

6Lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2020

Y. Choi, Ed.
Y-G. Hong
ETRI
J-S. Youn
Donggeui Univ
D-K. Kim
KNU
J-H. Choi
Samsung Electronics Co.,
July 8, 2019

**Transmission of IPv6 Packets over Near Field Communication
draft-ietf-6lo-nfc-15**

Abstract

Near field communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm apart. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other devices. This document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques.

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 <https://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 January 9, 2020.

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](https://trustee.ietf.org/license-info) 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	2
2.	Conventions and Terminology	3
3.	Overview of Near Field Communication Technology	3
3.1.	Peer-to-peer Mode of NFC	4
3.2.	Protocol Stacks of NFC	4
3.3.	NFC-enabled Device Addressing	5
3.4.	MTU of NFC Link Layer	6
4.	Specification of IPv6 over NFC	7
4.1.	Protocol Stacks	7
4.2.	Link Model	7
4.3.	Stateless Address Autoconfiguration	8
4.4.	IPv6 Link Local Address	9
4.5.	Neighbor Discovery	9
4.6.	Dispatch Header	10
4.7.	Header Compression	10
4.8.	Fragmentation and Reassembly Considerations	11
4.9.	Unicast and Multicast Address Mapping	11
5.	Internet Connectivity Scenarios	12
5.1.	NFC-enabled Device Connected to the Internet	13
5.2.	Isolated NFC-enabled Device Network	13
6.	IANA Considerations	14
7.	Security Considerations	14
8.	Acknowledgements	14
9.	Normative References	14
	Authors' Addresses	16

[1. Introduction](#)

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to

424 kbit/s [[ECMA-340](#)]. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered. NFC builds upon RFID systems by allowing two-way communication between endpoints. At the time of this writing, it has been used in devices such as mobile phones, running Android operating system, named with a feature called "Android Beam". It is expected for the other mobile phones, running other operating systems (e.g., iOS, etc.) to be equipped with NFC technology in the near future.

Considering exponential growth in the number of heterogeneous air interface technologies, NFC has been widely used like Bluetooth Low Energy (BT-LE), Wi-Fi, and so on. Each of the heterogeneous air interface technologies has its own characteristics, which cannot be covered by the other technologies, so various kinds of air interface technologies would co-exist together. NFC can provide secured communications with its short transmission range.

When the number of devices and things having different air interface technologies communicate with each other, IPv6 is an ideal internet protocol owing to its large address space. Also, NFC would be one of the endpoints using IPv6. Therefore, this document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques.

[RFC4944] specifies the transmission of IPv6 over IEEE 802.15.4. The NFC link also has similar characteristics to that of IEEE 802.15.4. Many of the mechanisms defined in [[RFC4944](#)] can be applied to the transmission of IPv6 on NFC links. This document specifies the details of IPv6 transmission over NFC links.

2. Conventions and Terminology

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.

3. Overview of Near Field Communication Technology

NFC enables simple and two-way interaction between two devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC complements many popular consumer level wireless technologies, by utilizing the key elements in existing standards for contactless card

technology (ISO/IEC 14443 A&B and JIS-X 6319-4). NFC can be compatible with existing contactless card infrastructure and it enables a consumer to utilize one device across different systems.

Extending the capability of contactless card technology, NFC also enables devices to share information at a distance that is less than 10 cm with a maximum communication speed of 424 kbps. Users can share business cards, make transactions, access information from a smart poster or provide credentials for access control systems with a simple touch.

3.1. Peer-to-peer Mode of NFC

NFC-enabled devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer. Only peer-to-peer in the three modes enables two NFC-enabled devices to communicate with each other to exchange information and share files, so that users of NFC-enabled devices can quickly share contact information and other files with a touch. Therefore, the peer mode is used for ipv6-over-nfc. In addition, NFC-enabled devices can securely send IPv6 packets in wireless range when an NFC-enabled gateway is linked to the Internet.

3.2. Protocol Stacks of NFC

IP can use the services provided by the Logical Link Control Protocol (LLCP) in the NFC stack to provide reliable, two-way transmission of information between the peer devices. Figure 1 depicts the NFC P2P protocol stack with IPv6 bindings to LLCP.

