

6Lo Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: February 12, 2021

Y. Choi, Ed.  
Y-G. Hong  
ETRI  
J-S. Youn  
Donggeui Univ  
D-K. Kim  
KNU  
J-H. Choi  
Samsung Electronics Co.,  
August 11, 2020

Transmission of IPv6 Packets over Near Field Communication  
draft-ietf-6lo-nfc-17

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 February 12, 2021.

## Copyright Notice

Copyright (c) 2020 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 . . . . .	2
2.	Conventions and Terminology . . . . .	3
3.	Overview of Near Field Communication Technology . . . . .	3
3.1.	Peer-to-peer Mode of NFC . . . . .	3
3.2.	Protocol Stack of NFC . . . . .	4
3.3.	NFC-enabled Device Addressing . . . . .	5
3.4.	MTU of NFC Link Layer . . . . .	5
4.	Specification of IPv6 over NFC . . . . .	6
4.1.	Protocol Stack . . . . .	6
4.2.	Stateless Address Autoconfiguration . . . . .	7
4.3.	IPv6 Link-Local Address . . . . .	8
4.4.	Neighbor Discovery . . . . .	8
4.5.	Dispatch Header . . . . .	9
4.6.	Header Compression . . . . .	9
4.7.	Fragmentation and Reassembly Considerations . . . . .	10
4.8.	Unicast and Multicast Address Mapping . . . . .	10
5.	Internet Connectivity Scenarios . . . . .	11
5.1.	NFC-enabled Device Network Connected to the Internet . . . . .	11
5.2.	Isolated NFC-enabled Device Network . . . . .	12
6.	IANA Considerations . . . . .	12
7.	Security Considerations . . . . .	12
8.	Acknowledgements . . . . .	13
9.	Normative References . . . . .	13
	Authors' Addresses . . . . .	14

## 1. Introduction

NFC is a set of short-range wireless technologies, typically requiring a distance between sender and receiver of 10 cm or less. NFC operates at 13.56 MHz, and at rates ranging from 106 kbit/s to 424 kbit/s, as per the ISO/IEC 18000-3 air interface [ECMA-340]. NFC

builds upon RFID systems by allowing two-way communication between endpoints. 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, while avoiding the need for batteries. NFC peer-to-peer communication is possible, provided that both devices are powered. As of the writing, NFC is supported by the main smartphone operating systems.

NFC is often regarded as a secure communications technology, due to its very short transmission range.

In order to benefit from Internet connectivity, it is desirable for NFC-enabled devices to support IPv6, considering its large address space, along with tools for unattended operation, among other advantages. This document specifies how IPv6 is supported over NFC by using IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) techniques [RFC4944], [RFC6282], [RFC6775]. 6LoWPAN is suitable, considering that it was designed to support IPv6 over IEEE 802.15.4 networks, and some of the characteristics of the latter are similar to those of NFC.

## 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

This section presents an overview of NFC, focusing on the characteristics of NFC that are most relevant for supporting IPv6.

NFC enables simple, two-way, interaction between two devices, allowing users to perform contactless transactions, access digital content, and connect electronic devices with a single touch. NFC utilizes key elements in existing standards for contactless card Technology, such as ISO/IEC 14443 A&B and JIS-X 6319-4. NFC allows devices to share information at a distance up to 10 cm with a maximum physical layer bit rate of 424 kbps.

### 3.1. Peer-to-peer Mode of NFC

NFC defines three modes of operation: card emulation, peer-to-peer, and reader/writer. Only the peer-to-peer mode allows two NFC-enabled devices to communicate with each other to exchange information

bidirectionally. The other two modes do not support two-way communications between two devices. Therefore, the peer-to-peer mode is used for IPv6 over NFC.

