qualified Domain Name (FQDN) option [RFC4704] is used by DHCPv6 clients and servers to exchange information about the client's fully qualified domain name and about who has the responsibility for updating the DNS with the associated AAAA and PTR RRs.

A client can use this option to convey all or part of its domain name to a DHCPv6 server for the IPv6-address-to-FQDN mapping. In most case a client sends its hostname as a hint for the server. The DHCPv6 server MAY be configured to modify the supplied name or to substitute a different name. The server should send its notion of the complete FQDN for the client in the Domain Name field.

3.6. Client Link-layer Address Option

The Client link-layer address option [RFC6939] is used by first-hop DHCPv6 relays to provide the client's link-layer address towards the server.

DHCPv6 relay agents that receive messages originating from clients may include the link-layer source address of the received DHCPv6 message in the Client Link-Layer Address option, in relayed DHCPv6 Relay-Forward messages.

3.7. Option Request Option

DHCPv6 clients include an Option Request option [RFC3315] in DHCPv6 messages to inform the server about options the client wants the server to send to the client.

The content of an Option Request option are the option codes for options requested by the client. The client may additionally include instances of those options that are identified in the Option Request option, with data values as hints to the server about parameter values the client would like to have returned.

3.8. Vendor Class and Vendor-specific Information Options

The Vendor Class option, defined in Section 22.16 of [RFC3315], is used by a DHCPv6 client to identify the vendor that manufactured the hardware on which the client is running.

The Vendor-specific Information option, defined in Section 22.17 of [RFC3315], includes enterprise number, which identifies the client's vendor and often includes a number of additional parameters that are specific to a given vendor. That may include any type of information the vendor deems useful. It should be noted that this information may be present (and different) in both directions: client to server and server to client communications.

The information contained in the data area of this option is contained in one or more opaque fields that identify details of the hardware configuration, for example, the version of the operating

system the client is running or the amount of memory installed on the client.

3.9. Civic Location Option

DHCPv6 servers use the Civic Location option [RFC4776] to deliver location information (the civic and postal addresses) from the DHCPv6 server to DHCPv6 clients. It may refer to three locations: the location of the DHCPv6 server, the location of the network element believed to be closest to the client, or the location of the client, identified by the "what" element within the option.

3.10. Coordinate-Based Location Option

The GeoLoc options [RFC6225] are used by DHCPv6 server to provide coordinate-based geographic location information to DHCPv6 clients. They enable a DHCPv6 client to obtain its location.

3.11. Client System Architecture Type Option

The Client System Architecture Type option [RFC5970] is used by DHCPv6 client to send a list of supported architecture types to the DHCPv6 server. It is used by clients that must be booted using the network rather than from local storage, so the server can decide which boot file should be provided to the client.

3.12. Relay Agent Options

A DHCPv6 relay agent may include a number of options. Those option contain information that can be used to identify the client. Those options are almost exclusively exchanged between the relay agent and the server, thus never leaving the operators network. In particular, they're almost never present in the last wireless hop in case of WiFi networks. The only exception to that rule is somewhat infrequently used Relay Supplied Options option [RFC6422]. This fact implies that the threat model related relay options is slightly different. Traffic sniffing at the last hop and related class of attacks typically do not apply. On the other hand, all attacks that involve operator's intfrastructure (either willing or coerced cooperation or infrastructure being compromised) usually apply.

The following subsections describe various options inserted by the relay agents.

3.12.1. Subscriber ID Option

A DHCPv6 relay may include a Subscriber ID option [RFC4580] to associate some provider-specific information with clients' DHCPv6 messages that is independent of the physical network configuration.

In many deployments, the relay agent that inserts this option is configured to use client's link-layer address as Subscriber ID.

3.12.2. Interface ID Option

A DHCPv6 relay includes the Interface ID [RFC3315] option to identify the interface on which it received the client message that is being relayed.

Although in principle Interface ID can be arbitrarily long with completely random values, it is sometimes a text string that includes the relay agent name followed by interface name. This can be used for fingerprinting the relay or determining client's point of attachment.

3.12.3. Remote ID Option

A DHCPv6 relay includes a Remote ID option [RFC4649] to identify the remote host end of the circuit.

The remote-id is vendor specific, for which the vendor is indicated in the enterprise-number field. The remote-id field may encode the information that identified DHCPv6 clients:

- a "caller ID" telephone number for dial-up connection
- a "user name" prompted for by a Remote Access Server
- a remote caller ATM address o a "modem ID" of a cable data modem
- the remote IP address of a point-to-point link
- an interface or port identifier

3.12.4. Relay-ID Option

Relay agent may include Relay-ID [RFC5460], which contains a unique relay agent identifier. While its intended use is to provide additional information for the server, so it would be able to respond to leasequeries later, this information can be also used to identify client's location within the network.