For data communication in IPv6 over NFC, an IPv6 packet MUST be passed down to LLCP of NFC and transported to an Information (I) and an Unnumbered Information (UI) Field in Protocol Data Unit (PDU) of LLCP of the NFC-enabled peer device. LLCP does not support fragmentation and reassembly. For IPv6 addressing or address configuration, LLCP MUST provide related information, such as link layer addresses, to its upper layer. The LLCP to IPv6 protocol binding MUST transfer the SSAP and DSAP value to the IPv6 over NFC protocol. SSAP stands for Source Service Access Point, which is a 6-bit value meaning a kind of Logical Link Control (LLC) address, while DSAP means an LLC address of the destination NFC-enabled device.

Numbers Register. Address values between 10h and 1Fh are assigned by the local LLC to services registered by local service environment. In addition, address values between 20h and 3Fh are assigned by the local LLC as a result of an upper layer service request. Therefore, the address values between 20h and 3Fh can be used for generating IPv6 interface identifiers.

3.4. MTU of NFC Link Layer

As mentioned in [Section 3.2](#), an IPv6 packet MUST be passed down to LLC of NFC and transported to an Unnumbered Information Protocol Data Unit (UI PDU) and an Information Field in Protocol Data Unit (I PDU) of LLC of the NFC-enabled peer device.

The information field of an I PDU contains a single service data unit. The maximum number of octets in the information field is determined by the Maximum Information Unit (MIU) for the data link connection. The default value of the MIU for I PDUs is 128 octets. The local and remote LLCs each establish and maintain distinct MIU values for each data link connection endpoint. Also, an LLC is announce a larger MIU for a data link connection by transmitting an MIUX extension parameter within the information field. If no MIUX parameter is transmitted, the MIU value is 128 bytes. Otherwise, the MTU size in NFC LLC MUST be calculated from the MIU value as follows:

$$\text{MTU} = \text{MIU} = 128 + \text{MIUX}.$$

According to [\[LLCP-1.3\]](#), Figure 2 shows an example of the MIUX parameter TLV. Each of TLV Type and TLV Length field is 1 byte, and TLV Value field is 2 bytes.

0	0	1	2	3				
0	8	6	2	1				
+-----+-----+-----+-----+								
	Type		Length		Value			
+-----+-----+-----+-----+								
	00000010		00000010		1011		0x0~0x7FF	
+-----+-----+-----+-----+								

Figure 2: Example of MIUX Parameter TLV

When the MIUX parameter is encoded as a TLV option, the TLV Type field MUST be 0x02 and the TLV Length field MUST be 0x02. The MIUX parameter MUST be encoded into the least significant 11 bits of the TLV Value field. The unused bits in the TLV Value field MUST be set to zero by the sender and ignored by the receiver. A maximum value of the TLV Value field can be 0x7FF, and a maximum size of the MTU in

NFC LLCP is 2176 bytes including the 128 byte default of MIU. This value MUST be 0x480 to cover MTU of IPV6 if FAR is not used in IPv6 over NFC.

4. Specification of IPv6 over NFC

NFC technology also has considerations and requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards [RFC4944], [RFC6775], and [RFC6282] provide useful functionality for reducing overhead which can be applied to NFC. This functionality consists of link-local IPv6 addresses and stateless IPv6 address auto-configuration (see [Section 4.3](#)), Neighbor Discovery (see [Section 4.5](#)) and header compression (see [Section 4.7](#)).

4.1. Protocol Stacks

Figure 3 illustrates IPv6 over NFC. Upper layer protocols can be transport layer protocols (TCP and UDP), application layer protocols, and others capable running on top of IPv6.

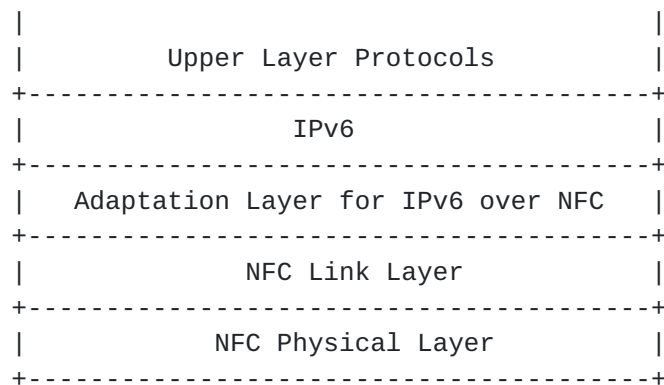


Figure 3: Protocol Stacks for IPv6 over NFC

The adaptation layer for IPv6 over NFC support neighbor discovery, stateless address auto-configuration, header compression, and fragmentation & reassembly.