### 3.2. Protocol Stack of NFC

NFC defines a protocol stack for the peer-to-peer mode (Figure 1). The peer-to-peer mode is offered by the Activities Digital Protocol at the NFC Physical Layer. The NFC Logical Link Layer comprises the Logical Link Control Protocol (LLCP), and when IPv6 is used over NFC, it also includes an IPv6-LLCP Binding. IPv6 and its underlying adaptation Layer (i.e., IPv6-over-NFC adaptation layer) are placed directly on the top of the IPv6-LLCP Binding. An IPv6 datagram is transmitted by the Logical Link Control Protocol (LLCP) with reliable, two-way transmission of information between the peer devices.

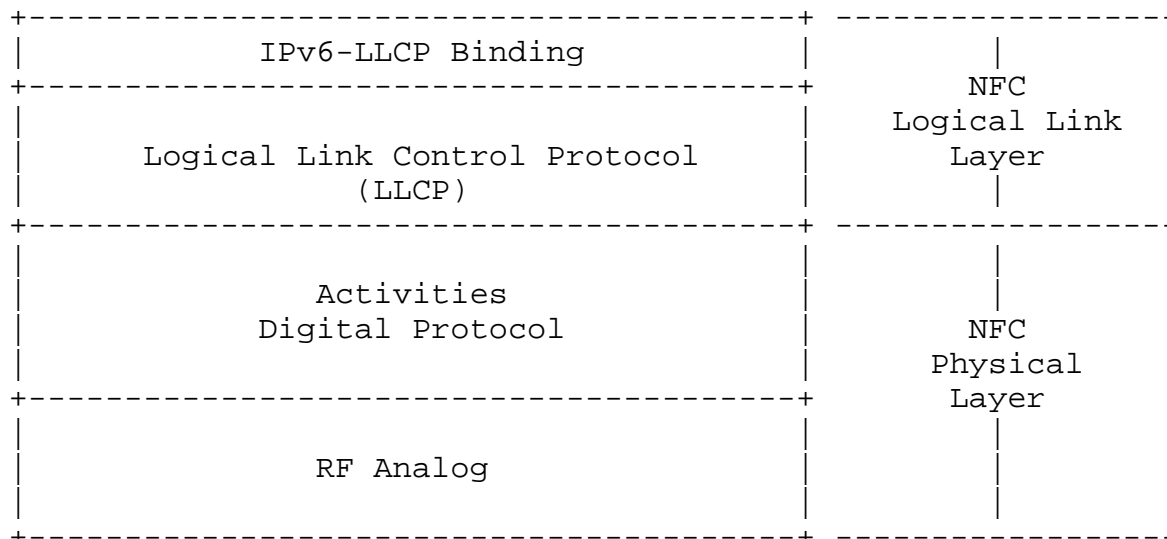


Figure 1: Protocol Stack of NFC

The LLCP consists of Logical Link Control (LLC) and MAC Mapping. The MAC Mapping integrates an existing RF protocol into the LLCP architecture. The LLC contains three components, such as Link Management, Connection-oriented Transmission, and Connectionless Transmission. The Link Management component is responsible for serializing all connection-oriented and connectionless LLC PDU (Protocol Data Unit) exchanges and for aggregation and disaggregation of small PDUs. The Connection-oriented Transmission component is responsible for maintaining all connection-oriented data exchanges including connection set-up and termination. The Connectionless

Transmission component is responsible for handling unacknowledged data exchanges.

In order to send an IPv6 packet over NFC, the packet MUST be passed down to the LLC layer of NFC and carried by an Information Field in an LLC Protocol Data Unit (I PDU). The LLC does not support fragmentation and reassembly. For IPv6 addressing or address configuration, the LLC MUST provide related information, such as link layer addresses, to its upper layer. The LLC to IPv6 protocol binding MUST transfer the Source Service Access Point (SSAP) and Destination Service Access Point (DSAP) value to the IPv6 over NFC protocol. SSAP is a Logical Link Control (LLC) address of the source NFC-enabled device with a size of 6 bits, while DSAP means an LLC address of the destination NFC-enabled device. Thus, SSAP is a source address, and DSAP is a destination address.