4. Existing Mechanisms That Affect Privacy

This section describes deployed DHCPv6 mechanisms that can affect privacy.

4.1. Temporary addresses

[RFC3315] defines a mechanism for a client to request temporary addresses. The idea behind temporary addresses is that a client can request a temporary address for a specific purpose, use it, and then never renew it. i.e. let it expire.

There are a number of serious issues, both related to protocol and its implementations, that make temporary addresses nearly useless for their original goal. First, [RFC3315] does not include T1 and T2 renewal timers in IA_TA (a container for temporary addresses). However, in section 18.1.3 it explicitly mentions that temporary addresses can be renewed. Client implementations may mistakenly renew temporary addresses if they are not careful (i.e., by including the IA_TA with the same IAID in Renew or Rebind requests, rather than a new IAID - see [RFC3315] Section 22.5), thus forfeiting short liveness. [RFC4704] does not explicitly prohibit servers to update DNS for assigned temporary addresses and there are implementations that can be configured to do that. However, this is not advised as publishing a client's IPv6 address in DNS that is publicly available is a major privacy breach.

4.2. DNS Updates

The Client FQDN Option[RFC4704] used along with DNS Update [RFC2136] defines a mechanism that allows both clients and server to insert into the DNS domain information about clients. Both forward (AAAA) and reverse (PTR) resource records can be updated. This allows other nodes to conveniently refer to a host, despite the fact that its IPv6 address may be changing.

This mechanism exposes two important pieces of information: current address (which can be mapped to current location) and client's hostname. The stable hostname can then by used to correlate the client across different network attachments even when its IPv6 address keeps changing.

4.3. Allocation strategies

A DHCPv6 server running in typical, stateful mode is given a task of managing one or more pools of IPv6 resources (currently non-temporary addresses, temporary addresses and/or prefixes, but more resource types may be defined in the future). When a client requests a

resource, server must pick a resource out of configured pool. Depending on the server's implementation, various allocation strategies are possible. Choices in this regard may have privacy implications.

Iterative allocation - a server may choose to allocate addresses one by one. That strategy has the benefit of being very fast, thus being favored in deployments that prefer performance. However, it makes the resources very predictable. Also, since the resources allocated tend to be clustered at the beginning of an available pool, it makes scanning attacks much easier.

Identifier-based allocation - some server implementations use a fixed identifier for a specific client, seemingly taken from the client's MAC address when available or some lower bits of client's source IPv6 address. This has a property of being convenient for converting IP address to/from other identifiers, especially if the identifier is or contains MAC address. It is also convenient, as a returning client is very likely to get the same address, even if the server does not retain previous client's address. Those properties are convenient for system administrators, so DHCPv6 server implementors are sometimes requested to implement it. There is at least one implementation that supports it. The downside of such allocation is that the client now discloses its identifier in its IPv6 address to all services it connects to. That means that correlation of activities over time, location tracking, address scanning and OS/ vendor discovery attacks apply.

Hash allocation - it's an extension of identifier-based allocation. Instead of using the identifier directly, it is hashed first. If the hash is implemented correctly, it removes the flaw of disclosing the identifier, a property that eliminates susceptibility to address scanning and OS/vendor discovery. If the hash is poorly implemented (e.g., can be reversed), it introduces no improvement over identifier-based allocation. Even a well implemented hash does not mitigate the threat of correlation over time.

Random allocation - a server can pick a resource pseudo-randomly out of an available pool. This allocation scheme essentially prevents returning clients from getting the same address or prefix again. On the other hand, it is beneficial from privacy perspective as addresses and prefixes generated that way are not susceptible to correlation attacks, OS/vendor discovery attacks, or identity discovery attacks. Note that even though the address or prefix itself may be resilient to a given attack, the client may still be susceptible if additional information is disclosed other way, e.g., the client's address may be randomized, but it still can leak its MAC address in the client-id option.

Other allocation strategies may be implemented.

5. Attacks

5.1. Device type discovery (fingerprinting)

The type of device used by the client can be guessed by the attacker using the Vendor Class option, Vendor-specific Information option, the Client Link-layer Address option, and by parsing the Client ID option. All of those options may contain OUI (Organizationally Unique Identifier) that represents the device's vendor. That knowledge can be used for device-specific vulnerability exploitation attacks. See Section 3.4 of [I-D.ietf-6man-ipv6-address-generation-privacy] for a discussion about this type of attack.