4.2. Link Model

In the case of BT-LE, the Logical Link Control and Adaptation Protocol (L2CAP) supports fragmentation and reassembly (FAR) functionality; therefore, the adaptation layer for IPv6 over BT-LE does not have to conduct the FAR procedure. The NFC LLCP, in contrast, does not support the FAR functionality, so IPv6 over NFC needs to consider the FAR functionality, defined in [RFC4944]. However, the MTU on an NFC link can be configured in a connection

procedure and extended enough to fit the MTU of IPv6 packet (see [Section 4.8](#)).

This document does NOT RECOMMEND using FAR over NFC link. In addition, the implementation for this specification MUST use MIUX extension to communicate the MTU of the link to the peer as defined in [Section 3.4](#).

The NFC link between two communicating devices is considered to be a point-to-point link only. Unlike in BT-LE, an NFC link does not support a star topology or mesh network topology but only direct connections between two devices. Furthermore, the NFC link layer does not support packet forwarding in link layer. Due to this characteristics, 6LoWPAN functionalities, such as addressing and auto-configuration, and header compression, need to be specialized into IPv6 over NFC.

4.3. Stateless Address Autoconfiguration

An NFC-enabled device (i.e., 6LN) performs stateless address autoconfiguration as per [\[RFC4862\]](#). A 64-bit Interface identifier (IID) for an NFC interface is formed by utilizing the 6-bit NFC SSAP (see [Section 3.3](#)). In the viewpoint of address configuration, such an IID should guarantee a stable IPv6 address during the course of a single connection, because each data link connection is uniquely identified by the pair of DSAP and SSAP included in the header of each LLC PDU in NFC.

Following the guidance of [\[RFC7136\]](#), interface identifiers of all unicast addresses for NFC-enabled devices are 64 bits long and constructed by using the generation algorithm of random (but stable) identifier (RID) [\[RFC7217\]](#) (see Figure 4).

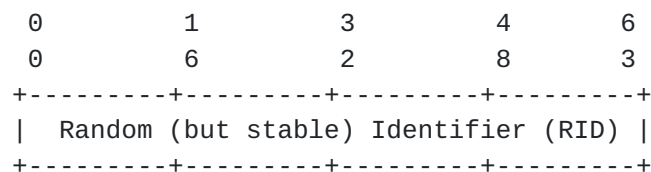


Figure 4: IID from NFC-enabled device

The RID is an output which is created by the algorithm, `F()` with input parameters. One of the parameters is `Net_IFace`, and NFC Link Layer address (i.e., SSAP) is a source of the `NetIFace` parameter. The 6-bit address of SSAP of NFC is easy and short to be targeted by attacks of third party (e.g., address scanning). The `F()` can provide secured and stable IIDs for NFC-enabled devices. In addition, an

optional parameter, Network_ID is used to increase the randomness of the generated IID.

4.4. IPv6 Link Local Address

The IPv6 link-local address for an NFC-enabled device is formed by appending the IID, to the prefix FE80::/64, as depicted in Figure 5.