### 3.3. NFC-enabled Device Addressing

According to NFC LLC v1.3 [LLCP-1.3], NFC-enabled devices have two types of 6-bit addresses (i.e., SSAP and DSAP) to identify service access points. Several service access points can be installed on a NFC device. However, the SSAP and DSAP can be used as identifiers for NFC link connections with the IPv6 over NFC adaptation layer. Therefore, the SSAP can be used to generate an IPv6 interface identifier. Address values between 00h and 0Fh of SSAP and DSAP are reserved for identifying the well-known service access points, which are defined in the NFC Forum Assigned 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, when an IPv6 packet is transmitted, the packet MUST be passed down to LLC of NFC and transported to an 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 may announce a larger MIU for a data link connection by transmitting an optional Maximum Information Unit Extension (MIUX) parameter within the information field. If no MIUX parameter is transmitted, the MIU

value is 128 bytes. Otherwise, the MTU size in NFC LLCP 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. The Type and Length fields of the MIUX parameter TLV have each a size of 1 byte. The size of the 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 used, 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. The maximum possible value of the TLV Value field is 0x7FF, and the maximum size of the LLCP MTU is 2175 bytes. The MIUX value MUST be 0x480 to support the IPv6 MTU requirement (of 1280 bytes).

#### 4. Specification of IPv6 over NFC

NFC technology has requirements owing to low power consumption and allowed protocol overhead. 6LoWPAN standards [RFC4944], [RFC6775], and [RFC6282] provide useful functionality for reducing the overhead of IPv6 over NFC. This functionality consists of link-local IPv6 addresses and stateless IPv6 address auto-configuration (see Section 4.2 and Section 4.3), Neighbor Discovery (see Section 4.4) and header compression (see Section 4.6).

##### 4.1. Protocol Stack

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

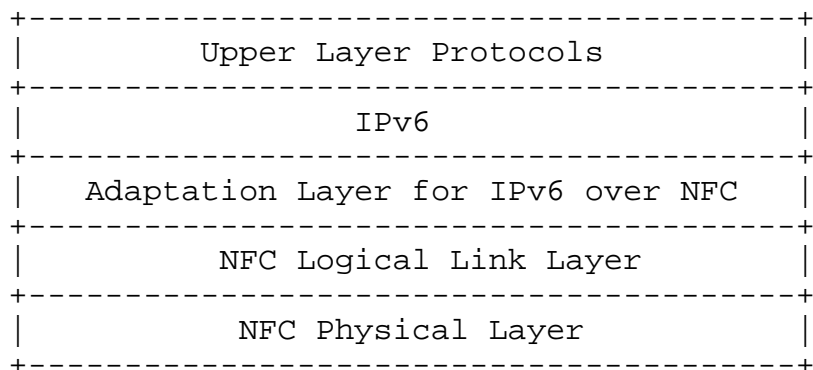


Figure 3: Protocol Stack for IPv6 over NFC

The adaptation layer for IPv6 over NFC supports neighbor discovery, stateless address auto-configuration, header compression, and fragmentation & reassembly, based on 6LoWPAN.

#### 4.2. Stateless Address Autoconfiguration

An NFC-enabled device 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).

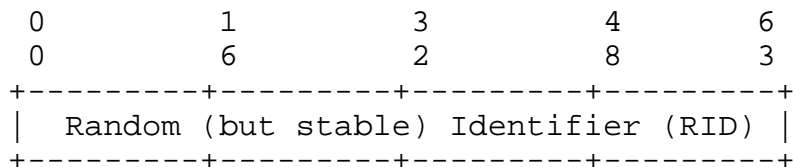


Figure 4: IID from NFC-enabled device

The RID is an output which is created by the F() algorithm with input parameters. One of the parameters is Net\_Iface, and NFC Link Layer address (i.e., SSAP) is a source of the Net\_Iface parameter. The 6-bit address of SSAP of NFC is short and easy to be targeted by attacks of third party (e.g., address scanning). The F() algorithm 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.