5.2. Operating system discovery (fingerprinting)

The operating system running on a client can be guessed using the Vendor Class option, the Vendor-specific Information option, the Client System Architecture Type option, or by using fingerprinting techniques on the combination of options requested using the Option Request option. See Section 3.4 of [I-D.ietf-6man-ipv6-address-generation-privacy] for a discussion about this type of attack.

5.3. Finding location information

The physical location information can be obtained by the attacker by many means. The most direct way to obtain this information is by looking into a message originating from the server that contains the Civic Location or GeoLoc option. It can also be indirectly inferred using the Remote ID option, the Interface ID option (e.g., if an access circuit on an Access Node corresponds to a civic location), or the Subscriber ID option (if the attacker has access to subscriber info).

Another way to discover client's physical location is to use geolocation services. Those services typically map IP prefixes into geographical locations. Those services are usually based on known locations of the subnet, so they may reveal client's location as precise as they can locate a network it is connected to. They usually are not able to discover specific physical location within a network. That is not awlays true and it depends on the quality of the apriori information available in the geolocation services databases. It should be noted that this threat is general to the DHCPv6 mechanism. Regardless of the allocation strategy used by the DHCPv6 server implementation, the addresses assigned will always

belong to the subnet the server is configured to manage. Cases of using ULA (Unique Local Addresses) assigned by the DHCPv6 server are out of scope for this document.

5.4. Finding previously visited networks

When DHCPv6 clients connect to a network, they attempt to obtain the same address they had used before they attached to the network. They do this by putting the previously assigned address(es) in the IA Address option(s). [RFC3315] does not exclude IA_TA in such a case, so it is possible that a client implementation includes an address contained in an IA_TA for the Confirm message. By observing these addresses, an attacker can identify the network the client had previously visited.

5.5. Finding a stable identity

An attacker might use a stable identity gleaned from DHCPv6 messages to correlate activities of a given client on unrelated networks. The Client FQDN option, the Subscriber ID option, and the Client ID option can serve as long-lived identifiers of DHCPv6 clients. The Client FQDN option can also provide an identity that can easily be correlated with web server activity logs.

It should be noted that in general case, the MAC addresses as such are not available in the DHCPv6 packets. Therefore they cannot be used directly in a reliable way. However, they may become indirectly available using other mechanisms: client-id contains link-local address if DUID-LL or DUID-LLT types are used, source IPv6 address may use EUI-64 that contains MAC address, some access technologies may specify MAC address in dedicated options (e.g., cable modems use MAC addresses in DOCSIS options). Relay agents may insert additional information that are used to help the server to identify the client. This could be Remote-Id option, Subscriber-Id option, client link-layer address option or vendor specific information options. Options inserted by relay agents usually traverse only relay-server path, so they typically can't be eavesdropped by intercepting client's transmissions. This depends on the actual deployment model and used access technologies.

5.6. Pervasive monitoring

Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive

monitoring. PM is distinguished by being indiscriminate and very large scale, rather than by introducing new types of technical compromise.

See [RFC7258] for a discussion about PM.

5.7. Finding client's IP address or hostname

Many DHCPv6 deployments use DNS Updates [RFC4704] that put client's information (current IP address, client's hostname) into the DNS, where it is easily accessible by anyone interested. Client ID is also disclosed, albeit in not easily accessible form (SHA-256 digest of the client-id). As SHA-256 is considered irreversible, DHCID can't be converted back to client-id. However, SHA-256 digest can be used as an unique identifier that is accessible by any host.

5.8. Correlation of activities over time

As with other identifiers, an IPv6 address can be used to correlate the activities of a host for at least as long as the lifetime of the address. If that address was generated from some other, stable identifier and that generation scheme can be deduced by an attacker, the duration of the correlation attack extends to that of the identifier. In many cases, its lifetime is equal to the lifetime of the device itself. See Section 3.1 of [I-D.ietf-6man-ipv6-address-generation-privacy] for detailed discussion.

5.9. Location tracking

If a stable identifier is used for assigning an address and such mapping is discovered by an attacker (e.g., a server that uses IEEE-identifier-based IID to generate IPv6 address), all scenarios discussed in Section 3.2 of [I-D.ietf-6man-ipv6-address-generation-privacy] apply. In particular both passive (a service that the client connects to can log the client's address and draw conclusions regarding its location and movement patterns based on the prefix it is connecting from) and active (an attacker can send ICMPv6 echo requests or other probe packets to networks of suspected client locations) can be used. To give specific example, by accessing a social portal from tomek-laptop.coffee.somecity.com.example, tomek-laptop.mycompany.com.example and tomek-laptop.myisp.example.com, the portal administrator can draw conclusions about tomek-laptop's owner's current location and his habits.