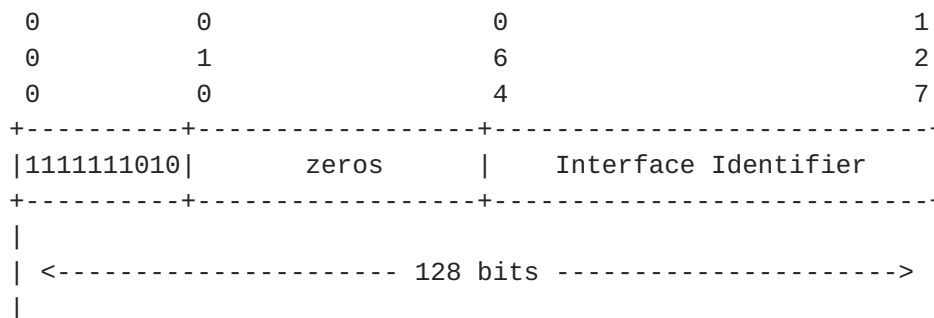


Figure 5: IPv6 link-local address in NFC

The tool for a 6LBR to obtain an IPv6 prefix for numbering the NFC network can be accomplished via DHCPv6 Prefix Delegation ([RFC3633]). The "Interface Identifier" is used the secured and stable IIDs for NFC-enabled devices.

4.5. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs ([RFC6775]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC does not support a complicated mesh topology but only a simple multi-hop network topology or directly connected peer-to-peer network. Therefore, the following aspects of RFC 6775 are applicable to NFC:

- o When an NFC-enabled device (6LN) is directly connected to a NFC-enabled 6LBR, an NFC 6LN MUST register its address with the 6LBR[RFC4944] by sending a Neighbor Solicitation (NS) message with the Address Registration Option (ARO) and process the Neighbor Advertisement (NA) accordingly. In addition, when the 6LN and 6LBR are directly connected, DHCPv6 is used for address assignment. Therefore, Duplicate Address Detection (DAD) is not necessary between them.
- o When two or more NFC 6LNs[RFC4944](or 6LRs) are connected, there are two cases. One is that three or more NFC devices are linked with multi-hop connections, and the other is that they meet within a single hop range (e.g., isolated network). In a case of multi-hops, all of 6LNs, which have two or more connections with

different neighbors, is a router for 6LR/6LBR. In a case that they meet within a single hop and they have the same properties, any of them can be a router.

- o For sending Router Solicitations and processing Router Advertisements, the NFC 6LNs MUST follow Sections [5.3](#) and [5.4](#) of [\[RFC6775\]](#).
- o When a NFC device becomes a 6LR or a 6LBR, the NFC device MUST follow [Section 6](#) and 7 of [\[RFC6775\]](#).

[4.6.](#) Dispatch Header

All IPv6-over-NFC encapsulated datagrams are prefixed by an encapsulation header stack consisting of a Dispatch value followed by zero or more header fields. The only sequence currently defined for IPv6-over-NFC is the LOWPAN_IPHC header followed by payload, as depicted in Figure 6.

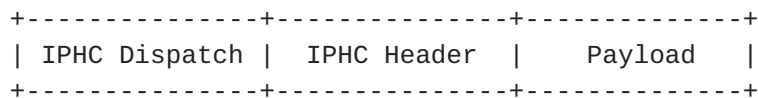


Figure 6: A IPv6-over-NFC Encapsulated 6LOWPAN_IPHC Compressed IPv6 Datagram

The dispatch value is treated as an unstructured namespace. Only a single pattern is used to represent current IPv6-over-NFC functionality.

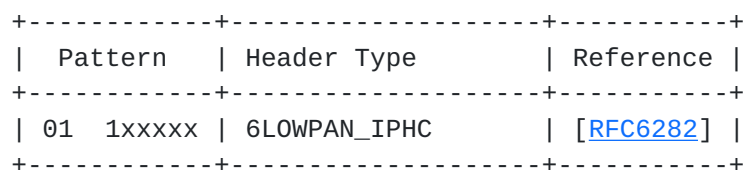


Figure 7: Dispatch Values

Other IANA-assigned 6LowPAN Dispatch values do not apply to this specification.

[4.7.](#) Header Compression

Header compression as defined in [\[RFC6282\]](#), which specifies the compression format for IPv6 datagrams on top of IEEE 802.15.4, is REQUIRED in this document as the basis for IPv6 header compression on top of NFC. All headers MUST be compressed according to [RFC 6282](#) encoding formats.

Therefore, IPv6 header compression in [[RFC6282](#)] MUST be implemented. Further, implementations MUST also support Generic Header Compression (GHC) of [[RFC7400](#)].

If a 16-bit address is required as a short address, it MUST be formed by padding the 6-bit NFC link-layer (node) address to the left with zeros as shown in Figure 8.