#### 4.3. 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.

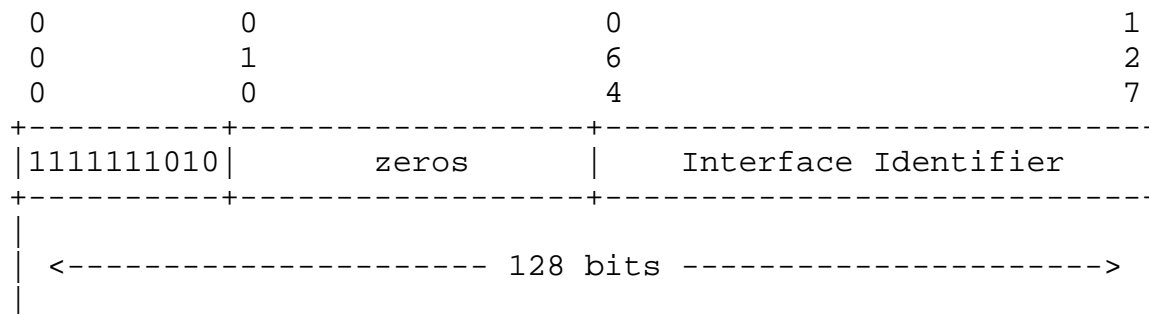


Figure 5: IPv6 link-local address in NFC

A 6LBR may obtain an IPv6 prefix for numbering the NFC network via DHCPv6 Prefix Delegation ([RFC3633]). The "Interface Identifier" can be a secured and stable IID.

#### 4.4. Neighbor Discovery

Neighbor Discovery Optimization for 6LoWPANs ([RFC6775]) describes the neighbor discovery approach in several 6LoWPAN topologies, such as mesh topology. NFC supports mesh topologies but most of all applications would use a simple multi-hop network topology or directly connected peer-to-peer network because NFC RF range is very short.

- o When an NFC-enabled 6LN is directly connected to an NFC-enabled 6LBR, the NFC 6LN MUST register its address with the 6LBR by sending a Neighbor Solicitation (NS) message with the Extended Address Registration Option (EARO) [RFC8505], 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 devices 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. Two NFC devices might still talk to each other (point-to-point topology), but one of them may be connected to the Internet. In a case of multi-hop topology, devices which have two or more



connections with neighbor devices, may act as routers. 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 is a 6LR or a 6LBR, the NFC device MUST follow Section 6 and 7 of [RFC6775].

#### 4.5. Dispatch Header

All IPv6-over-NFC encapsulated datagrams are prefixed by an encapsulation header stack consisting of a Dispatch value. The only sequence currently defined for IPv6-over-NFC is the LOWPAN\_IPHC compressed IPv6 header (see Section 4.6) header followed by payload, as depicted in Figure 6.

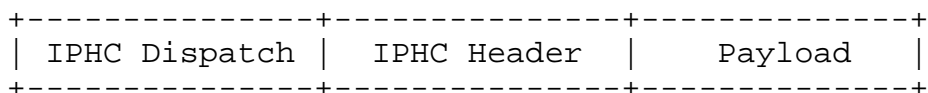


Figure 6: A IPv6-over-NFC Encapsulated 6LOWPAN\_IPHC Compressed IPv6 Datagram

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

Pattern	Header Type	Reference
01 1xxxxx	6LOWPAN_IPHC	[RFC6282]

Figure 7: Dispatch Values

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

#### 4.6. 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.

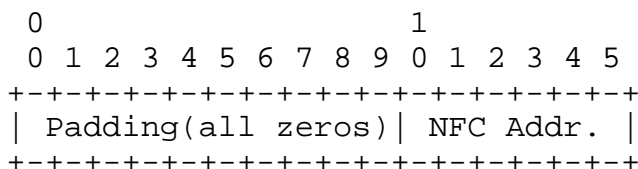


Figure 8: NFC short address format

#### 4.7. Fragmentation and Reassembly Considerations

IIPv6-over-NFC MUST NOT use fragmentation and reassembly (FAR) at the adaptation layer 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 support the IPv6 MTU requirement (of 1280 bytes). To this end, the MIUX value is 0x480.