5.10. Leasequery & bulk leasequery

Attackers may masquerade to be an access concentrator, either as a DHCPv6 relay agent or as a DHCPv6 client, to obtain location information directly from the DHCPv6 server(s) using the DHCPv6 Leasequery [RFC5007] mechanism.

Location information is information needed by the access concentrator to forward traffic to a broadband-accessible host. This information includes knowledge of the host hardware address, the port or virtual circuit that leads to the host, and/or the hardware address of the intervening subscriber modem.

Furthermore, the attackers may use the DHCPv6 bulk leasequery [RFC5460] mechanism to obtain bulk information about DHCPv6 bindings, even without knowing the target bindings.

Additionally, active leasequery [RFC7653] is a mechanism for subscribing to DHCPv6 lease update changes in near real-time. The intent of this mechanism is to update an operator's database, but if misused, an attacker could defeat the server's authentication mechanisms and subscribe to all updates. He then could continue receiving updates, without any need for local presence.

6. Security Considerations

In current practice, the client privacy and client authentication are mutually exclusive. The client authentication procedure reveals additional client information in their certificates/identifiers. Full privacy for the clients may mean the clients are also anonymous to the server and the network.

7. Privacy Considerations

This document in its entirety discusses privacy considerations in DHCPv6. As such, no dedicated discussion is needed.

8. IANA Considerations

This draft does not request any IANA action.

9. Acknowledgements

The authors would like to thank Stephen Farrell, Ted Lemon, Ines Robles, Russ White, Christian Schaefer, Jinmei Tatuya, Bernie Volz, Marcin Siodelski, Christian Huitema, Brian Haberman, Robert Sparks, Peter Yee and other members of DHC WG for their valuable comments.

This document was produced using the xml2rfc tool [RFC7749].

10. References

10.1. Normative References

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-08 (work in progress), September 2015.

[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>.

[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>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

10.2. Informative References

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <http://www.rfc-editor.org/info/rfc2136>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <http://www.rfc-editor.org/info/rfc3633>.

[RFC4580] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option", RFC 4580, DOI 10.17487/RFC4580, June 2006, <http://www.rfc-editor.org/info/rfc4580>.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, DOI 10.17487/RFC4649, August 2006, <http://www.rfc-editor.org/info/rfc4649>.

[RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4704, DOI 10.17487/RFC4704, October 2006, <http://www.rfc-editor.org/info/rfc4704>.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, DOI 10.17487/RFC4776, November 2006, <http://www.rfc-editor.org/info/rfc4776>.

[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>.

[RFC5007] Brzozowski, J., Kinnear, K., Volz, B., and S. Zeng, "DHCPv6 Leasequery", RFC 5007, DOI 10.17487/RFC5007, September 2007, <http://www.rfc-editor.org/info/rfc5007>.

[RFC5460] Stapp, M., "DHCPv6 Bulk Leasequery", RFC 5460, DOI 10.17487/RFC5460, February 2009, <http://www.rfc-editor.org/info/rfc5460>.

[RFC5970] Huth, T., Freimann, J., Zimmer, V., and D. Thaler, "DHCPv6 Options for Network Boot", RFC 5970, DOI 10.17487/RFC5970, September 2010, <http://www.rfc-editor.org/info/rfc5970>.

[RFC6225] Polk, J., Linsner, M., Thomson, M., and B. Aboba, Ed., "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", RFC 6225, DOI 10.17487/RFC6225, July 2011, <http://www.rfc-editor.org/info/rfc6225>.

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, DOI 10.17487/RFC6355, August 2011, <http://www.rfc-editor.org/info/rfc6355>.

[RFC6422] Lemon, T. and Q. Wu, "Relay-Supplied DHCP Options", RFC 6422, DOI 10.17487/RFC6422, December 2011, <http://www.rfc-editor.org/info/rfc6422>.

[RFC6939] Halwasia, G., Bhandari, S., and W. Dec, "Client Link-Layer Address Option in DHCPv6", RFC 6939, DOI 10.17487/RFC6939, May 2013, <http://www.rfc-editor.org/info/rfc6939>.

[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>.

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

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Tomek Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
USA

Email: tomasz.mrugalski@gmail.com

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 BeiQing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: jiangsheng@huawei.com