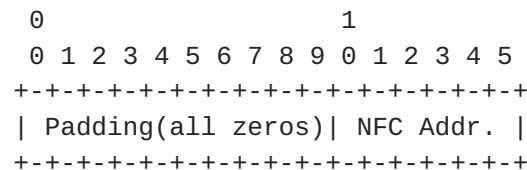


Figure 8: NFC short address format

[4.8.](#) Fragmentation and Reassembly Considerations

IPv6-over-NFC MUST NOT use fragmentation and reassembly (FAR) for the payloads as discussed in [Section 3.4](#). The NFC link connection for IPv6 over NFC MUST be configured with an equivalent MIU size to fit the MTU of IPv6 Packet. The MIUX value is 0x480 in order to fit the MTU (1280 bytes) of a IPv6 packet if NFC devices support extension of the MTU. However, if the NFC device does not support extension, IPv6-over-NFC uses FAR with the default MTU (128 bytes), as defined in [[RFC4944](#)].

[4.9.](#) Unicast and Multicast Address Mapping

The address resolution procedure for mapping IPv6 non-multicast addresses into NFC link-layer addresses follows the general description in [Section 4.6.1](#) and 7.2 of [[RFC4861](#)], unless otherwise specified.

The Source/Target link-layer Address option has the following form when the addresses are 6-bit NFC link-layer (node) addresses.

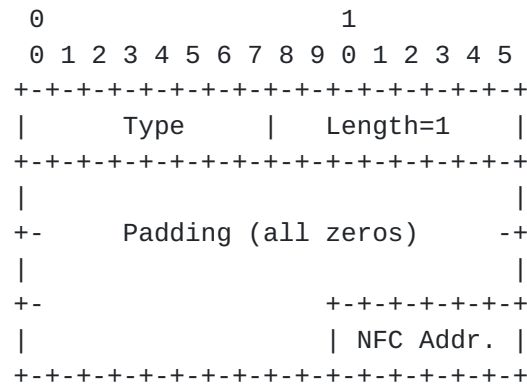


Figure 9: Unicast address mapping

Option fields:

Type:

- 1: for Source Link-layer address.
- 2: for Target Link-layer address.

Length:

This is the length of this option (including the type and length fields) in units of 8 octets. The value of this field is 1 for 6-bit NFC node addresses.

NFC address:

The 6-bit address in canonical bit order. This is the unicast address the interface currently responds to.

The NFC Link Layer does not support multicast. Therefore, packets are always transmitted by unicast between two NFC-enabled devices. Even in the case where a 6LBR is attached to multiple 6LNs, the 6LBR cannot do a multicast to all the connected 6LNs. If the 6LBR needs to send a multicast packet to all its 6LNs, it has to replicate the packet and unicast it on each link.

5. Internet Connectivity Scenarios

NFC networks can be isolated and connected to the Internet.

5.1. NFC-enabled Device Connected to the Internet

One of the key applications of using IPv6 over NFC is securely transmitting IPv6 packets because the RF distance between 6LN and 6LBR is typically within 10 cm. If any third party wants to hack into the RF between them, it must come to nearly touch them. Applications can choose which kinds of air interfaces (e.g., BT-LE, Wi-Fi, NFC, etc.) to send data depending on the characteristics of the data.

Figure 10 illustrates an example of an NFC-enabled device network connected to the Internet. The distance between 6LN and 6LBR is typically 10 cm or less. If there is any laptop computers close to a user, it will become a 6LBR. Additionally, when the user mounts an NFC-enabled air interface adapter (e.g., portable NFC dongle) on the close laptop PC, the user's NFC-enabled device (6LN) can communicate with the laptop PC (6LBR) within 10 cm distance.



Figure 10: NFC-enabled device network connected to the Internet

Two or more 6LNs are connected with a 6LBR, but each connection uses a different subnet. The 6LBR is acting as a router and forwarding packets between 6LNs and the Internet. Also, the 6LBR MUST ensure address collisions do not occur and forwards packets sent by one 6LN to another.

5.2. Isolated NFC-enabled Device Network

In some scenarios, the NFC-enabled device network may transiently be a simple isolated network as shown in the Figure 11.