#### 4.8. 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.

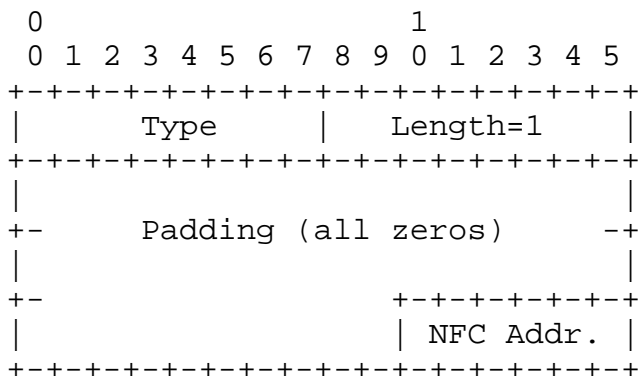


Figure 9: Unicast address mapping

### 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 either be isolated or connected to the Internet. The NFC link between two communicating devices is considered to be a point-to-point link only. An NFC link does not support a star topology or mesh network topology but only direct connections between two devices. The NFC link layer does not support packet forwarding at link layer.

### 5.1. NFC-enabled Device Network Connected to the Internet

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. For example, a laptop computer that is connected to the Internet (e.g. via Wi-Fi, Ethernet, etc.) may also support NFC and act as a 6LBR. Another NFC-enabled device may run as a 6LN and communicate with the 6LBR, as long as both are within each other's range.

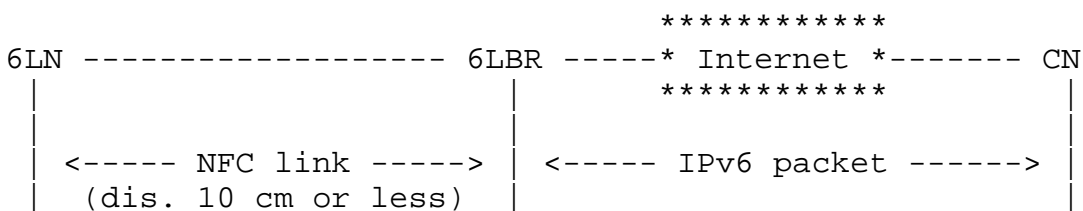


Figure 10: NFC-enabled device network connected to the Internet

Two or more 6LNs may be 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 permanently be a simple isolated network as shown in the Figure 11.

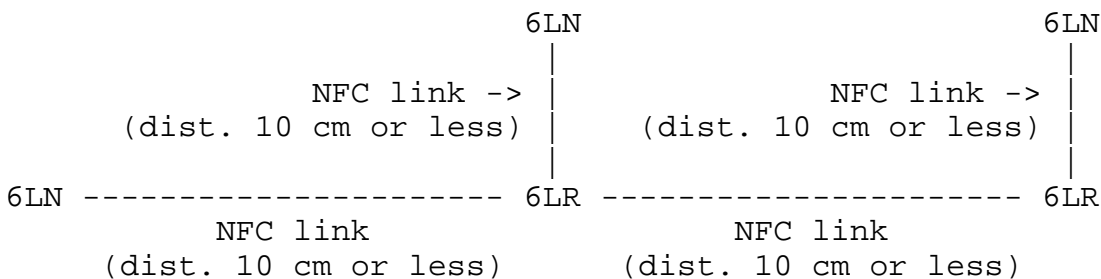


Figure 11: Isolated NFC-enabled device network

## 6. IANA Considerations

There are no IANA considerations related to this document.

## 7. Security Considerations

NFC is often considered to offer intrinsic security properties due to its short link range. 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 a different address is used for each connection, where the latter is of extremely short duration.

## 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, Gabriel Montenegro and Carles Gomez Montenegro have provided valuable feedback for this document.

## 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>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.

#### 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](mailto: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