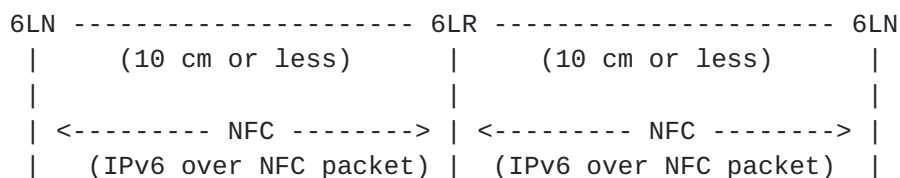


Figure 11: Isolated NFC-enabled device network

In mobile phone markets, applications are designed and made by user developers. They may image interesting applications, where three or

more mobile phones touch or attach each other to work achieve a common objective. In an isolated NFC-enabled device network, when two or more 6LRs are connected with each other, and then they are acting like routers, the 6LR MUST ensure address collisions do not occur.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

This document does not RECOMMEND sending NFC packets over the Internet or any unsecured network.

When interface identifiers (IIDs) are generated, devices and users are required to consider mitigating various threats, such as correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning.

IPv6-over-NFC uses an IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits for the modified EUI-64 format. However, NFC applications use short-lived connections, and the every connection is made with different address of NFC link with an extremely short-lived link.

This document does not RECOMMEND sending NFC packets over the Internet or any unsecured network. Especially, there can be a threat model in the scenario of [Section 5.1](#). when the NFC-enabled device links to a NFC-enabled gateway for connectivity with the Internet, the gateway can be attacked. Even though IPv6 over NFC guarantees security between the two NFC devices, there can be another threat during packet forwarding.

8. Acknowledgements

We are grateful to the members of the IETF 6lo working group.

Michael Richardson, Suresh Krishnan, Pascal Thubert, Carsten Bormann, Alexandru Petrescu, James Woodyatt, Dave Thaler, Samita Chakrabarti, and Gabriel Montenegro have provided valuable feedback for this draft.

9. Normative References

[ECMA-340]

"Near Field Communication - Interface and Protocol (NFCIP-1) 3rd Ed.", ECMA-340 , June 2013.

[LLCP-1.3]

"NFC Logical Link Control Protocol version 1.3", NFC Forum Technical Specification , March 2016.

- [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>>.

- [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, <<https://www.rfc-editor.org/info/rfc3633>>.

- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc4862>>.

- [RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", [RFC 4944](#), DOI 10.17487/RFC4944, September 2007, <<https://www.rfc-editor.org/info/rfc4944>>.

- [RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", [RFC 6282](#), DOI 10.17487/RFC6282, September 2011, <<https://www.rfc-editor.org/info/rfc6282>>.

- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.

- [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", [RFC 7136](#), DOI 10.17487/RFC7136, February 2014, <<https://www.rfc-editor.org/info/rfc7136>>.

- [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, <<https://www.rfc-editor.org/info/rfc7217>>.
- [RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 7400](#), DOI 10.17487/RFC7400, November 2014, <<https://www.rfc-editor.org/info/rfc7400>>.
- [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>>.

Authors' Addresses

Younghwan Choi (editor)
Electronics and Telecommunications Research Institute
218 Gajeongno, Yuseung-gu
Daejeon 34129
Korea

Phone: +82 42 860 1429
Email: yhc@etri.re.kr

Yong-Geun Hong
Electronics and Telecommunications Research Institute
161 Gajeong-Dong Yuseung-gu
Daejeon 305-700
Korea

Phone: +82 42 860 6557
Email: yghong@etri.re.kr

Joo-Sang Youn
DONG-EUI University
176 Eomgwangno Busan_jin_gu
Busan 614-714
Korea

Phone: +82 51 890 1993
Email: joosang.youn@gmail.com

Dongkyun Kim
Kyungpook National University
80 Daehak-ro, Buk-gu
Daegu 702-701
Korea

Phone: +82 53 950 7571
Email: dongkyun@knu.ac.kr

JinHyouk Choi
Samsung Electronics Co.,
129 Samsung-ro, Youngdong-gu
Suwon 447-712
Korea

Phone: +82 2 2254 0114
Email: jinchoe@samsung.com

